UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

FEDERAL TRADE COMMISSION, Plaintiff, v. KOCHAVA, INC., Defendant.	Case No. 2:22-cv-00377-BLW MEMORANDUM DECISION AND ORDER

INTRODUCTION

Before the Court is Defendant Kochava, Inc.'s Motion to Dismiss First Amended Complaint Pursuant to Fed. R. Civ. P. 12(b)(6) (Dkts. 33 & 34). The motion is fully briefed, and the Court has determined that oral argument would not aid in the decisional process. For the reasons explained below, the Court will deny the motion.

BACKGROUND[1]

1. This Lawsuit

The Federal Trade Commission (FTC) claims that Kochava, Inc. is violating Section 5(a) of the Federal Trade Commission Act (the "FTC Act") by aggregating

[1] At this stage, the Court must assume the truth of the FTC's factual allegations.

and selling vast amounts of data collected from mobile devices. *See Am. Compl.*, Dkt. 26. The FTC argues that Kochava's data sales invade consumers' privacy and expose them to risks of secondary harms by third parties. Thus, according to the FTC, Kochava is engaging in an "unfair . . . act or practice" prohibited by Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)(1). To prevent Kochava from continuing to do so, the FTC seeks a permanent injunction under Section 13(b), 15 U.S.C. § 53(b).

In its original Complaint (Dkt. 1), the FTC focused on one subset of Kochava's data: geolocation coordinates. The FTC alleged that, by linking mobile device location coordinates to Mobile Advertising IDs (MAIDs), Kochava enables its customers to identify specific device users who have visited certain sensitive locations. According to the FTC, Kochava's geolocation data invades consumers' personal privacy and creates a risk that third parties will target consumers based upon their visits to certain sensitive locations, such as abortion clinics.

2. Dismissal of the Original Complaint

On October 28, 2022, Kochava moved to dismiss the FTC's original Complaint and the Court held oral argument on February 21, 2023. Dkt. 20. Ultimately, the Court dismissed the Complaint because it lacked adequate allegations that Kochava's data sales "cause[] or [are] likely to cause" a "substantial injury" to consumers, as required by Section 5(n) of the FTC Act. *See*

Mem. Decision & Order at 24–25, Dkt. 24. Although the Court held that both of the FTC's theories of consumer injury were legally plausible, it concluded that the alleged injury did not rise to the requisite level of substantiality.

Under the FTC's first theory, Kochava's data sales create a risk of secondary harm to consumers. That is, Kochava's customers could use the geolocation data to identify mobile device users who have visited sensitive locations and, based on inferences arising from that information, inflict secondary harms including stigma, discrimination, physical violence, and emotional distress. *Compl.* ¶ 29, Dkt. 1. The Court agreed that a company could substantially injure consumers within the meaning of Section 5(n) by selling their sensitive location information and thereby subjecting them to a significant risk of suffering concrete harms at the hands of third parties. *Mem. Decision & Order* at 14, Dkt. 24. However, the Court found insufficient allegations as to the significance of such risks in this case. The Court explained that to adequately plead this theory of consumer injury, the FTC must "go one step further and allege that Kochava's practices create a 'significant risk' that third parties will identify and harm consumers." *Id.* at 17.

Under the FTC's second theory, Kochava's geolocation data deprives consumers of their privacy. That is, the loss of privacy—rather than some secondary harm that could flow from the disclosure of the information—is itself an injury to consumers. The Court also agreed that this theory is legally plausible but

concluded that the privacy intrusion alleged in the Complaint was not severe enough to constitute a "substantial injury" under Section 5(n).

The Court dismissed the Complaint but gave the FTC an opportunity to file an amended complaint containing additional factual allegations. The FTC did so, filing its Amended Complaint (Dkt. 26) on June 26, 2024. Kochava promptly moved to dismiss the Amended Complaint under Rule 12(b)(6), arguing that the FTC has not cured the deficiencies identified in the Court's prior Memorandum Decision and Order, Dkt. 24. As explained below, the Court disagrees.

LEGAL STANDARD

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). "[D]ismissal may be based on either a lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Johnson v. Riverside Healthcare Sys.*, 534 F.3d 1116, 1121 (9th Cir. 2008) (cleaned up). However, Rule 12(b)(6) "does not impose a probability requirement at the pleading stage; it simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence" of the truth of the allegations. *Twombly*, 550 U.S. at 556.

