UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CASE NO: 9:19-cv-81160-RS

APPLE INC.,

Plaintiff,
v.

CORELLIUM, LLC,
Defendant.

_____/

CORELLIUM'S ANSWER, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS TO APPLE'S SECOND AMENDED COMPLAINT

Defendant, Corellium, LLC ("Corellium" or "Defendant"), by and through its undersigned counsel, files its Answer, Affirmative Defenses, and Counterclaims to Plaintiff, Apple Inc.'s ("Apple" or "Plaintiff") Second Amended Complaint and Demand for Jury Trial:

RELEVANT BACKGROUND

Long before Apple accused Corellium of copyright infringement and violations of the Digital Millennium Copyright Act ("DMCA"), Apple not only encouraged Corellium to continue developing its technology, but went to great lengths to acquire Corellium and its technology. During this time, Apple approved of Corellium participating in its invitation-only Security Bounty Program ("bug bounty program") with an assurance that Apple would pay for software bugs identified by Corellium. While Apple gladly accepted and utilized bugs submitted by Corellium as part of this program, it failed to pay for them. Finally, only after the parties could not agree on an acquisition purchase price, Apple announced its own competing product and soon after sued Corellium. Tellingly, despite its lengthy discussions with Corellium's founders and familiarity

with Corellium's technology, including unrestricted access to Corellium's proprietary information, Apple never hinted that it believed Corellium was infringing its copyrights or violating the DMCA.

Apple's behavior with respect to security research is widely viewed as harmful to the public. By way of example, Apple's behavior toward Corellium exemplifies its desire to exclusively control the manner in which security researchers identify vulnerabilities in, e.g., a mobile device's operating system. This research is extremely important to the public's interest. By requiring that security researchers use its physical development ("dev") devices to the exclusion of other products, including its attempt to stop Corellium from offering a more efficient alternative to its dev devices, Apple is trying to exclusively control (1) how security research is performed, and (2) who is able to perform that research.

The Copyright Act is grounded in the constitutional directive to grant limited protections to the authors of copyrighted material while preserving – not suffocating – innovation. U.S. Const. art. I, § 8, cl. 8. The DMCA is no different. Congress enacted the DMCA for the purpose of preventing *digital piracy*, not to prevent innovators like Corellium from developing cutting-edge tools that benefit the public by empowering developers and researchers to more effectively and efficiently advance the security and stability of iOS devices, applications ("apps"), and services that play an integral part in end users' daily lives.

Corellium's technology is not a trafficking tool; nor does it enable others to pirate copyrighted works. Rather, Corellium's technology enables its users to run publicly available, unencrypted iOS files for the purpose of conducting advanced security research in an environment highly constrained by that purpose. Apple cannot claim that it effectively controls access to iOS

when it makes iOS freely available to the public to download, open, view its object code, and run.[1] With respect to Apple's breach of DMCA allegations, it makes no sense to say that the DMCA's access control provisions apply to otherwise-readily-accessible copyrighted works. Further, use of Corellium's technology fits within the DMCA's exemptions.

In short, this lawsuit is not driven by Apple's genuine belief that Corellium infringes its copyrights or traffics a product in violation of the DMCA, but by Apple's frustration at not being able to make Corellium's technology its own and exclusively control iOS-related security research. Apple's behavior, which spans the course of several years and has culminated in filing this lawsuit, amounts to unfair business practices that must be put to an end by the Court and finds no support in the letter or spirit of federal copyright law.

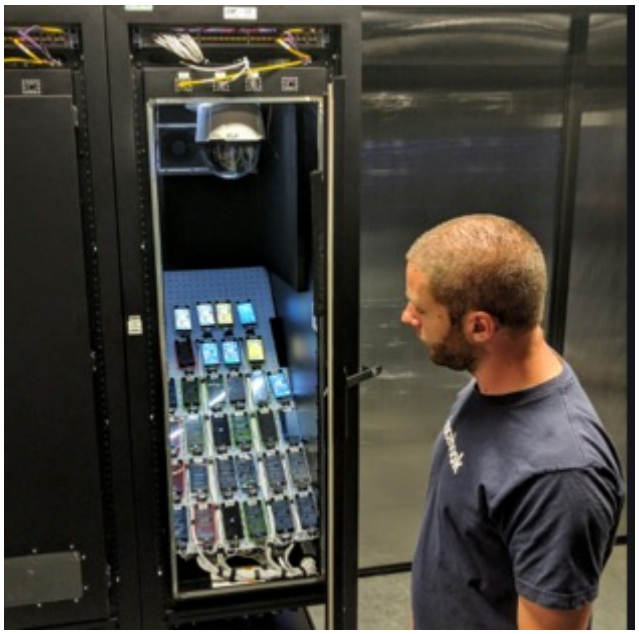
Corellium's Innovative And Transformative Technology Has Transformed Security Research

Apple wanted to purchase Corellium's technology because it is innovative and highly transformative. It virtualizes physical devices, including Apple mobile devices, enabling users to execute various device operating systems in a simple unified environment. By replacing racks of physical devices[2] with a single virtual platform, Corellium empowers software engineers to test, teach, research, and develop more efficiently and more effectively.

