UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

R.N. NEHUSHTAN TRUST LTD.,

Plaintiff,

v.

APPLE INC.,

Defendant.

Case No. 22-cv-01832-WHO

**ORDER DENYING MOTION TO DISMISS**

Re: Dkt. No. 28

Defendant Apple Inc. ("Apple") moves to dismiss a complaint filed by plaintiff R.N. Nehushtan Trust Ltd. ("RNN Trust"), alleging that Apple's iPhones, iPads, and Watches directly infringe on claims in two of RNN Trust's patents. At issue is a technology directed at preventing the hacking and cloning of devices, in part by using a "device unique security setting" to restrict access to a "data mode" in which data can be read and written and the device's settings changed. Apple's arguments depend on how the asserted claims are constructed; it is premature to construct those claims now. RNN Trust sufficiently pleaded that the challenged elements of the asserted claims are met, which is enough for the case to proceed. Apple's motion to dismiss is DENIED.

## BACKGROUND

RNN Trust holds the rights, title, and interest to U.S. Patent Nos. 9,642,002 ("the '002 Patent") and 9,635,544 ("the '544 Patent"). Compl. [Dkt. No. 1] ¶ 1. The patents are directed to a "cellular communication security technology" aimed at preventing the cloning and hacking of devices. *See id.* ¶¶ 8-9. At a high level, the patents claim technology that includes, among other components, an "access restrictor" where a "device unique security setting" must be used to access a "data mode" that allows the reading and writing of data and the changing of settings on the device. *See id.* ¶¶ 9-13.

RNN Trust alleges that Apple sold devices—including its well-known and widely used iPhones, iPads, and Watches—that directly infringe on "at least" Claim 5 of the '002 Patent and "at least" Claim 17 of the '544 Patent. *See id*. ¶¶ 15, 19. Claim Five of the '002 Patent claims:

> A cellular communication device comprising a processor, a memory and a data mode, said data mode allowing reading and writing of data in said memory and changing of settings on said cellular communication device, said settings comprising personal data, cellular communication device configuration data and technical data relating to the cellular communication device; wherein
>
> said cellular communication device also comprises an access restrictor to restrict use of said data mode in accordance with a device unique security setting, the device unique security setting provided remotely to said cellular communication device using a predetermined security protocol;
>
> said device unique security setting is obtained remotely and provided to the cellular communication device before the data mode is used;
>
> said data mode permits actions comprising uploading, maintaining or replaying an operating system in said cellular communication device that are provided by a cellular provider using an active connection; the device further being configured to carry out one member of the group consisting of:
>
> enabling said cellular communication device to use said data mode when it is determined that said device unique security setting is correct; and
>
> disabling use of said data mode when said active connection is no longer active.

Compl., Ex. A ("'002 Patent) 22:49-23:8.

Claim 17 of the '544 Patent claims:

> A cellular communication device comprising a processor, a memory and a data mode, said data mode allowing reading and writing of data and changing of settings on said cellular communication device by an active connection;
>
> said settings comprising personal data, device configuration data and technical data relating to said cellular communication device;
>
> said cellular communication device further comprising an access restrictor to restrict use of said data mode in response to a cellular communication device unique security setting;
>
> wherein said device unique security setting is obtained remotely and provided to the cellular communication device before use of the data mode; said data mode being usable for transfer of icons to the cellular communication device; and

> wherein said cellular communication device is associated with a client program for managing a predetermined communication protocol, and carrying out one member of the group consisting of:
>
> setting said cellular communication device into said data mode when said device unique security setting is correct; and
>
> disabling said data mode when said active connection is no longer active.

*Id.*, Ex. B ("'544 Patent") 23:45-24:2.

Apple moved to dismiss on May 23, 2022. Dkt. No. 28.

## LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. To survive a Rule 12(b)(6) motion, the plaintiff must allege "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is facially plausible when the plaintiff pleads facts that allow the court to "draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citation omitted). There must be "more than a sheer possibility that a defendant has acted unlawfully." *Id.* While courts do not require "heightened fact pleading of specifics," a plaintiff must allege facts sufficient to "raise a right to relief above the speculative level." *See Twombly*, 550 U.S. at 555, 570.

In deciding whether the plaintiff has stated a claim upon which relief can be granted, the court accepts her allegations as true and draws all reasonable inferences in her favor. *See Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences." *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008).

## DISCUSSION

Under section 271(a) of the Patent Act, "whoever without authority makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent." 35 U.S.C. § 271(a). A device must practice all elements of a claim to be liable for direct infringement. *Fortinet, Inc. v. Forescout Techs., Inc.*, No. 20-CV-03343-EMC, 2020 WL 6415321, at *11 (N.D.

Cal. Nov. 2, 2020). Accordingly, a direct infringement claim "does not satisfy the standards of *Twombly* and *Iqbal* where it does not at least contain factual allegations that the accused product practices every element of at least one exemplary claim." *AlterG, Inc. v. Boost Treadmills LLC*, 388 F. Supp. 3d 1133, 1142-43 (N.D. Cal. 2019) (citation omitted).

The majority of RNN Trust's allegations regarding the infringement of the asserted claims are set forth in six claim charts totaling approximately 100 pages, which are incorporated by reference into its complaint. *See* Compl. ¶¶ 15, 20 (citing Exs. C-H). Each chart covers the claim limitations with respect to each of allegedly infringing Apple products—iPhones, iPads, and Watches—and cites evidence including user and security guides in support. *See id.*, Exs. C-H. Apple focuses on three limitations found within both of the asserted claims.

**I. "Data Mode" and "Settings" Limitations**

Apple argues that RNN Trust has failed to state a claim for direct infringement because the complaint does not plausibly allege that in Apple's devices, "the settings adjusted while in 'data mode' can *only* be changed when in 'data mode.'" Mot. to Dismiss ("MTD") [Dkt. No. 28] 6:16-17 (emphasis in original). Apple reads the claims to "require that certain security protocols are satisfied 'before the data mode is used' and any claimed settings are adjusted." *Id*. at 6:17-19. It acknowledges that RNN Trust "points to certain security protocols used for software updates to allegedly show the Apple devices meet the claims," but argues that it does not allege that other settings are changed using those protocols. *Id*. at 6:19-23.

Apple contends that many of the personal data settings that RNN Trust cites in its claim charts ("Apple ID and iCloud data, personal health data, emergency medical ID data, and data related to Apply pay") can be changed even if the Apple device is not connected to a cellular network, either because the user has turned off the device's cellular connectivity or because the device operates only with wireless internet. *See id*. at 8:7-24 (citing Ex. C at 5.2).[1] Apple makes the same argument about the configuration data (which, according to the claim charts, includes

[1] The numeric references to the limitations come from RNN Trust's claim charts. Although the charts include allegations regarding each Apple device (iPhones, iPads, and Watches) the

"data regarding notifications, sounds and haptics, date and time and fonts"). *See id*. at 8:24-27; *see also* Ex. C. at 5.2. Because the claimed data mode "requires an active, secure connection to a cellular network," Apple contends, the limitation is not met. *See id*. at 8:16-19.

Additionally, Apple argues that RNN Trust has failed to allege that technical data settings on Apple devices can be changed at all. *Id*. at 9:20-22. According to RNN Trust, technical information "can include the model number and serial number" of the device. *See* Ex. C at 5.2. Pointing to the section of the iOS 14 User Guide that RNN Trust cites, Apple argues that a user can only view the model and serial numbers on an Apple device—not change it. *See* MTD at 9:1-22. Accordingly, Apple argues, RNN Trust's "assertions are factually insupportable by the very evidence [it] cites." *Id*. at 9:1-2.

According to RNN Trust, these arguments amount to claim construction, which would be prematurely decided on a motion to dismiss. *See* Oppo. [Dkt. No. 29] 2:16-4:13. It rejects Apple's reading of the claims—"that the settings only can be changed in a single data mode, and that each of the three types of settings must be changed in a single data mode"—as too narrow, pointing to what it describes as "non-exclusive" language in the specification stating that the data mode "allows any access to the device to change settings and/or accept commands." *See id*. at 2:25-26, 4:13-22 (citing '002 Patent at 1:64-2:1). It also describes the claim language itself as "permissive"—that the data mode "allows access to the device to change settings"—rather than "mandatory or exclusionary." *Id*. at 4:23-5:3.

Apple's arguments boil down to one primary issue: whether, according to the asserted claims, specific settings can *only* be changed while the device is in data mode. This is not evident from the plain language of the asserted claims—the word "only" is nowhere to be found. *See* '002 Patent at Claim 5; '544 Patent at Claim 17. Rather, in making their points for and against their respecting reading of the claim language, the parties cite to the patents' abstracts and specifications. *See, e.g.,* Oppo. at 4:24 ("the pertinent language from the specification"); Reply [Dkt. No. 33] 3:5-22 (citing the abstracts). This is classic claim construction. In arguing what the claim terms mean, Apple misses the point: the dispute over those terms indicates that construction is necessary to understanding the claims.

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.