Section 5(a) of the FTC Act prohibits "unfair" and "deceptive" acts or practices that harm consumers or competitors. 15 U.S.C. § 45(a). And Section

13(b) of the same statute authorizes the FTC to seek injunctive relief if it "has reason to believe" that a business "is violating, or is about to violate, any provision of law enforced by the [FTC]," including Section 5(a). 15 U.S.C. § 53(b). To demonstrate that an act or practice is "unfair" under Section 5(a), the FTC must prove that it "[1] causes or is likely to cause substantial injury to consumers which is [2] not reasonably avoidable by consumers themselves and [3] not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. 45(n); *see also Mem. Decision & Order*, Dkt. 24.

DISCUSSION

According to the FTC, Kochava sells a substantial amount of data obtained from millions of mobile devices across the world. This includes precise geolocation data and a "staggering amount of sensitive and identifying information," including device users' "names, MAIDs, addresses, phone numbers, email addresses, gender, age, ethnicity, yearly income, 'economic stability,' marital status, education level, political affiliation, 'app affinity' (i.e. what apps consumers have installed on their phones), app usage," and "interests and behaviors." *Am. Compl.* ¶¶ 11, 16 & 20, Dkt. 26. By selling this data, the FTC claims, Kochava substantially harms consumers in violation of Section 5(a) of the FTC Act. *See* 15 U.S.C. § 45(a) & (n).

The FTC's claim is legally and factually plausible. In other words, Kochava's practice of selling vast amounts of data about mobile device users *may* violate Section 5(a) by depriving consumers of their privacy and exposing them to significant risks of secondary harms. The FTC's Amended Complaint significantly expands the factual allegations in its original Complaint, and it easily satisfies the liberal plausibility standard.

1. The FTC's Allegations

The Amended Complaint focuses on four of Kochava's data products: geolocation data, the Database Graph, the App Graph, and audience segments. A summary of each product may be helpful.

Geolocation Data. Kochava's geolocation data feeds contain timestamped latitude and longitude coordinates and associated MAIDs from "125 million monthly active users, and 35 million daily active users, on average observing more than 90 daily transactions per device." *Am. Compl.* ¶¶ 27 & 30, Dkt. 26. The coordinates can pinpoint a device's location within less than 10 meters "for at least the past year" and reflect "movements as recent as the prior day." *Id.* ¶ 26.

Database Graph. Kochava's Database Graph contains "comprehensive profiles of individual consumers," with up to "300 data points" for "over 300M unique individuals." *Id.* ¶ 46. A given profile may contain a device user's name, address, phone number, MAID, ethnicity, gender identity, date of birth, status as a

minor, status as a parent and number of children, political association, marital status, education, economic status, employment, languages spoken, device settings, and social media presence. *Id.* ¶¶ 47–49, 53.

App Graph. Kochava's App Graph shows device users' activities in particular mobile device applications. The graph contains usage information and the associated MAIDs from over 275,000 mobile apps, including app names, the dates and lengths of app usage, the type of actions taken in the apps, and the amount of money spent in the apps. *Am. Compl.* ¶¶ 60 & 61, Dkt. 26. For example, the App Graph would show whether a device user has downloaded an LGBTQ+ dating app, a Muslim prayer app, or an app for monitoring specific health concerns, like cancer or sexually transmitted infections. *Id.* ¶ 62.

Audience Segments. Kochava also sells "audience segments," which are "subsets of its database of consumer information that identify consumers based on interests or characteristics." *Id.* ¶ 64. For example, device users can be sorted by geography, demography, points of interest, web usage, political associations, parental status, or religious affiliations. *Id.* ¶¶ 64–76. Thus, one of Kochava's customers could generate a list of devices—with each device linked to a MAID—that are used by expecting parents, or pregnant people, or those with particular gender identities, or those associated with other specified interests or characteristics. *Id.* ¶ 67–76.

