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

This case is about mobile devices, location data, and privacy. The underlying dispute is whether the defendant, Kochava, Inc., is engaging in an "unfair . . . act or practice" by selling geolocation data that could enable third parties to track mobile device users to and from sensitive locations. At this early stage in the litigation, however, the Court must only decide whether the plaintiff, the Federal Trade Commission (FTC), has stated at least a plausible claim against Kochava.

Before getting into the legal issues, the Court will review the factual

allegations underlying the FTC's Complaint.[1]

BACKGROUND

Kochava, Inc. is a data analytics company that offers various digital marketing and analytics services. One of its services involves aggregating and selling data collected from billions of mobile devices across the world. Among other things, Kochava's data includes timestamped location coordinates and unique device identifiers which, viewed together, reveal the past movements of mobile devices.

1. Geolocation Data

Geolocation data is a broad term for information about a mobile device's geographical location. It may reveal where a device currently is, as with Global Position Systems (GPS), or it may only reveal where a device has been in the past. Real-time and historical geolocation data are used by various commercial and

[1] At this early stage in the litigation, the Court must assume the truth of the FTC's factual allegations. This does not mean, however, that the Court believes those allegations. Rather, the Court makes no determination whatever as to the truth or falsity of the factual assertions in the FTC's Complaint.

Relatedly, Kochava asks the Court to take judicial notice of the existence of three documents: (1) a 2014 FTC press release (Dkt. 7-3), (2) an FTC webpage (Dkt. 7-4), and (3) an article published by the Wall Street Journal (Dkt. 18-1). The Court grants these requests as proper under Federal Rule of Evidence 201(b). *Lee v. City of Los Angeles*, 250 F.3d 668, 689 (9th Cir. 2001).

governmental entities in many ways. Familiar uses include the use by emergency dispatch to track 9-1-1 callers and the use by cellphone applications that provide turn-by-turn driving directions and traffic alerts. A less visible but equally ubiquitous use of geolocation data is by data analytics companies who analyze consumer trends and develop targeted marketing strategies.

Kochava is one such data analytics company. It obtains geolocation data from third-party data brokers, such as app developers, who collect the data with consent directly from mobile device users. Kochava then aggregates the data in its proprietary data bank, called the Kochava Collective, and lets its paying customers access the data bank. The data bank contains data from "billions of devices globally" and includes around ninety-four billion coordinates per month, from thirty-five million daily active users, with each device generating an average of over ninety data points per day. *Compl.* ¶ 11, Dkt. 1. That means the location coordinates in the data bank reveal where each mobile device has been approximately every fifteen minutes.

Kochava does not, however, sell real-time location data. Instead, according to the FTC, Kochava's customers can only access "historical location data" collected during the seven days prior to the date they pay for access to the data bank. *Id.* ¶ 19. