Apple targets jailbreaking in lawsuit against iOS virtualization company

Enlarge / An image from Apple’s lawsuit shows a real iPhone X and Corellium’s service running a virtual iPhone X.

reader comments

48 with 33 posters participating

Share this story

Apple has expanded a lawsuit against an iOS virtualization company, claiming that its actions facilitate jailbreaking and violate the Digital Millennium Copyright Act (DMCA) prohibition on circumvention of copyright-protection systems.

Apple sued Corellium, a company that sells access to virtual machines that run copies of the operating system used in iPhones and iPads, in August 2019. We detailed the initial allegations in a previous article; Apple said that Corellium sells “perfect replicas” of iOS without a license from Apple and markets its software as “a research tool for those trying to discover security vulnerabilities and other flaws in Apple’s software.” But instead of aiding good-faith security research, Corellium “encourages its users to sell any discovered information on the open market to the highest bidder,” Apple alleged.

The first version of Apple’s lawsuit accused Corellium of copyright infringement. A new version filed on December 27 alleges both copyright infringement and “unlawful trafficking of a product used to circumvent security measures in violation

of 17 U.S.C. § 1201," a statute that's part of the DMCA. Apple argued that Corellium gives users the ability to jailbreak iOS for either benign or malicious purposes.

Apple "demonizes" jailbreaking, Corellium says

Corellium CEO Amanda Gorton responded to the newly expanded allegations in a blog post, writing that "Apple's latest filing against Corellium should give all security researchers, app developers, and jailbreakers reason to be concerned."

Corellium is "deeply disappointed by Apple's persistent demonization of jailbreaking," with Gorton writing that "developers and researchers rely on jailbreaks to test the security of both their own apps and third-party apps." Apple's filing, according to Corellium, essentially "assert[s] that anyone who provides a tool that allows other people to jailbreak, and anyone who assists in creating such a tool, is violating the DMCA."

Apple, Gorton wrote, "is using this case as a trial balloon in a new angle to crack down on jailbreaking" and "is seeking to set a precedent to eliminate public jailbreaks."

The case is in the US District Court for the Southern District of Florida.

Jailbreaking of smartphones and tablets such as iPhones and iPads is allowed in the US due to a DMCA exemption granted by the US Copyright Office (a division of the Library of Congress).

The Copyright Office says the DMCA exemption for jailbreaking phones and tablets is intended "to allow the device to interoperate with or to remove software applications." There's also a DMCA exemption for security research on all types of devices. But to qualify for the security exemption, it must be

“good-faith security research” that is “carried out in an environment designed to avoid any harm to individuals or the public.”

The Electronic Frontier Foundation describes DMCA exemptions in general as “too narrow and too complex for most technology users.”

Corellium bypasses encryption and hardware checks, Apple says

Apple argues that Corellium’s alleged DMCA violations enable both violations of Apple’s copyright and the spread of security vulnerabilities.

Apple’s updated lawsuit notes that iOS uses “technological protection measures that control access to and protect Apple’s exclusive rights in its software,” such as “measures that prevent iOS and iTunes from being installed onto non-Apple-manufactured hardware.” Apple said iOS also has “software restrictions that prevent unfettered access to the operating system,” for example by “prevent[ing] a user from modifying the operating system.”

Corellium violates Apple’s rights by “enabl[ing] its users to circumvent the security protections that Apple has implemented to protect its copyrighted works and its exclusive rights in those works,” Apple’s updated lawsuit says.

Apple alleges that Corellium’s sale of iOS replicas without Apple’s authorization amounts to “trafficking in technologies, products, or services” designed to bypass or remove technological measures that control access to Apple’s copyrighted works, in violation of Section 1201. Those Apple technological measures “include encryption, hardware checks, and server checks that prevent iOS from being installed and executed on non-Apple-authorized hardware, and prevent

unfettered access to the iOS operating system."

While Apple accused Corellium of facilitating jailbreaking, the alleged jailbreaking is of virtual iOS devices and not physical iPhones and iPads. Apple wrote:

> *The Apple Corellium Product also provides users with the ability to "jailbreak" virtual iOS devices. Jailbreaking refers to the act of modifying iOS to circumvent the software restrictions that prevent unfettered access to the operating system. Corellium openly markets the ability of its technology to "jailbreak… any version" of iOS. Corellium provides its jailbreaking technology to all its customers, regardless of their purpose.*

Apple also said that Corellium's product "makes modifications to iOS that allows it to be installed on, and run from, Corellium-developed or Corellium-operated hardware. Such modifications include disabling loadable firmware validation, disabling self-verification of the FIPS [Federal Information Processing Standard] module, adding Corellium software to the 'trust cache,' and instructing the restore tool not to contact Apple servers for kernel/device tree/firmware signing."

Apple: Corellium doesn't care about security

While Corellium argues that its software helps companies identify iOS bugs for the purpose of improving the product and protecting users, Apple claims that Corellium "makes no effort whatsoever to confine use of its product to good-faith research and testing of iOS."

Apple cited a Motherboard article that describes Azimuth Security as Corellium's first customer. Apple wrote:

> *The Motherboard article reported that Azimuth sells a range*

> *of tools that exploit flaws in software. Azimuth's customers reportedly include foreign governments, including foreign intelligence agencies. And when a reporter recently asked Azimuth's founder Mark Dowd, whether Azimuth had ever reported a bug found using Corellium to Apple, he answered, "no." Contrary to its lofty rhetoric, Corellium in fact sells Apple's technology and the ability to circumvent the security measures embedded in that technology for its own profit, and makes no effort to ensure its customers are engaged solely in good-faith security research.*

iFixit founder Kyle Wiens, who has testified to the US Copyright Office in support of legalized jailbreaking for the purpose of fixing products, wrote yesterday that Apple's complaint is "a dangerous DMCA lawsuit." If Apple wins, "the damage will reverberate beyond the security community and into the world of repair and maintenance," Wiens wrote.

Corellium hasn't filed its response to Apple's expanded complaint in court yet, but the company vowed a strong fight. "We are prepared to strongly defend against this attack, and we look forward to sharing our formal response to this claim when we file it in court," Gorton wrote.

As for the more straightforward copyright allegation that Corellium sells replicas of iOS without a license from Apple, a Corellium response in October claimed that "Apple impliedly, directly, or indirectly, authorized, licensed, consented to, or acquiesced to Corellium's allegedly infringing use of Apple's works." Corellium wrote that Apple was "aware of Corellium's technology for several years" and "encouraged its development."

"During this time, Apple approved of Corellium participating in its invitation-only Security Bounty Program ('bug bounty program') with a promise to pay for software bugs identified by Corellium. While Apple gladly accepted and utilized bugs

submitted by Corellium as part of this program, it broke its promise to pay for them," Corellium wrote. Apple eventually "announced its own competing product and soon after sued Corellium," the response said.

Corellium also claimed it "has made quintessential fair use of Apple's technology."

"Corellium's technology is highly transformative because it does not merely replicate Apple's products for the same purposes for which the products were developed. Instead, Corellium's technology utilizes portions of Apple's technology for entirely distinct purposes, which provide significant societal benefits," Corellium wrote.

Rather than using or replicating iOS, Corellium claimed that it "uses its own proprietary software to facilitate executing iOS on different hardware."

https://arstechnica.com/?p=1638563