UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

ALD SOCIAL, LLC, Plaintiff, v. APPLE, INC., Defendant.	Case No. 23-cv-02695-JSC **ORDER RE: DEFENDANT APPLE'S MOTION TO DISMISS** Re: Dkt. No. 21

ALD Social sues Apple for infringement of two patents directed to systems to detect crowd safety risks and alert emergency personnel of such risks: U.S. Patent Nos. 9,198,054 ("the '054 patent") and 9,402,158 ("the '158 patent"). (Dkt. No. 1.)[1] Before this Court is Apple's motion to dismiss. (Dkt. No. 21.) After carefully considering the briefing, and with the benefit of oral argument on July 13, 2023, the Court GRANTS the motion with leave to amend. The documents Plaintiff attached to the complaint are inconsistent with the Accused Product satisfying the Asserted Patents' "crowd risk determinant" limitation or the '158 patent's "location aggregation" limitation.

BACKGROUND

A. ALD Social's Patents

Plaintiff filed suit against Apple for patent infringement in the Western District of Texas. (Dkt. No. 1.) Both the '054 patent and the '158 patent ("Asserted Patents") are titled "Aggregate Location Dynometer (ALD)." (Dkt. No. 1 at 4.) The '158 patent is a continuation of the '054 patent. '158 patent, col. 1 ll. 4-13. Both Asserted Patents' abstracts describe:

[1] Record citations are to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of the documents.

United States District Court
Northern District of California

> An Aggregate Location Dynometer (ALD) in a physical wireless network alerts to a problematic crowd risk using location based services (LBS). An Aggregate Location Dynometer (ALD) comprises a Network Monitor, a Crowd Risk Determinant and an Alert Module. The Network Monitor monitors wireless traffic for a potential viral event, associated with a formation of a plurality of wireless devices. The Crowd Risk Determinant requests location information associated with a plurality of wireless devices in a given area regarding a respective viral event. The Crowd Risk Determinant determines if the viral event also indicates a crowd safety risk, based on the shape and movement of observed wireless devices. The Alert Module triggers an alert of an impending crowd problem when crowd risk is above a given threshold. Historical databases are empirically determined and maintained in the Aggregate Location Dynometer (ALD) for use in viral event and crowd risk assessment.

'054 patent, abstract; '158 patent, abstract. The Asserted Patents elaborate on the significance of wireless devices:

> The Aggregate Location Dynometer (ALD) analyzes a bird's-eye view of people formation, presuming those individuals possess respective handheld wireless devices that permit collection of current location information, whether that current location information be obtained from the wireless devices themselves, and/or from a network-based location server.

'054 patent, col. 2 ll. 57-63; '158 patent, col. 2 ll. 61-67.

The invention claims a system to track the geographic location of wireless devices and determine whether a particular geographic region represents a "crowd related public safety risk." '054 patent, col. 2 ll. 45–col. 3 ll. 26; '158 patent, col. 2 ll. 49–col. 3 ll. 30. One such risk is a potential viral outbreak when the system detects, *e.g.*, too many wireless devices in one geographical area. *Id.* More specifically, claim 1 of the '054 patent states:

> 1. An aggregate location dynometer in a physical wireless network server, said aggregate location dynometer comprising:
>
> a network monitor to monitor a wireless network for an indication of a viral event;
>
> a location aggregator to obtain a location of each of a plurality of wireless devices associated with said viral event;
>
> a crowd risk determinant, triggered by said network monitor, to determine a crowd risk based on an aggregation of said location of each of said plurality of wireless devices associated with said viral event; and

EX. 1014
APPLE INC. / Page 2 of 15

> an alert module to initiate an alert message relating to a public safety risk determined from an analysis of said viral event.

'054 patent, col. 9 ll. 10-24. Claim 1 of the '158 patent states:

> 1. An aggregate location dynometer in a physical wireless network server, said aggregate location dynometer comprising:
>
> a network monitor to monitor a wireless network for an indication of a potential viral event indicated by an aggregation of current locations of a plurality of physical wireless devices associated with said potential viral event; and
>
> a crowd risk determinant to assess said aggregation of said current locations of said plurality of physical wireless devices pertaining to said potential viral event triggered by said network monitor.

'158 patent, col. 9 ll. 18-29.

