Case No. 21-12835

UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

APPLE, INC.,

Plaintiff-Appellant,

v.

CORELLIUM, LLC,

Defendant-Appellee.

On Appeal from the United States District Court
for the Southern District of Florida,
District 113C-9, Case No. 9:19-cv-81160-RS
Honorable Rodney Smith

BRIEF OF AMICI CURIAE COMPUTER SECURITY RESEARCHERS, ELECTRONIC FRONTIER FOUNDATION, AND PUBLIC KNOWLEDGE, IN SUPPORT OF APPELLEE AND AFFIRMANCE

Alejandra Caraballo
Counsel of Record
HARVARD CYBERLAW CLINIC
Harvard Law School
1557 Massachusetts Ave, 4th Fl
Cambridge, MA 02138
Tel: (617) 384-8511
Email: acaraballo@law.harvard.edu

Corynne McSherry
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Email: corynne@eff.org

John Bergmayer
PUBLIC KNOWLEDGE
1818 N Street NW, Suite 410
Washington, DC 20036
Tel: (202) 861-0020
Email: john@publicknowledge.org

Counsel for Amici Curiae

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Local Rule 26.1-1, *amici curiae* certify that the following trial judges, attorneys, persons, associations of persons, firms, partnerships, and corporations have an interest in the outcome of this case or appeal, in addition to those listed in prior filings:

1. Bergmayer, John: Counsel for Amici Curiae
2. Caraballo, Alejandra: Counsel for Amici Curiae
3. Electronic Frontier Foundation: Amicus Curiae
4. Ellis, Casey: Amicus Curiae
5. McSherry, Corynne: Counsel for Amici Curiae
6. Miller, Charlie: Amicus Curiae
7. Moussouris, Katie: Amicus Curiae
8. Public Knowledge: Amicus Curiae
9. Schneier, Bruce: Amicus Curiae
10. Shostack, Adam: Amicus Curiae
11. Valasek, Chris: Amicus Curiae
12. Wheeler, Tarah: Amicus Curiae
13. Zatko, Peiter: Amicus Curiae
14. Zatko, Sarah: Amicus Curiae

Pursuant to Fed. R. App. P. 26.1, *amici curiae* certify that Electronic Frontier Foundation and Public Knowledge are non-profit organizations that have no parent corporation, and no publicly held corporation owns 10 percent or more of their stock.

Dated: February 16, 2022

Respectfully submitted,

/s/ Alejandra Caraballo

Alejandra Caraballo
Counsel of Record
HARVARD CYBERLAW CLINIC
Harvard Law School
1557 Massachusetts Ave, 4th Fl
Cambridge, MA 02138
Tel: (617) 384-8511
Email: acaraballo@law.harvard.edu

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

Lorenzo Franceschi-Bicchierai, *Apple's Copyright Lawsuit Has Created a 'Chilling Effect' on Security Research*, VICE (May 5, 2020)................................21

Mark A. Lemley and R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 Stan. L. Rev. 1345 (2004)............................22

Michael A. Carrier, *Copyright and Innovation: The Untold Story*, 2012 WIS. L. REV. 891 (2012)...22

Michael Kan, *Apple Patches New Zero-Day iOS Vulnerability Possibly Under Exploitation*, PCMAG (Oct. 11, 2021)..28

Nicole Perlroth, *Apple Issues Emergency Security Updates to Close a Spyware Flaw*, NEW YORK TIMES (Oct. 15, 2021) 5, 29

Nissan Leaf Can be Hacked via Mobile App and Web Browser, TREND MICRO (Feb. 26, 2016) 10

Pamela Samuelson, *Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519 (1999)...20

PIA Research Team, *Hacking the World – Part 4: The Cost and Future of Hacking (Plus: Safety Tips)*, PRIVATE INTERNET ACCESS (Oct. 25, 2021)...........................7

Redscan, *NIST Security Vulnerability Trends in 2020: An Analysis* (2021).............7

Reed Albergotti, *Apple Pays Hackers Six Figures to Find Bugs in its Software. Then it Sits on Their Findings.*, WASHINGTON POST (Sept. 9, 2021)............ 16, 18

Research Threats: Legal Threats Against Security Researchers, disclose.io .. 20, 21

Simon J. Frankel and Matt Kellogg, *Bad Faith and Fair Use*, 60 J. COPYRIGHT SOC'Y U.S.A. 1 (2012) 30, 31

Sunoo Park and Kendra Albert, Berkman Klein Center for Internet & Society and Electronic Frontier Foundation, *A Researcher's Guide to Some Legal Risks of Security Research* (2020) 20

The Heartbleed Bug (June 3, 2020)...9

Thomas Brewster, *Watch a Tesla Have Its Doors Hacked Open by a Drone*, FORBES (Apr. 29, 2021)..6

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization working to protect free speech and privacy in the digital world. Founded in 1990, EFF has more than 33,000 active donors and dues-paying members across the United States. EFF offers pro bono legal services to researchers who conduct cutting-edge inquiry into technology in the public interest that may be chilled by unfounded litigation.

Public Knowledge is a non-profit public interest organization that defends consumer rights online. Public Knowledge promotes balanced intellectual property policies that promote the public interest, ensure that the public can access knowledge, and protect the legitimate interests of authors.