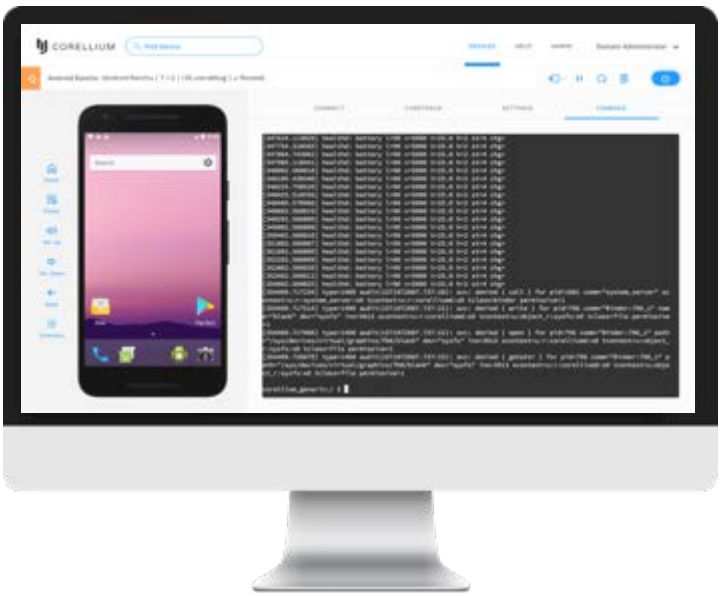
[1] Any person can download the iOS files, or "IPSWs," directly from Apple's servers. Direct download links can be found at https://itunes.com/versions, as well as from various third party sites including, for example, https://ipsw.me, https://www.ipswdownloader.com, and https://www.theiphonewiki.com.

[2] *See, e.g.*, Frederic Lardinois, *Facebook Lifts The Veil On Its Mobile Device Testing Lab*, TECHCRUNCH (July 13, 2016), https://techcrunch.com/2016/07/13/facebook-lifts-the-veil-on-its-mobile-device-lab/ (noting the way in which Facebook tests changes to its smartphone application).

BEFORE CORELLIUM



AFTER CORELLIUM



Corellium's technology provides a substantially more scalable, convenient, and efficient solution than the status quo. For example, using Corellium's technology, security researchers and

developers can quickly search for errors and vulnerabilities ("bugs") in an app or operating system across multiple device models and operating system versions and write programs to automate these tasks. Similarly, if a bug "bricks" a virtual device and renders it unusable, a security researcher can instantly generate a new virtual machine rather than having to obtain a new physical device. This is one of several examples where Corellium's technology is more efficient than the use of physical devices to perform security research.

Corellium's technology is not only more efficient, but also provides new and advanced functionality that is more effective than a physical device. For example, Corellium's technology allows a virtual device to be paused during testing, which gives researchers a detailed look at its state at any given moment.

Given the benefits of Corellium's technology, it is no wonder third-party security experts have endorsed Corellium's technology:

> "Corellium was founded in Florida in 2017, in the last two years it has earned a ***sterling reputation*** among mobile jail breakers and cybersecurity specialists . . . ." [3]
>
> "Its product provides 'virtualized' versions of iOS. For security researchers, such software-only versions of the Apple operating system are ***incredibly valuable***. For instance, it's possible to use Corellium to pause the operating system and analyze what's happening at the code level. ***Some in the industry have called it 'magic,'*** as it should help security researchers uncover vulnerabilities with greater ease and speed than having to work with a commercial iPhone."[4]
>
> "You are obviously all from other planets as there is NO WAY in hell this was made by humans. Alien tech and I for one welcome our new overlords. ***This is magic and truly will change stuff***. The sheer flexibility to virtualise

[3] Conor Reynolds, *Apple Sues Virtualization Firm Corellium for "Perfect Digital Facsimile" of iOS*, COMPUTER BUSINESS REVIEW (Aug. 16, 2019), https://www.cbronline.com/news/apple-sues-corellium (emphasis added).

[4] Thomas Brewster, *Apple Sues Cybersecurity Startup for 'Illegally Replicating' iPhone for iOS*, FORBES (Aug. 15, 2019), https://www.forbes.com/sites/thomasbrewster/2019/08/15/apple-is-suing-a-cybersecurity-startup-for-illegally-replicating-iphones/#7d0ff994522b (emphasis added).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.