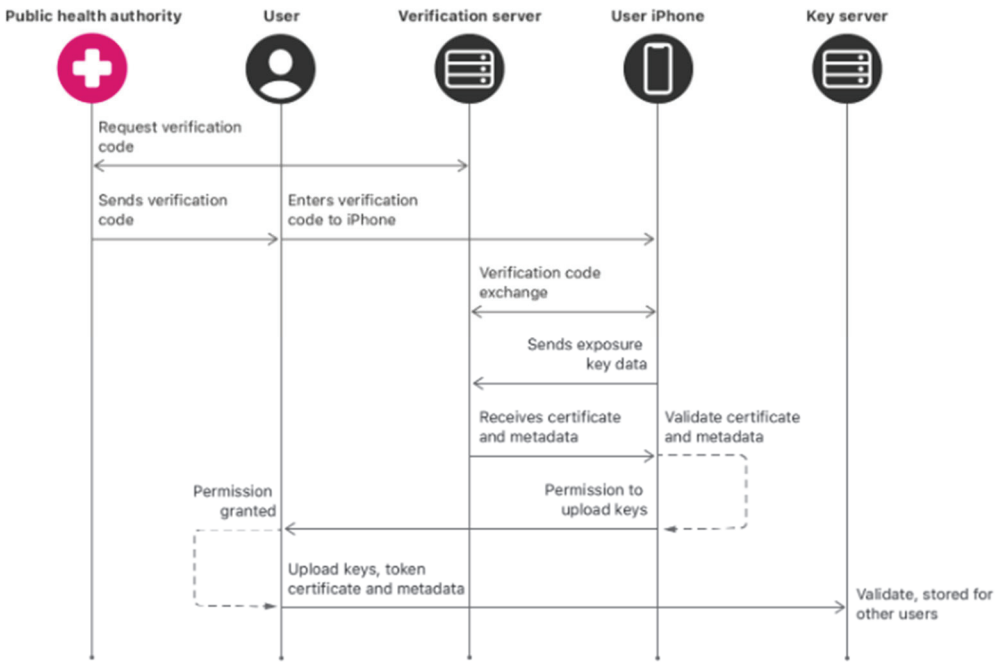
B. Complaint Allegations

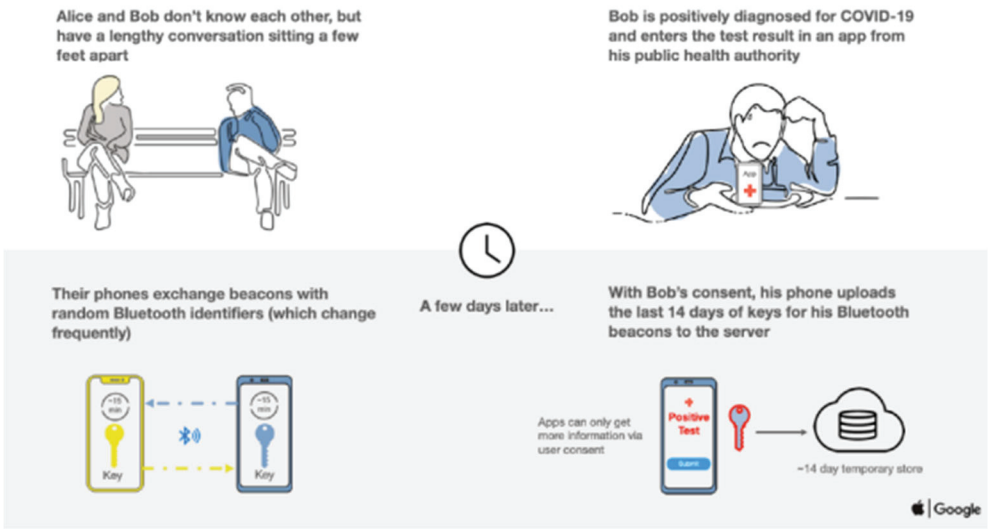
Plaintiff alleges Apple's Exposure Notification system (the "Accused Product") directly infringes, literally and/or under the doctrine of equivalents, at least claim 1 of both the '054 and '158 patents. (Dkt. No. 1 ¶¶ 18, 25.) Plaintiff's complaint attaches claim charts for each patent. (Dkt. No. 1-1 at 35-55.)