Amici also include individual computer security researchers who have helped advance the safety and integrity of information technology in the service of consumers, businesses, and governments. *Amici* believe their work serves the public interst in multiple ways, and does not infringe copyright. *Amici* also know that legal

[1] All parties consent to the filing of this brief. No party's counsel authored this brief in whole or in part, and neither any party, nor any party's counsel, contributed money towards the preparation of this brief. No person other than amici, their members, or their counsel contributed money that was intended to fund preparing or submitting this brief. In an abundance of caution and for the sake of transparency, counsel state that amicus Electronic Frontier Foundation and co-counsel Cyberlaw Clinic each consulted briefly with Appellee prior to the commencement of this litigation.

threats can chill research and innovation, and rely on protections, such as fair use, to help us resist such threats. Individual *amici* are:

Casey Ellis
Founder/Chairman/CTO, Bugcrowd

Charlie Miller
Principal Autonomous Vehicle Security Architect, Cruise Automation

Katie Moussouris
Co-Editor, ISO 29147 Vulnerability Disclosure
Co-Editor, ISO 30111 Vulnerability Handling Processes
Board Member, NIST ISPAB

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Adam Shostack
President, Shostack & Associates

Tarah Wheeler
CEO, Red Queen Technologies
Cybersecurity Fellow, Harvard Belfer Center

Chris Valasek
Director of Product Security, Cruise Automation

Peiter "Mudge" Zatko
Chairman of the Board, Cyber Independent Testing Lab

Sarah Zatko
Chief Scientist, Cyber Independent Testing Lab

STATEMENT OF ISSUES

1. Whether the district court correctly held that independent, permissionless security research serves the public interest and is thus a non-infringing fair use of copyrighted software; and
2. Whether the district court erred in considering good faith and fair dealing in its fair use analysis.

SUMMARY OF ARGUMENT

The stakes of this case extend well beyond the corporate interests of the parties. The fair use at issue here—copying for purposes of independent testing—serves the public interest in security, innovation, and competition. When vulnerabilities go undetected, they go unfixed, and malicious actors can exploit them to inflict financial, emotional, and even physical injury. Security experts have long recognized that disclosure, not secrecy, is the best way to prevent these harms. By testing the architecture of popular software, researchers help software companies identify and neutralize vulnerabilities—while also adding a dose of innovation and competitive pressure.

Too often, however, companies try to muzzle security researchers with legal threats. Without meaningful protection from such claims, organizations like Corellium cannot develop research tools, researchers cannot conduct independent testing, and the public loses out on the benefits of security, innovation, and competition.

The doctrine of fair use is a crucial part of that protection. Because independent security researchers use copies of software to facilitate understanding, and not to exploit its copyrighted elements or provide a market substitute, their activities do not infringe copyright. *Amici* urge the Court to affirm the district court's holding that Corellium's product constitutes fair use of Apple's iOS. *Amici* further urge that the Court clarify that good faith, or lack thereof, is irrelevant to fair use—especially where the purported bad faith is by third-parties, not the alleged infringer.

ARGUMENT

The world we live in is increasingly mediated by complex technologies, from satellite relays in space to the cell phones in our pockets. Such technologies enable exciting new forms of interaction—and present new risks. Technological vulnerabilities allow malicious actors to target personal devices, voting booths, automobiles, even bodily privacy.[2] Apple's products, which are among the most popular in the world, are no exception.[3]

Independent testing helps mitigate the danger of security flaws, and often also supports innovation and competiton. Undermining those benefits does not serve the purpose of copyright or the public interest. Accordingly, *amici* respectfully urge the Court to affirm the district court's finding of fair use.

I. INDEPENDENT TESTING SERVES THE PUBLIC INTEREST BY PROMOTING SECURITY, INNOVATION, AND COMPETITION

Independent testing, conducted free from the influence of software companies, is an essential element of the software development industry. Independent researchers have discovered flaws in systems ranging from Apple's

[2] Kari Paul, *How Your Heart Rate Monitor Could Help Criminals*, MARKETWATCH (Sept. 17, 2019), https://www.marketwatch.com/story/how-your-heart-rate-monitor-could-help-criminals-2017-09-18 [https://perma.cc/4K63-DTYC].

[3] Nicole Perlroth, *Apple Issues Emergency Security Updates to Close a Spyware Flaw*, NEW YORK TIMES (Oct. 15, 2021), https://www.nytimes.com/2021/09/13/technology/apple-software-update-spyware-nso-group.html [https://perma.cc/F7TX-33H8].

iMessage[4] to automobiles[5]—flaws that could inflict serious harm on end users if exploited by malicious actors. To prevent this, independent researchers have developed procedures for safely disclosing such flaws, allowing first-party developers to fix them before they can be exploited. Moreover, the same testing methods that enable disclosure of security vulnerabilities also promote innovation and competition through processes such as adversarial interoperability and independent repair. Allowing companies to quash independent research, as Apple seeks to do here, would deprive the public of an increasingly vital service.

A. Independent Testing Improves Security by Enabling Discovery and Disclosure of Software Flaws

Though they have enriched our personal lives, streamlined our professional work, and connected us with our communities, ever-expanding device capabilities

[4] Bill Marczak et al., *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, CITIZENLAB (Sept. 13, 2021), https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/ [https://perma.cc/N462-DHXZ].