The FTC claims that Kochava's customers "can and do purchase any and all of this data."[2] *Am. Compl.* ¶ 23, Dkt. 26. Consequently, although the data is contained in separate collections, it "is not anonymized and is linked or easily linkable to individual consumers." *Id.* ¶ 77. For example, drawing upon data contained in Kochava's various collections, a customer could identify "a woman who visits a particular building, the woman's name, email address, and home address, and whether the woman is African-American, a parent (and if so, how many children), or has an app identifying symptoms of cancer on her phone." *Id.* ¶ 23. And the customer could do this without "min[ing] other sources of data," because "[t]his ability is a featured product of Kochava." *Id.* ¶¶ 80 & 81, Dkt. 26 ("For example, Kochava advertises that customers are able to search through its '500M+ MAIDs' to identify, among other things, the consumer's name, address, phone number, email address, gender, age, yearly income, 'economic stability,' marital status, education level, app affinity, and interests and behaviors.").

According to the FTC, Kochava's data sales harm consumers in two distinct ways. First, by putting them at an increased risk of suffering secondary harms, such as stigma, discrimination, physical violence, and emotional distress. And

[2] To be clear, Kochava adamantly disputes the truth of this allegation. *Def.'s Memo. in Supp. Of Motion for Sanctions Under Rule 11* at 9, Dkt. 40-1 ("Kochava's customers neither do nor can they purchase all of this data, which are all separate, non-overlapping feeds and products without linkages to one another."). But, of course, this is not the time for resolving factual disputes.

second, by invading their privacy. The FTC has alleged facts sufficient to proceed under both theories.

2. Theory #1: Increased Risk of Secondary Harms

First, the FTC claims that Kochava's practices expose consumers to significant risks of secondary harms, including "stigma, discrimination, physical violence, [and] emotional distress." *Am. Compl.* ¶ 97, Dkt. 26. By using Kochava's precise geolocation data, the FTC explains, Kochava's customers can target consumers who have visited certain sensitive locations. *Id.* ¶ 98. The FTC identifies two factors that "exacerbate[]" those risks. First, the "lack of controls surrounding who accesses this data, and how those entities use it." *Id.* ¶ 99. And second, Kochava's practice of linking geolocation data to MAIDs and thereby making it "easy" to "identify[] consumers by name or other identifying information[.]" *Id.* ¶ 100.

Unlike the original Complaint, the Amended Complaint contains allegations that the targeting of consumers based on geolocation data "has and does occur." *Id.* ¶ 101. To illustrate, the FTC provides several real-world examples of harms inflicted on device users due to the disclosure of their geolocation and app-use data. *Id.* ¶¶ 101 & 104–05. Kochava responds that none of the FTC's "anecdotes" involve its own data. *Def.'s Reply* at 7, Dkt. 51. But that misses the point. Under Section 5(n), the FTC must allege that Kochava's acts or practices cause *or are*

likely to cause substantial injury to consumers. 15 U.S.C. § 45(n). By demonstrating that harms have resulted from the sale of similar mobile device data, the FTC supports its claim that Kochava's practices are likely to cause consumer injury.[3]

In sum, the FTC plausibly alleges that Kochava causes or is likely to cause substantial injury to consumers by selling "massive amounts of private and encyclopedic information" that puts consumers at a significant risk of suffering secondary harms. *Pl.'s Resp.* at 1, Dkt. 45.

3. Theory #2: Invasion of Privacy

The FTC's second theory of consumer injury is also plausible. Kochava's practices arguably inflict a substantial injury on consumers by invading their privacy. As this Court previously explained, privacy has long been a legally protected interest at the state, local, and federal levels. *See Mem. Decision and Order* at 19, Dkt. 24. Accordingly, an invasion of privacy may constitute an injury that gives rise to liability under Section 5(a). *Id.* The remaining question is simply

[3] Kochava also argues that the alleged consumer injury "is not caused by Kochava but instead by some unknown third parties." *Def.'s Memo. in Supp.* at 10, Dkt. 33-1. However, as the Court already explained, Section 5(a) does not require that the defendant be the one actually inflicting the ultimate harm. *See Mem. Decision & Order* at 15–16, Dkt. 24 ("[A] defendant can 'cause' substantial injury under Section 5(n) merely by creating 'a significant risk of concrete harm.'") (quoting *Neovi, Inc.*, 604 F.3d at 1157).

whether the alleged privacy intrusion rises to the requisite level of "substantial" injury. *See id.* at 22. It does.