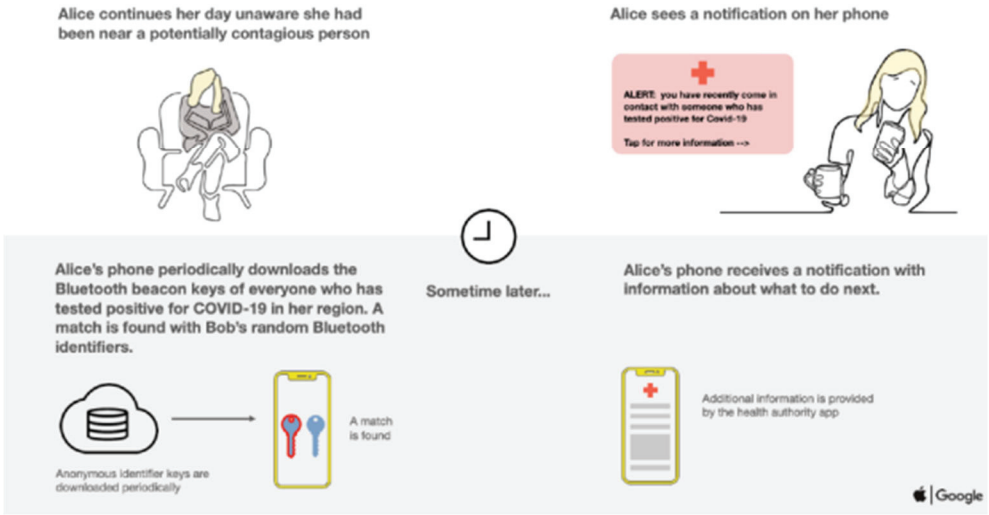
C. The Accused Product

Apple's product is a "[contact] tracing system that utilizes Bluetooth wireless technology to determine proximity of COVID-19 positive individuals and assess the risk of infection to alert users of this risk." (Dkt. No. 1-1 at 36, 49.) The system "has the capability to monitor a wireless network through Bluetooth beacon keys to verify and store COVID-19 positive case information, and once validated, send indication of the positive cases to users through a wireless network." *Id*. Apple's system can "determine exposure risk value based on risk parameters including but not limited to exposure proximity and duration." *Id*. at 42, 53.

Plaintiff offers the following illustrations of the Accused Product:


Public health authority
User
Verification server
User iPhone
Key server
Request verification code
Sends verification code
Enters verification code to iPhone
Verification code exchange
Sends exposure key data
Receives certificate and metadata
Validate certificate and metadata
Permission granted
Permission to upload keys
Upload keys, token certificate and metadata
Validate, stored for other users


Alice and Bob don't know each other, but have a lengthy conversation sitting a few feet apart
Bob is positively diagnosed for COVID-19 and enters the test result in an app from his public health authority
Their phones exchange beacons with random Bluetooth identifiers (which change frequently)
A few days later...
With Bob's consent, his phone uploads the last 14 days of keys for his Bluetooth beacons to the server
Key
Key
Apps can only get more information via user consent
Positive Test
~14 day temporary store
Google


Alice continues her day unaware she had been near a potentially contagious person
Alice sees a notification on her phone
ALERT: you have recently come in contact with someone who has tested positive for Covid-19
Tap for more information -->
Alice's phone periodically downloads the Bluetooth beacon keys of everyone who has tested positive for COVID-19 in her region. A match is found with Bob's random Bluetooth identifiers.
Sometime later...
Alice's phone receives a notification with information about what to do next.
Anonymous identifier keys are downloaded periodically
A match is found
Additional information is provided by the health authority app
Google

(Dkt. No. 1-1 at 37-38, 50-51.) These images show the Accused Product's "ability to exchange Bluetooth proximity identifiers, or keys, between devices as a form of location aggregation relative to a device" to "identify potential exposure to the virus between individuals." (Dkt. No. 1-1 at 36, 49.) The keys of users who report a positive COVID-19 diagnosis are added to a positive diagnosis list that devices "will periodically download and search" for "matches indicating proximity to COVID-19 positive individuals." *Id*. Apple's system can then send "alert messages to those with potential exposure to COVID-19 positive individuals." *Id*. at 45.

D. Procedural Background

While the matter was pending in the Western District of Texas, Apple filed a motion to dismiss the complaint for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6). (Dkt. No. 21.) The case was then transferred to this Court with the motion still pending. (Dkt. Nos. 32, 33.) Apple's motion to dismiss the complaint in its entirety is now pending. (Dkt. Nos. 21, 23, 24.)