[5] Thomas Brewster, *Watch a Tesla Have Its Doors Hacked Open by a Drone*, FORBES (Apr. 29, 2021), https://www.forbes.com/sites/thomasbrewster/2021/04/29/watch-a-tesla-have-its-doors-hacked-open-by-a-drone [https://perma.cc/37HD-6Y2L].

also come with significant privacy and economic risks. Data breaches alone are projected to cost $10.5 trillion a year by 2025.[6]

The best way to limit those harms is to detect vulnerabilities before they can be exploited—but this is no easy feat. In 2020 alone, more than 18,000 vulnerabilities were logged in the U.S. National Vulnerability Database.[7] At this scale, security requires widespread, independent testing. That's why the National Institute of Standards and Technology has warned that "system security should not depend on the secrecy of the implementation or its components" and has recommended "open design."[8] As one security expert notes, "[p]ublic scrutiny is the only reliable way to improve security, while secrecy only makes us less secure."[9]

Further, security researchers must be free not only to test software, but to disclose their findings. Disclosure of security flaws is, in essence, constructive

[6] PIA Research Team, *Hacking the World – Part 4: The Cost and Future of Hacking (Plus: Safety Tips)*, PRIVATE INTERNET ACCESS (Oct. 25, 2021), https://www.privateinternetaccess.com/blog/hacking-the-world-part-4-the-cost-and-future-of-hacking-plus-safety-tips/ [https://perma.cc/ARQ7-U944].

[7] Redscan, *NIST Security Vulnerability Trends in 2020: An Analysis* 4 (2021), https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf [https://perma.cc/TDR6-TKBP].

[8] Karen Scarfone et al., Nat'l Inst. Standards and Tech., Special Pub. 800-123, *Guide to Central Server Security* 2-4 (July 2008), http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf [https://perma.cc/XEA5-JALY].

[9] Bruce Schneier, *Schneier: Full Disclosure of Security Vulnerabilities is a 'Damned Good Idea'*, SCHNEIER ON SECURITY (Jan. 2007), https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html [https://perma.cc/M2LQ-7DCG].

criticism. Disclosure allows developers of affected software to implement fixes, empowers other developers to avoid similar problems in their own software, and informs users that they should update their software or switch products.

Disclosure can happen in a number of ways, including "coordinated discosure." Researchers following coordinated disclosure practices will give the original developer notice of the problem and an opportunity to fix it prior to notifying the public.[10] Notice to the public may occur after, or in lieu of, coordinated disclosure, through informal means such as chatrooms[11] or mailing lists,[12] or as a well-orchestrated campaign with branding, a logo, and a professional-quality website, as in the case of the Heartbleed bug.[13]

Testing and disclosure has revealed vulnerabilities that threaten our privacy, our democratic processes, and even our lives. Flaws discovered through independent testing include vulnerabilities in Zoom that enabled hackers to take over an Apple

[10] Alana Maurushat, DISCLOSURE OF SECURITY VULNERABILITES: LEGAL AND ETHICAL ISSUES 52 (Springer 2013); Andrew J. Stewart, A VULNERABLE SYSTEM: THE HISTORY OF INFORMATION SECURITY IN THE COMPUTER AGE 137 (Cornell University Press 2021).

[11] Maurushat, *supra* note 10, at 26.

[12] Catalin Cimpanu, *Iconic BugTraq Security Mailing List Shuts Down After 27 Years*, ZDNET (January 15, 2021), https://www.zdnet.com/article/iconic-bugtraq-security-mailing-list-shuts-down-after-27-years [https://perma.cc/EU7C-VKFK].

[13] The Heartbleed Bug (June 3, 2020), https://heartbleed.com [https://perma.cc/3MAW-SSFA].

computer's microphone and camera;[14] in a voting app that was used in the 2018 midterm elections in West Virginia;[15] and in automobile software that allowed hackers to control in-car systems remotely.[16] Just a few months ago, researchers uncovered a "zero-click zero day" attack that allowed state actors to silently take over an iPhone without the owner's input or knowledge,[17] leading Apple itself to sue the company behind the hack.[18] These are but a few examples of the security flaws that independent researchers regularly discover and disclose to safeguard the devices on we which increasingly depend. Recognizing the vital role that disclosure plays in

[14] Kate O'Flaherty, *Zoom Users Beware: Here's How a Flaw Allows Attackers to Take Over Your Mac Microphone and Webcam*, FORBES (Apr. 1, 2020), https://www.forbes.com/sites/kateoflahertyuk/2020/04/01/zoom-users-beware-heres-how-a-flaw-allows-attackers-to-take-over-your-mac-microphone-and-webcam/ [https://perma.cc/4NUL-L7WA].

[15] Abby Abazorius, *MIT Researchers Identify Security Vulnerabilities in Voting App*, MIT NEWS (Feb. 13, 2020), https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213 [https://perma.cc/4MU6-S7LJ].

[16] *Nissan Leaf Can be Hacked via Mobile App and Web Browser*, TREND MICRO (Feb. 26, 2016), https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/nissan-leaf-can-be-hacked-via-mobile-app-and-web-browser [https://perma.cc/A4NC-U5AJ].

[17] *Forced Entry: NSO Group Spies Secretly Seized Control of Apple Devices by Exploiting Flaw in Code*, DEMOCRACY NOW! (Sept. 15, 2021), https://www.democracynow.org/2021/9/15/apple_pegasus_spyware_emergency_security_update [https://perma.cc/7QLK-7CH6]. A zero-day exploit is a security vulnerability that is identified by a third party before the developer has the opportunity to fix it.

[18] *Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware*, APPLE (Nov. 23, 2021), https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/ [https://perma.cc/V353-S4CS].

software security, the U.S. government requires agencies to implement policies allowing the public to report vulnerabilities in agency systems.[19]

B. Independent Testing Promotes Innovation and Competition Through Interoperability

In addition to improving software security, permissionless testing of copyrighted software drives innovation and reduces anticompetitive conduct. Many of the technologies that are interwoven into our lives today, including Apple's own software, have their origins in products that were created to interact with, enhance, and challenge the dominant technologies of their time. This process, called "adversarial interoperability," often depends on permissionless research.

One example of this dynamic is the Unix operating system. Invented at AT&T Bell Labs in the early 1970s, Unix could not be commercialized because the company entered a consent decree in an earlier antitrust case.[20] Nonetheless, a community of developers *outside* AT&T began to contribute improvements and adapt Unix to different systems.[21] The resulting adaptations created a lineage of

[19] Department of Homeland Security, *Binding Operational Direction 20-01* (2020), https://cyber.dhs.gov/assets/report/bod-20-01.pdf [https://perma.cc/PR69-7SU8].

[20] Warren Toomey, *The Strange Birth and Long Life of Unix*, IEEE SPECTRUM (Nov. 28, 2011), https://spectrum.ieee.org/the-strange-birth-and-long-life-of-unix [https://perma.cc/7M82-Z9C4].

[21] *Id.*

operating systems that run everything from supercomputers to smartphones, all incorporating many of the innovations from the original Unix system.[22]

Another example involves Apple itself. In the early 2000s, Microsoft's Office suite dominated the market.[23] The versions Microsoft provided for Apple computers were not interoperable with files created on Microsoft's own Windows operating system, allowing Microsoft control the operating system market.[24] Apple responded by reverse-engineering the Office software—without permission—and developing applications to read and write documents in Microsoft's proprietary file formats. This undermined Microsoft's software-operating system lockdown, allowing Apple to remain competitive and go on to become the world's most valuable company.[25]

The value of adversarial interoperability is not limited to new products. Independent research is also necessary for consumers to get the most out products they already own. The Federal Trade Commission has noted that "manufacturers—in particular mobile phone and car manufacturers—may limit repairs by consumers and repair shops, and . . . those limitations may increase costs, limit choice, and

[22] *Id.*
[23] Cory Doctorow, *Adversarial Interoperability: Reviving an Elegant Weapon From a More Civilized Age to Slay Today's Monopolies*, EFF (June 7, 2019), https://www.eff.org/deeplinks/2019/06/adversarial-interoperability-reviving-elegant-weapon-more-civilized-age-slay [https://perma.cc/7ZXX-48Q2].
[24] *Id.*
[25] *Id.*

impact consumers' rights."[26] One way companies limit consumer choice is by failing to disclose the operation of embedded software. For example, farmers often need to wait days for simple repairs of their John Deere tractors because of inaccessible diagnostic software.[27] In other cases, manufacturers have tried to lock third-party developers out of making cheaper components for existing products.[28] Sometimes, proprietary software is required just for consumers to enjoy their lawfully-purchased products.[29] In these situations, interoperability, founded on permissionless testing, is necessary to prevent manufacturers from restricting after-market uses of their products. Adversarial interoperability allows end users to create the diagnostic tools

[26] Federal Trade Commission, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* 3 (2021), https://www.ftc.gov/system/files/documents/reports/nixing-fix-ftc-report-congress-repair-restrictions/nixing_the_fix_report_final_5521_630pm-508_002.pdf [https://perma.cc/3F4W-QAPJ].

[27] Uri Berliner, *Standoff Between Farmers and Tractor Makers Intensifies Over Repair Issues*, NPR (May 26, 2021), https://www.npr.org/2021/05/26/1000400896/standoff-between-farmers-and-tractor-makers-intensifies-over-repair-issues [https://perma.cc/4C2V-FESB].

[28] Josh Dzieza, *Keurig's Attempt to 'DRM' Its Coffee Cups Totally Backfired*, THE VERGE (Feb. 5, 2015), https://www.theverge.com/2015/2/5/7986327/keurigs-attempt-to-drm-its-coffee-cups-totally-backfired [https://perma.cc/GK8J-QVTP].

[29] Will Nelson, *Denuvo DRM Issues May Be Cause of PC Games Going Down This Weekend*, NME (Nov. 8, 2021), https://www.nme.com/news/gaming-news/denuvo-drm-issues-may-be-cause-for-pc-titles-going-down-over-the-weekend-3090059 [https://perma.cc/CLU3-4E3S].

needed to repair their vehicles,[30] refill their printers,[31] and access their video games.[32]

The Ninth Circuit has recognized the value of adversarial interoperability in inhibiting anticompetitive behavior and spurring innovation. In *Sega Enterprises Ltd. v. Accolade, Inc.*, the Ninth Circuit explained that Accolade's unsanctioned research into the functional aspects of Sega's video game software was "precisely [the] growth in creative expression . . . that the Copyright Act was intended to promote." 977 F.2d 1510, 1522–23 (9th Cir. 1992). The Court reaffirmed this reasoning in *Sony Computer Ent., Inc. v. Connectix Corp.*, validating Connectix's copying of the PlayStation's basic input-output system to construct an emulator—a "legitimate competitor" of the original console. 203 F.3d 596, 606–08 (9th Cir. 2000). These cases and others teach that adversarial interoperability is beneficial—but only if it remains a legally protected process. *See, e.g.*, *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1203-04 (2021) (summarizing "numerous ways" in

[30] U.S. Copyright Office, *Software-Enabled Consumer Products* (Dec. 2016), https://www.copyright.gov/policy/software/software-full-report.pdf [https://perma.cc/WP74-RZMV].

[31] Adam Liptak and Vindu Goel, *Supreme Court Rules Patent Laws Can't Be Used to Prevent Reselling*, NEW YORK TIMES (May 30, 2017), https://www.nytimes.com/2017/05/30/business/supreme-court-patent-rights-lexmark.html [https://perma.cc/39HT-8H6F].

[32] Benjamin Burns, *Back From The Dead: The People Keeping Old MMOs Alive*, GAMESINDUSTRY.BIZ (Nov. 2, 2018), https://www.gamesindustry.biz/articles/2018-11-02-the-people-keeping-old-mmos-alive [https://perma.cc/ME82-EA6U].

which interoperability promotes growth and limits anti-competitive behavior); *Computer Assocs. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 711–23 (2d Cir. 1992) (noting the "corrosive effects" of anti-competitive threats to interoperability).

II. FIRST-PARTY TESTING ALONE CANNOT PROVIDE THE BENEFITS OF INDEPENDENT, PERMISSIONLESS RESEARCH

The benefits to security, innovation, and competition described above require independent research. Independent researchers have incentives to find and disclose software gaps that are not necessarily shared by software companies, and thereby play a crucial corrective role. Without researchers holding them accountable, companies may be unable or unwilling to address vulnerabilities, and even less willing to disclose them to the public.[33] Too often, however, software companies see outside security research as unwanted publicity, and try to quash it with legal threats. These threats have chilled security researchers, to the detriment of the public.

A. Companies Lack Incentives to Fully Test and Report on Vulnerabilities

Companies generally hold their products out as safe, but fear of responsibility presents a perverse incentive to avoid the very testing from which they, and the public at large, would benefit. Companies may suffer commercial and reputational

[33] Reed Albergotti, *Apple Pays Hackers Six Figures to Find Bugs in its Software. Then it Sits on Their Findings.*, WASHINGTON POST (Sept. 9, 2021), https://www.washingtonpost.com/technology/2021/09/09/apple-bug-bounty/ [https://perma.cc/F39T-N5VC].

costs when security vulnerabilities are disclosed to their customers.[34] Moreover, many companies that produce "smart" devices do not specialize in software and may have other priorities that lead them to rush products to market, leaving vulnerable customers high and dry.[35] And when companies do acknowledge vulnerabilities, they do not always remedy them responsibly, leading to "the absurdity of vendors creating the vulnerable software that put its paying customers at risk while . . . creating the circumstance that adds additional risk."[36]

Some companies, like Apple, try to address the problem of vulnerabilities in part through "bug bounty" programs.[37] Under these programs, companies will pay security researchers for flagging security flaws, typically in exchange for a certain degree of confidentiality, e.g., until the bug has been fixed. Indeed, Apple offers up

[34] Keman Huang et al., *Is Third-Party Software Leaving You Vulnerable to Cyberattacks?*, HARVARD BUSINESS REVIEW (May 13, 2021), https://hbr.org/2021/05/is-third-party-software-leaving-you-vulnerable-to-cyberattacks [https://perma.cc/MQA6-YDLU].

[35] *Id.*

[36] Jonathan Greig, *Microsoft, Oracle, and Google Top List of Companies With Most Vulnerabilities Disclosed In Q2*, TECHREPUBLIC (Aug. 31, 2020), https://www.techrepublic.com/article/microsoft-oracle-and-google-top-list-of-companies-with-most-vulnerabilities-disclosed-in-q2/ [https://perma.cc/ZN3C-8S8G].

[37] *Apple Security Bounty*, Apple, https://developer.apple.com/security-bounty/ [https://perma.cc/KK2B-GJKM].

to $1 million for certain types of vulnerabilities that are reported, indicating how valuable these reports can be.[38]

However, bug bounty programs are only effective when the company responds with alacrity. Interviews with dozens of security researchers revealed that, compared with its rivals, Apple often fails to fix reported bugs quickly, or sometimes at all.[39] As one security researcher recently wrote,

> I want to share my frustrating experience participating in Apple Security Bounty program. I've reported four 0-day vulnerabilities this year between March 10 and May 4, as of now three of them are still present in the latest iOS version (15.0) and one was fixed in 14.7, but Apple decided to cover it up and not list it on the security content page. When I confronted them, they apologized, assured me it happened due to a processing issue and promised to list it on the security content page of the next update. There were three releases since then and they broke their promise each time.[40]

Moreover, even well-run bug bounty programs still leave companies in control of vital information about their own products.[41] The same is true of programs that

[38] *Id.*

[39] *See* Albergotti, *supra* note 33.

[40] *Disclosure of Three 0-Day IOs Vulnerabilities and Critique Of Apple Security Bounty Program*, HABR (Sept. 23, 2021), https://habr.com/en/post/579714 [https://perma.cc/58MX-QD4U].

[41] J.M. Porup, *Bug Bounty Platforms Buy Researcher Silence, Violate Labor Laws, Critics Say*, CSO (Apr. 2, 2020), https://www.csoonline.com/article/3535888/bug-bounty-platforms-buy-researcher-silence-violate-labor-laws-critics-say.html [https://perma.cc/L8KT-SN27].

require researchers to purchase approved "research devices" with numerous strings attached.[42]

Any self-interested company would likely prefer to be informed privately of security flaws rather than having to respond to public reports. However, allowing first-party developers to control third-party testing and reporting means companies can deal with vulnerabilities if and when it suits them. Independent research provides an essential check by ensuring that vulnerabilities are in fact addressed, regardless of the developer's private interests.

B. Companies Use Legal Threats to Inhibit Independent Testing and Interoperability

Because some companies perceive security research as harmful to their interests, independent security researchers are often forced to work without the explicit permission of the companies whose creations they are helping to improve.[43] Not surprisingly, companies regularly threaten legal action against such researchers.[44] Common claims include unlawful access under the Computer Fraud

[42] *Apple Security Research Device Program*, Apple, https://developer.apple.com/programs/security-research-device/ [https://perma.cc/N9P6-JWJM].
[43] *See* Pamela Samuelson, *Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 545 (1999).
[44] See *Research Threats: Legal Threats Against Security Researchers*, disclose.io, https://github.com/disclose/research-threats [https://perma.cc/5EXC-UEA9].

and Abuse Act ("CFAA"), technical circumvention under the Digital Millennium Copyright Act ("DMCA"), or, as in this case, copyright infringement.[45]

For example, when one researcher found that a dental practice management program was exposing patients' information, he disclosed the vulnerability and the company fixed it.[46] But when he took the customary next step of announcing the breach publicly, the company reported him for criminal violation of the CFAA, resulting in a dawn FBI raid on his house where he was held at gunpoint and handcuffed.[47]

These kinds of threats have real consequences for the public when "white-hat hackers and security researchers hesitate to report vulnerabilities and weaknesses to technology firms for fear of facing legal retribution."[48] Security researchers who have used Corellium's tools in particular have "expressed fear of retribution from

[45] *See* Sunoo Park and Kendra Albert, Berkman Klein Center for Internet & Society and Electronic Frontier Foundation, *A Researcher's Guide to Some Legal Risks of Security Research* 7 (2020), https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf [https://perma.cc/C88T-HY66].

[46] Dissent Doe, *FBI Raids Dental Software Researcher Who Discovered Private Patient Data on Public Server*, Daily Dot (May 27, 2016), https://www.dailydot.com/debug/justin-shafer-fbi-raid/ [https://perma.cc/K5B4-5UFP].

[47] *Id.*

[48] Zack Whittaker, *Lawsuits Threaten Infosec Research—Just When We Need It Most*, ZDNet (Feb. 19, 2018), https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/ [https://perma.cc/T8WC-KQGN]

Apple."[49] The concern over legal action is so great that security researchers track threats issued in relation to their work in a collaborative database—including this very lawsuit.[50] Attention to such risks also distracts from valuable work and deters new researchers from entering the field.

The problem extends beyond security research. Apple itself has claimed that removing content controls from an iPhone, which can be a necessary part of repairing it, infringes copyright,[51] and other companies have used legal threats to shut down fan servers for defunct games.[52] Uncertainty surrounding the standards for interoperable software also prevents newcomers from entering the market because investors are disincentivized by the expense of protracted litigation over intellectual property rights.[53]

[49] Lorenzo Franceschi-Bicchierai, *Apple's Copyright Lawsuit Has Created a 'Chilling Effect' on Security Research*, VICE (May 5, 2020), https://www.vice.com/en/article/wxqee4/apple-copyright-lawsuit-corellium-chilling-effect-security-research [https://perma.cc/X8YL-FKXL].

[50] *Research Threats*, *supra* note 44.

[51] Fred von Lohman, *Apple Says iPhone Jailbreaking is Illegal*, EFF (Feb. 12, 2009), https://www.eff.org/deeplinks/2009/02/apple-says-jailbreaking-illegal [https://perma.cc/6P3L-GUCG].

[52] Justin Olivetti, *Asheron's Call Emulator Lead Explains What Went Down With the Cease-and-Desist*, MASSIVELY OVERPOWERED (Sept. 18, 2017), https://massivelyop.com/2017/09/18/asherons-call-emulator-lead-explains-what-went-down-with-the-cease-and-desist/ [https://perma.cc/9RUZ-MB3K].

[53] *See* Michael A. Carrier, *Copyright and Innovation: The Untold Story*, 2012 WIS. L. REV. 891 (2012) (discussing the debilitating effects of copyright litigation on

III. SECURITY RESEARCH IS A CLASSIC AND ESSENTIAL FAIR USE

For the reasons stated above, independent researchers need assurance that their work can continue without constant threats of litigation, including claims of copyright infringement. Fair use is the obvious recourse; as judges and commenters have noted, one purpose of fair use is "precisely to make possible a use that generally cannot be bought." *Fisher v. Dees*, 794 F. 2d 432, 437 (9th Cir. 1986). Affirming the district court's decision will send a message to the security research community that fair use protects their crucial activities.

A. All Four Fair Use Factors Weigh In Favor of Permissionless Security Research

i. Purpose and Character of the Use

The "central purpose" of the first factor is to determine whether or not the use in question "merely supersedes the objects of the original creation" or is instead transformative. *Campbell v. Acuff Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (internal quotations omitted). Research, criticism, comment, and scholarship are all classic fair use purposes. 17 U.S.C. § 107. Precedent in this Circuit and others

innovators and investors); Mark A. Lemley and R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1388 (2004) (pointing to evidence that threats of litigation deter innovation in software development, particularly surrounding encryption and other sensitive areas).

specifically addresses research into functional aspects of software, confirming that copying software for the purpose of examination, interoperability, and extension are fair uses. *See Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1547 (11th Cir. 1996) (holding that external "considerations such as compatibility may negate a finding of infringement"); *Accolade*, 977 F.2d at 1522–23; *Connectix*, 203 F.3d at 608; *see also Oracle*, 141 S.Ct. at 1203 (holding that Google's purpose to "expand the use and usefulness of [its] smartphones" weighed in favor of fair use).