Both the United States Supreme Court and the Ninth Circuit Court of Appeals have recognized the unique threat that modern technology can pose to privacy rights. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019) ("[A]dvances in technology can increase the potential for unreasonable intrusions into personal privacy."). In *Carpenter v. United States*, for example, the Supreme Court addressed the expectation of privacy in cell phone location records. 138 S.Ct. 2206, 2217 (2018).[4] The Court explained that cell phones have become "almost a feature of human anatomy," and consequently, historic cell phone location data—unlike the real-time GPS monitoring at issue in *United States v. Jones*, 565 U.S. 400 (2012)—"provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 2217–18 (internal quotations omitted).

The Ninth Circuit recently applied the principle from *Carpenter* in a case more factually similar to this one. *See In re Facebook, Inc. Internet Tracking*

[4] Although *Carpenter* arose in the Fourth Amendment context, the Ninth Circuit has "found analogies to Fourth Amendment cases applicable when deciding issues of privacy related to technology." *In re Facebook Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020). This Court does, too.

Litigation, 956 F.3d 589 (9th Cir. 2020). There, social media users sued Facebook for using plug-ins to track their internet browsing histories across third-party websites, and for compiling that data into "personal profiles which [were] sold to advertisers to generate revenue." *Id.* at 596. The court denied Facebook's motion to dismiss and held that compiling "highly personalized profiles from sensitive browsing histories and habits" plausibly constituted a "highly offensive" invasion of privacy. *Id.* at 606. Indeed, the court explained, modern technology has enabled the collection of "otherwise unknowable" information that "'implicates privacy concerns' in a manner different from traditional intrusions as a 'ride on horseback' is different from 'a flight to the moon.'" *Id.* at 603 (quoting *Patel*, 932 F.3d at 1273).

Kochava allegedly provides its customers with vast amounts of essentially non-anonymized information about millions of mobile device users' past physical locations, personal characteristics (including age, ethnicity, and gender), religious and political affiliations, marital and parental statuses, economic statuses, and more. In doing so, Kochava does not merely sell "bits and pieces" of data that are available through other lawful means. *See In re Google Location History Litig.*, 428 F.Supp.3d 185, 198 (N.D. Cal. 2019). Rather, it sells comprehensive, aggregated collections of raw and synthesized data designed to give its customers a "360-degree perspective" on the unique traits of millions of individual device

users. *Am. Compl.* ¶ 80, Dkt. 26. This alleged invasion of privacy—which is substantial both in quantity and quality—plausibly constitutes a "substantial injury" to consumers. *See Neovi, Inc.*, 604 F.3d at 1157 ("An act or practice can cause substantial injury by doing a small harm to a large number of people.") (internal quotation omitted).

Kochava emphasizes that its data only inferentially reveals information about device users. This Court previously noted that inferences based on geolocation data, alone, *can be* unreliable. *See Mem. Decision & Order* at 22–23, Dkt. 24. But that conclusion is less applicable to the allegations in the FTC's Amended Complaint. According to the FTC's new allegations, Kochava itself makes inferences about consumers, rather than simply providing raw data from which its customers could make inferences. *See Pl.'s Resp.* at 16–18, Dkt. 45. Moreover, those inferences are generally more reliable than inferences drawn solely from geolocation data. For example, data revealing a device user's daily use of an app specifically designed to track and manage cancer treatments leaves little to the imagination.

4. Conclusion

In sum, the FTC claims that Kochava sells vast amounts of "highly granular" personal information about millions of people in a format that is essentially non-anonymized. *Pl.'s Resp.* at 3, Dkt. 45. That data can reveal a person's political and

religious affiliations, sexual orientation, medical conditions, and much more. By selling that data, Kochava arguably invades consumers' privacy and exposes them to significant risks of secondary harms. Accordingly, the FTC has stated a plausible claim under Section 5(a) of the FTC Act, and the Court will deny Kochava's request to dismiss this case.

ORDER

IT IS ORDERED that Kochava's Motion to Dismiss First Amended Complaint Pursuant to Fed. R. Civ. P. 12(b)(6) (Dkts. 33 & 34) is **DENIED**.

DATED: February 3, 2024

B. Lynn Winmill
U.S. District Court Judge