DISCUSSION

Apple argues the complaint's factual allegations are insufficient to plausibly state a claim for infringement. In particular, Apple insists the complaint fails to allege facts demonstrating the Accused Product comprises a network monitor, location aggregator, or crowd risk determinant. Apple also argues both counts rely on Plaintiff's allegation the Accused Product aggregates location information, which is contradicted by the documents attached to the complaint.

For Plaintiff's complaint to survive, its factual allegations must raise a plausible right to relief. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554–56 (2007). "Determining whether a complaint states a plausible claim for relief is a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Ebner v. Fresh, Inc.*, 838 F.3d 958, 963 (9th Cir. 2016) (cleaned up). Though the Court must accept the complaint's factual allegations as true, conclusory assertions are insufficient to state a claim. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is facially plausible when the plaintiff pleads enough factual content to justify the reasonable inference that the defendant is liable for the misconduct alleged. *Id.*

EX. 1014
APPLE INC. / Page 5 of 15

An "element-by-element pleading standard for patent infringement . . . is unsupported and goes beyond the standard the Supreme Court articulated in *Iqbal* and *Twombly*." *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1352 (Fed. Cir. 2021). Rather, "[t]he adequacy of the facts pled depends on the breadth and complexity of both the asserted patent and the accused product or system and on the nature of the defendant's business activities." *K-Tech Telecomms., Inc. v. Time Warner Cable, Inc.*, 714 F.3d 1277, 1286 (Fed. Cir. 2013). For a "simple technology," a plaintiff may plausibly plead by providing the asserted patents, identifying the accused products "by name and by attaching photos of the product packaging," and alleging the accused products meet "each and every element of at least one claim… either literally or equivalently." *Disc Disease Sols. Inc. v. VGH Sols., Inc.*, 888 F.3d 1256, 1260 (Fed. Cir. 2018). However, "a plaintiff cannot assert a plausible claim for infringement under the *Iqbal/Twombly* standard by reciting the claim elements and merely concluding that the accused product has those elements. There must be some factual allegations that, when taken as true, articulate why it is plausible that the accused product infringes the patent claim." *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1353 (Fed. Cir. 2021) (agreeing with the district court's dismissal where the complaint's allegations were conclusory, merely tracked the claim language, and did not present plausible factual content in support of infringement).

Even when a complaint provides sufficient factual statements, a plaintiff may still fail to plausibly state a claim where (1) the infringement allegation rests on an implausible claim construction, *Ottah v. Fiat Chrysler*, 884 F.3d 1135, 1141-42 (Fed. Cir. 2018), or (2) "the factual allegations are actually *inconsistent* with and contradict infringement." *Bot M8 LLC*, 4 F.4th at 1354.

A. Direct Infringement

A party who "makes, uses, offers to sell, or sells" a patented invention "without authority" directly infringes a patent. 35 U.S.C. § 271(a). Direct infringement requires the accused product to literally infringe or infringe under the doctrine of equivalents. *Ottah v. Bracewell LLP*, No. 22-1876, 2022 WL 16754378, at *2 (Fed. Cir. Nov. 8, 2022). "A finding of literal patent infringement requires that each and every limitation set forth in a claim appear in an accused

EX. 1014
APPLE INC. / Page 6 of 15

product." *Id.* Apple seeks dismissal because the complaint fails to allege factual support for the Accused Product's infringement of elements ubiquitous to the Asserted Patents' claims: the "network monitor," "location aggregation," and "crowd risk determinant" limitations. The Court addresses each element in turn.

1. Network Monitor

Claim 1 of the Asserted Patents requires a "network monitor to monitor a wireless network for an indication of a viral event." '054 patent, col. 9 ll. 13-14; '158 patent, col. 9 ll. 21-22. Potential viral events are "indicated by an aggregation of current locations of a plurality of physical wireless devices associated with said potential viral event[s]." '158 patent, col. 9 ll. 21-25. More specifically,

> the Network Monitor utilizes location based services (LBS) to monitor the formation of a plurality of wireless devices at a given point in a wireless network. The Network Monitor compares obtained traffic parameters pertaining to monitored wireless traffic, with historical traffic parameters having to do with crowd risk determination to determine if a viral event may be occurring or impending. A snapshot look at current location data collected by the Network Monitor is subsequently logged in an appropriate historical database.

'054 patent, col. 1 ll. 44-54; '158 patent, col. 1 ll. 47-57.

Plaintiffs allege the Accused Product has a network monitor because of its "capability to monitor a wireless network through Bluetooth beacon keys to verify and store COVID-19 positive case information, and once validated, send indication of the positive cases to users through a wireless network." (Dkt. No. 1-1 at 36, 49.) Apple argues Plaintiff fails to identify a network monitor in the Accused Product because "there is no identification of a network monitor of any Bluetooth network," Dkt. No. 21 at 11, or "any monitoring for a viral event that is performed via the Bluetooth beacon keys." (Dkt. No. 24 at 7.)

The complaint alleges the existence of a network monitor in the Accused Product by referencing images included in Plaintiff's claim charts. (Dkt. No. 1-1 at 36-39, 49-52.)[2] The first

[2] The Court may consider Plaintiff's claim charts because Plaintiff attached them to the complaint. *See United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) (ruling courts may review "documents attached to the complaint" at the 12(b)(6) stage).

EX. 1014
APPLE INC. / Page 7 of 15

image is also the first pictured above in the Background section. In the first image, a user of the Accused Product requests a verification code from the public health authority, which then sends the verification code to the user, who then enters the verification code into their mobile device. (Dkt. No. 1-1 at 37, 50.) The mobile device then exchanges the verification code with and sends exposure key data to the verification server in exchange for a certificate and metadata the mobile device then validates before asking the user for permission to upload keys. *Id*. When the user grants permission, the user's keys, token certificate, and metadata are uploaded to the key server, which validates and stores COVID-19 exposure information for other users. *Id*.

The second image, which is the second image pictured above in the Background section, shows two users of the Accused Product, Alice and Bob, sitting next to each other on a bench as their mobile devices exchange random and frequently changing Bluetooth identifiers. (Dkt. No. 1-1 at 38, 51.) A few days after their bench encounter, Bob receives a positive COVID-19 diagnosis and enters the test result into his public health authority's application. *Id*. With Bob's consent, his mobile device uploads the last 14 days of keys for his Bluetooth beacons to the key server. *Id*. Because Alice's mobile device is periodically downloading the Bluetooth beacon keys of everyone who has tested positive for COVID-19 in her region, she receives a notification that she recently encountered someone who tested positive for COVID-19 when her mobile device finds Bob's Bluetooth identifier in the list of those associated with a positive COVID-19 diagnosis. *Id*.

The third image is a diagram illustrating the flow of broadcasting between two devices using the Accused Product. (Dkt. No. 1-1 at 52.) The image shows the Accused Product asks the user permission to enable exposure notification before generating a temporary exposure key for that user's device and saving the device's rolling proximity identifier and associated encrypted metadata into the key server. *Id*. Every 15 minutes, the user's rolling proximity identifier and associated encrypted metadata changes. *Id*. Every 24 hours, the Accused Product generates a new temporary exposure key with associated encrypted metadata for each user's device. *Id*.

Taken as true, the claim charts indicate the Accused Product senses the real-time proximity between a plurality of devices over a wireless network via Bluetooth "for the purpose of

EX. 1014
APPLE INC. / Page 8 of 15

computing an exposure event" and ultimately "to combat the spread of the coronavirus."[3] *Exposure Notification Bluetooth Specification* (April 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1 at 3, 4 (document cited at Dkt. No. 1-1 at 40, 44, 52, 55). This is sufficient to support an inference the Accused Product monitors the formation of mobile devices over a wireless network for indication of a viral event. The complaint plausibly alleges the existence of a network monitor in the Accused Product.

2. Location Aggregator

Claim 1 of the '054 patent requires a "location aggregator to obtain a location of each of a plurality of wireless devices associated with said viral event." '054 patent, col. 9 ll. 15-17. Claim 1 of the '158 patent requires "indication of a potential viral event indicated by an aggregation of current locations of a plurality of physical wireless devices associated with said potential viral event." '158 patent, col. 9 ll. 22-25.

Plaintiff alleges the Accused Product has a location aggregator because it "includes the ability to exchange Bluetooth proximity identifiers between devices as a form of location aggregation relative to a device." (Dkt. No. 1-1 at 39, 49.) Plaintiff identifies the Accused Product's "method to determine if the user traveled outside of their app-associated region," which Plaintiff contends "demonstrates that [the Accused Product] can access location data of each of a plurality of wireless devices associated with the viral event." (Dkt. No. 1-1 at 39.) Apple argues the complaint does not identify any "location aggregation," and relies on documents attached to Plaintiff's claim charts showing the Accused Product does not monitor location or aggregate any current location data.

i. Location Aggregation

Apple argues Plaintiff fails to identify an aggregation of locations in the Accused Product and instead only identifies an exchange of Bluetooth keys between two devices. Apple claims

[3] *Exposure Notification Bluetooth Specification* (April 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.2.pdf?1 at 3, 4 (document cited at Dkt. No. 1-1 at 40, 44, 52, 55), hereinafter referred to as "Bluetooth Specification."

EX. 1014
APPLE INC. / Page 9 of 15

Plaintiff's claim charts, which attach Apple's documents describing the functionality of the Accused Product, contradict any location aggregation in the Accused Product because "[l]ocation information is not collected from a user's device." (Dkt. No. 21 at 15.) The documents attached to Plaintiff's claim charts say the Accused Product "does not share location data from the user's device with the Public Health Authority, Apple, or Google,"[4] and "does not use location for proximity detection. It strictly uses Bluetooth beaconing to detect proximity." Bluetooth Specification at 8.

The "location aggregation" limitation requires the location of each of a plurality of mobile devices associated with a viral event be obtained and aggregated in a physical wireless network server. '054 patent, col. 9 ll. 10-17; '158 patent, col. 9 ll. 18-25. According to the claim charts, the Accused Product deploys two kinds of servers: the verification server and the key server. (Dkt. No. 1-1 at 37, 50.) The verification server validates positive diagnoses during key upload. The key server handles key uploads and downloads. According to Plaintiff's claim charts and attached documents, the servers contain information allowing the Accused Product to notify users who encountered an infected individual of the day, length, and degree of their COVID-19 exposure.

> If a user decides to participate, **exposure notification data will be stored and processed on device**. Other than the random Bluetooth identifiers that are broadcast, no data will be shared by the system with the public health authority unless one of the following two scenarios takes place:
>
> - If a user chooses to report a positive diagnosis of COVID-19, the user's most recent keys to their Bluetooth beacons will be added to the positive diagnosis list shared by the public health authority so that other users who came in contact with those beacons can be alerted.
> - If a user is notified that they have come into contact with an individual who is positive for COVID-19 **the system will share the day the contact occurred, how long it lasted and the Bluetooth signal strength of that contact, as well as the type of report** (such as confirmed by test, clinical diagnosis, or self-report). Any other information about the contact will

[4] *Exposure Notifications Frequently Asked Questions* (September 2020), https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-FAQv1.2.pdf at 5 (document cited at Dkt. No. 1-1 at 39, 42, 43, 45, 47, 52, 54), hereinafter referred to as "FAQ."

EX. 1014
APPLE INC. / Page 10 of 15

not be shared.

FAQ at 5 (emphasis added). Users are not alerted of *where* they encountered an infected individual—*i.e*, location of their exposure. *Id*. Plaintiff nonetheless alleges the Accused Product has a location aggregator because applications using the Accused Product must declare their geographic region of operation and the Accused Product can track users' travel across regions. (Dkt. No. 1-1 at 39, 49.)

All applications using the Accused Product must specify the region for which they work. *Id*. Plaintiff's claim charts identify the Accused Product's method for determining whether a user has traveled outside of the region associated with an application anytime in the last 14 days. *Id*.

```
func userTraveled() async throws -> Bool
```

getUserTraveled(completionHandler:), APPLE DEVELOPER, https://developer.apple.com/documentation/exposurenotification/enmanager/3644439-getusertraveled (document cited at Dkt. No. 1-1 at 39, 49). Apple's Developer page says this information can be used to determine when to share keys across regions. *Id*. This raises the plausible inference the Accused Product obtains and stores location data from users' devices so it can be accessed to determine users' location within the last 14 days. Without location data, how would the Accused Product determine whether and where a user traveled across geographic regions?

Apple side-steps this question, claiming Plaintiff improperly conflates Bluetooth beaconing with the Accused Product's ability to function in a given geographical region. Apple instead focuses on Plaintiff's failure to allege any connection between location aggregation and risk determination in the Accused Product. Apple insists the complaint must allege facts showing the Accused Product aggregates location information to determine COVID-19 exposure because the Asserted Patents' claims require aggregated location data be used for risk determination. The Court disagrees. Plaintiff need not prove its case at the pleading stage. *Bot M8 LLC v. Sony Corp. of Am.*, 4 F.4th 1342, 1352 (Fed. Cir. 2021). Apple is on notice that its system is being accused of

EX. 1014
APPLE INC. / Page 11 of 15

infringement based in part on its alleged aggregation of location information from mobile devices to assess coronavirus exposure. *Lifetime Indus., Inc. v. Trim-Lok, Inc.*, 869 F.3d 1372, 1379 (Fed. Cir. 2017) ("Our precedent requires that a complaint place the alleged infringer on notice of what activity is being accused of infringement." (cleaned up)). Plaintiff plausibly alleges the Accused Product employs location data to determine whether to share exposure information across geographic regions despite Apple's claim "an explicit feature of [the Accused Product] is that no location data is shared, stored, or analyzed." (Dkt. No. 21 at 9.) Accordingly, the complaint plausibly alleges facts supporting its claim of the Accused Product's infringement of the "location aggregation" limitation of both Asserted Patents.

ii. Current Location Data

The '158 patent requires "aggregation of **current** locations of a plurality of physical wireless devices associated with said potential viral event." '158 patent, col. 9 ll. 22-25 (emphasis added). According to Plaintiff's claim charts and attached documents, the Accused Product does not aggregate current locations of mobile devices to indicate a potential viral event. Rather, Plaintiff's claim charts and attached documents show the Accused Product indicates a viral event based on reported COVID-19 diagnoses and proximity data recorded from past interactions among mobile devices. When a user voluntarily reports a positive COVID-19 result, the Accused Product uploads the last 14 days of their beacon keys to the key server and notifies devices that encountered the infected user's device of their past, though recent, exposure. Because the documents Plaintiff attached to the complaint show the Accused Product does not aggregate current locations of mobile devices associated with positive COVID-19 diagnoses to indicate coronavirus exposure, Plaintiff does not plausibly plead the Accused Product satisfies the "location aggregation" limitation of the '158 patent.

3. Crowd Risk Determinant

Claim 1 of the Asserted Patents requires a "crowd risk determinant, triggered by said network monitor, to determine a crowd risk based on an aggregation of said location of each of said plurality of wireless devices associated with said viral event." '054 patent, col. 9 ll. 15-17; '158 patent, col. 9 ll. 26-29. The crowd risk determinant analyzes location information to

EX. 1014
APPLE INC. / Page 12 of 15

determine if a viral event indicates a crowd safety risk. ’054 patent, col. 1 ll. 56-58; ’158 patent, col. 1 ll. 59-61.

> In particular, the Crowd Risk Determinant initiates a location request to obtain location information pertaining to a multitude of wireless devices in a given area, regarding a viral event that has been triggered by the Network Monitor. The Crowd Risk Determinant compares the viral pattern formed by the shape and movement of wireless devices in locations observed, with predetermined risk rules to determine if the viral event is also a crowd safety risk.

’054 patent, col. 1 ll. 58-66; ’158 patent, col. 1 ll. 61 – col. 2 ll. 2.

Plaintiff alleges the Accused Product infringes the crowd risk determinant element because the Accused Product “includes an algorithm for determining risk after finding a match from the key data.” (Dkt. No. 1-1 at 42, 53.) Plaintiff’s claim charts and attached documents show the Accused Product can use an algorithm to determine exposure risk based on factors including but not limited to exposure proximity and duration. *Id*. at 53-55. Apple argues Plaintiff failed to identify a “crowd risk determinant” because the algorithm Plaintiff references determines risk to individuals, not crowd safety. In essence, Apple seeks dismissal of Plaintiff’s complaint because the documents Plaintiff attached to the complaint show the Accused Product does not determine “crowd risk” or indicate “crowd safety risk.” To address Apple’s argument, the Court considers the meaning of the term “crowd risk.”

Claim construction is generally not proper at the 12(b)(6) stage. *See Nalco Co. v. Chem-Mod, LLC*, 883 F.3d 1337, 1350 (Fed. Cir. 2018); *see also Fujitsu Ltd. v. Belkin Int’l, Inc.*, 782 F. Supp. 2d 868, 890 (N.D. Cal. 2011) (explaining a “motion to dismiss is not the proper time to initiate claim construction”). However, the Court may dismiss a complaint prior to claim construction if the complaint depends on an implausible claim construction. *See Fiat Chrysler*, 884 F.3d at 1141-42; *see also Nalco Co.*, 883 F.3d at 1349 (explaining patent infringement plaintiff must plead sufficient facts “to raise a reasonable expectation that discovery will reveal evidence” to support plaintiff’s allegations).