Security research like that enabled by Corellium also increases public access to information, a legitimate, socially-beneficial purpose that supports a finding of fair use. *See Perfect 10, Inc. v. Amazon.com, Inc*., 508 F.3d 1146, 1166 (9th Cir. 2007) (holding that "transformative nature of [image] search engine, particularly in light of its public benefit," supported finding of fair use); *Kelly v. Arriba Soft Corp*., 336 F.3d 811, 820 (9th Cir. 2002) (holding that first factor weighs in favor of fair use where copying "benefit[s] the public by enhancing information-gathering techniques on the Internet"); *Authors Guild, Inc. v. Google, Inc*., 954 F. Supp. 2d 282, 291, 293 (S.D.N.Y. 2013) (finding transformative use where digitization "transformed book text into data . . . opening up new fields of research" and providing "significant public benefit").

Finally, security researchers may evaluate the quality of software security, offering constructive criticism—or commendations, if their review did not reveal any vulnerabilities. These are entirely different purposes from those of the copyright owner; subjecting itself to public criticism is hardly one of the purposes Apple had in mind for iOS.

ii. Nature of the Copyrighted Work

The second factor weighs in favor of fair use where, as here, copying "protected, expressive aspects" of code is a necessary step in "gain[ing] access to the unprotected ideas and functional concepts." *Accolade*, 977 F.2d at 1525. As the Ninth Circuit has observed, some copying of copyrightable elements of code is necessary to prevent copyright owners from gaining a "de facto monopoly over the functional aspects of [their] work." *Id.* at 1526. Security research is similarly aimed at the functional aspects of computer code; any copying of protected expression is incidental.

iii. Amount and Substantiality of the Portion Used

The third fair use factor examines the amount of the copyrighted work used to determine whether the "quantity and value of the materials used are reasonable in relation to the purpose of the copying." *Campbell*, 510 U.S. at 586-87. Where, as here, copying an entire work is necessary to accomplish the transformative purpose, the third factor will not weigh against fair use. *Accolade*, 977 F.2d at 1526; *Connectix*, 203 F.3d at 606.

In search engine cases, for example, courts have found that that copying an entire work was necessary and fair where anything less would defeat the transformative purpose of enhancing access to knowledge. *See Kelly*, 336 F.3d at 820-21 (holding that third factor was neutral, where copying less than entire work would reduce usefulness); *Perfect 10*, 508 F.3d at 1165 (same); *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014) (holding that third factor favored fair use, where libraries copied entire books for full-text search). Security research likewise requires the use of the entire work because flaws may be found anywhere in the code—anything less would risk vulnerabilities going undetected. Accordingly, the third factor is, at worst, neutral in this case.

iv. Market for the Copyrighted Work

The fourth factor examines harms to the market for the copyrighted work. *Campbell*, 510 U.S. at 590. Copyright is designed to encourage the origination and dissemination of creative works, and "a use that has no demonstrable effect upon the potential market for, or the value of, the copyrighted work need not be prohibited in order to protect the author's incentive to create." *Sony Corp. of Am. v. Universal City Studios, Inc.*,464 U.S. 417, 450 (1984). Corellium, which offers ARM processor virtualization products and services,[54] does not compete with Apple's iPhone or iOS. Certainly, no consumer would use Corellium's product instead of buying an iPhone with iOS—it cannot be used on a mobile device, which makes it useless as an operating system on Apple phones.

Apple nevertheless claims Corellium's product is in "competition with iOS" because "through its Security Research Device Program, Apple licenses iOS installed on customized iPhones." Appellant's Br. 50–51. As an initial matter, this is not technically accurate. Corellium's product gives researchers more research tools than a physical device, while also avoiding the costly and wasteful prospect of "bricking" multiple iPhones during a research project. *See* App'x of Appellant at 64-5. More significantly, Apple's program is highly restrictive. For example, when a researcher reports a vulnerability, Apple sets a publication date—and until that date, the researcher is contractually barred from discussing the bug with others.[55] Thus, the Security Research Device Program serves a market of researchers who are willing to comply with Apple's demands. Corellium serves a different market: independent security researchers who want to evaluate and constructively criticize

[54] ARM is a company that produces a type of processor architecture that is typically used in mobile computing products such as mobile phones. This is in contrast to the x86 processor architecture typically used by Intel and AMD processors on desktop computers.

[55] *See Apple Security Research Device Program*, *supra* note 42.

iOS's security without being subject to restrictions about when and to whom they may speak. Corellium's product and an iPhone are simply not interchangeable; each has a different purpose and set of functions that the other does not offer.

While the market for the iPhone is not perfectly commensurate with the licensing market at issue here, it's worth noting that, if anything, Corellium's product actually *enhances* the market for the iPhone by helping to ensure that consumers are getting a safest product possible. Independent security research efforts have led to the discovery of several zero-day exploits that were reported to Apple and subsequently fixed, including in the iOS software update released in October.[56] In September, one iOS vulnerability discovered by a cybersecurity research group was so severe that it prompted Apple to issue an emergency software update to iPhone users.[57] Apple has long traded on its reputation as a security-minded company.[58] If vulnerabilities like these were left open to exploitation, consumers might well choose alternative products.

[56] Michael Kan, *Apple Patches New Zero-Day iOS Vulnerability Possibly Under Exploitation*, PCMAG (Oct. 11, 2021), https://www.pcmag.com/news/apple-patches-new-zero-day-ios-vulnerability-possibly-under-exploitation [https://perma.cc/S4A7-EA5K].

[57] *See* Perlroth, *supra* note 3.