For the Accused Product to infringe the Asserted Patents’ “crowd risk determinant” limitation, it must determine a “crowd risk.” The Asserted Patents’ claim an invention “to predict public safety risks, e.g., the unexpected impending formation of a flash mob, or a riot, etc.” ’054

EX. 1014
APPLE INC. / Page 13 of 15

patent, col. 2 ll. 52-56; '158 patent, col. 2 ll. 58-60. The invention alerts "to a problematic crowd risk in a given geographical location." '054 patent, col. 1 ll. 32-33; '158 patent, col. 1 ll. 35-36. The Asserted Patents' specifications are instructive:

> Crowd risk is assessed based upon given wireless network traffic parameters such as the number of wireless devices in communication with a given base station (e.g., a density), the shape formed by representations of the individual locations of the densest areas where active wireless devices are currently located, and/or the movement of the wireless devices within the region as defined.

'054 patent, col. 3 ll. 9-15; '158 patent, col. 3 ll. 13-19.

> Motion trends are also analyzed to assess crowd risk. The Crowd Risk Determinant preferably determines whether the accumulation of wireless devices is becoming more or less dense about a central location and whether or not this behavior is expected based on trends and configured thresholds established for particular locations.

'054 patent, col. 8 ll. 18-23; '158 patent, col. 8 ll. 26-31. The term "crowd risk," consistent with its plain language meaning and the Asserted Patents' descriptions, denotes a danger posed by a contemporaneous accumulation of people in a geographic location, as indicated by the observable location and movement of wireless devices.

Plaintiff argues the Accused Product determines and assesses a crowd risk because it "monitor[s] every interaction between two or more people, including crowd gatherings of any kind, and assesses the individual and unique risk of COVID-19 exposure of every individual in the crowd." (Dkt. No. 23 at 9.) This is contradicted by Plaintiff's claim charts and attached documents. First, it is an inaccurate description of the Accused Product. Neither the complaint nor the claim chart support a plausible inference the Accused Product monitors every interaction between people and assesses the individual, unique risk of COVID-19 exposure for every monitored individual. The documents attached to the complaint show the Accused Product monitors the proximity between mobile devices via Bluetooth and alerts specific devices of potential viral exposure based on reported COVID-19 results and past data of interactions between mobile devices.

Second, it is implausible to construe the term "crowd risk" to include exposure risk calculated from records of past encounters between mobile devices and communicated

EX. 1014
APPLE INC. / Page 14 of 15

retroactively to individuals. The Asserted Patents predict the occurrence of an impending viral outbreak based on present conditions at a geographic location. As described in the documents Plaintiff attached to the complaint, the Accused Product indicates the incidence and potential degree of past viral exposure to individuals based on past conditions untethered from geographic location. Risk to an individual is not the same as or equivalent to risk posed by a crowd. The term "crowd risk" does not encompass the likelihood of an individual's past exposure to COVID-19. *See Fiat Chrysler*, 884 F.3d at 1141-42 ("The district court correctly found that the "book holder" cannot plausibly be construed to include or be the equivalent of a camera holder, in view of the specification and the prosecution history.").

The complaint fails to plausibly allege the Accused Product infringes the Asserted Patents' "crowd risk determinant" limitation because the term "crowd risk" cannot plausibly be construed to include the likelihood of an individual's past exposure to COVID-19.

CONCLUSION

The documents Plaintiff attached to the complaint demonstrate the Accused Product does not satisfy the Asserted Patents' "crowd risk determinant" limitation or the '158 patent's "location aggregation" limitation. Apple's motion to dismiss is therefore GRANTED. Plaintiff may file an amended complaint on or before August 14, 2023. *Yagman v. Garcetti*, 852 F.3d 859, 863 (9th Cir. 2017). An initial case management conference is set for **November 9, 2023 at 1:30 p.m**. by a Zoom videoconference. A joint case management conference is due by November 2, 2023.

This Order disposes of Docket No. 21.

IT IS SO ORDERED.

Dated: July 24, 2023

JACQUELINE SCOTT CORLEY
United States District Judge