[58] See Bree Fowler, *Apple, Long a Champion of Consumer Privacy, Now Sits at a Crossroads*, CNET (Sept. 21, 2021), https://www.cnet.com/tech/apple-long-a-champion-of-consumer-privacy-and-security-now-sits-at-a-crossroads/ [https://perma.cc/4GSH-FEK6].

v. *Weighing the Factors Together*

Earlier this year, in *Google v. Oracle*, the Supreme Court held that Google's use of Oracle's code was fair because it enabled programmers to generate new expression with minimal market harm. 141 S. Ct. at 1201-08. The Court emphasized the need to consider of public benefits of the anticipated uses—and the harms of letting one company preempt those uses. *Id.* at 1206-08. Enabling and engaging in security research promotes both public safety and the creation and dissemination of new knowledge, advancing the purposes of copyright law without undermining the incentive to create. Just as the Supreme Court in *Google v. Oracle* concluded that Google's copying was fair when it created a platform for subsequent creativity and innovation, 141 S.Ct. 1183, this Court should find that Corellium's platform for security research is a fair use of Apple code.

B. Good Faith Is Irrelevant to the Fair Use Analysis

For the above reasons, *amici* respectfully ask the Court to affirm the district court's overall fair use holding. However, we also urge that the Court to reject the district court's improper invocation of good faith in its fair use analysis. The doctrine of fair use was developed to support the core purpose of copyright: promoting creation of useful new works. While tangible public benefit is relevant to this inquiry, a secondary user's good faith, or lack thereof, is not.[59]

Determining whether a given use is "fair" in the copyright context does not require an assessment of the parties' intentions. Rather, it weighs the predicted impact of competing social goods: the incentivizing function of copyright on one hand and the need for innovation, competition, and critique on the other. These are utilitarian inquiries, concerned with concrete, measurable impacts—not the sanctity of the creative purpose. Just as "'[c]opyright is not a privilege reserved for the well-behaved,'" *Oracle*, 141 S. Ct. at 1204 (quoting Pierre N. Leval, *Toward A Fair Use Standard*, 103 Harv. L. Rev. 1105, 1126 (1990)), fair use is not barred to those motivated by profit, reputation, or even personal animus, *Caner v. Autry*, 16 F. Supp. 3d 689, 712 (W.D. Va. 2014) (noting that if "dislike or distrust of the object of [] criticism" were a factor, "fair use would offer little protection, and the analysis would delve courts into a complex and highly subjective inquiry about the motivations and relationships between parties"). Small wonder that the Supreme Court recently noted that its decision in *Campbell* "expressed some skepticism about whether bad faith has any role in a fair use analysis," and found that skepticism to be "justifiable." *Oracle*, 141 S. Ct. at 1204.

[59] Simon J. Frankel and Matt Kellogg, *Bad Faith and Fair Use*, 60 J. COPYRIGHT SOC'Y U.S.A. 1, 3 (2012).

In any event, it is clear that good faith is irrelevant here. Apple alleges improper conduct because Corellium "fail[s] to guard against abuses of its product." Appellant's Brief at 30 n.4. But Apple's allegations pertain to Corellium's hypothetical users, not Corellium itself. When courts have considered bad faith in fair use, the bad faith in question pertains to the actual behavior of the defendant, *not* to potential future behavior by third parties. Specifically, the kinds of bad faith courts analyze in fair use fall into three categories: (1) "whether the defendant's access to the copyrighted work was proper"; (2) whether "the defendant failed to seek permission before using the [] work"; and (3) "the propriety of the use itself," such as lack of attribution or a misleading portrayal of the original work.[60] In all of these categories, the relevant conduct is by the defendant, not by users of the defendant's work. In other words, there is no doctrine of "secondary bad faith."

Apple may be concerned that bad actors will exploit vulnerabilities in iOS, or that researchers may not disclose to Apple the vulnerabilities they find. Corellium shares those concerns and has created a tool to help make iOS more secure. However, Corellium's good faith is not implicated by the uses to which others put its product, just as Apple does not act in bad faith when consumers use Apple devices to infringe the copyright of third-party creators.

[60] *Id.* at 23-24.

CONCLUSION

For the foregoing reasons, *amici* respectfully urge this Court to (1) affirm the district court's holding that Corellium's product constitutes a fair use of Apple's iOS and (2) reject good faith and fair dealing as part of the fair use analysis.[61]

Dated: February 16, 2022

Respectfully submitted,

/s/ Alejandra Caraballo

Alejandra Caraballo
Counsel of Record
HARVARD CYBERLAW CLINIC
Harvard Law School
1585 Massachusetts Ave Ste. 5018
Cambridge, MA 02138
Tel: (617) 384-8511
Email: acaraballo@law.harvard.edu

Corynne McSherry
John Bergmayer
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Email: corynne@eff.org

Counsel for Amicus Curiae

[61] Amicus curiae thanks Fall 2021 Cyberlaw Clinic students Karen Gover and Sibo Wang for their valuable contributions to this brief.

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitations of Fed. R. App. P. 32(a)(7)(B) because it contains 5683 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14 point Times New Roman.

Dated: February 16, 2022

Respectfully submitted,

/s/ Alejandra Caraballo

Alejandra Caraballo
Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I hereby certify, that on February 16, 2022, I electronically filed the foregoing Brief of Amicus Curiae Electronic Frontier Foundation was filed with the Clerk of the Court for the Eleventh Circuit Court of Appeals, using the CM/ECF system,

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: February 16, 2022

Respectfully submitted,

/s/ Alejandra Caraballo

Alejandra Caraballo
Counsel for Amicus Curiae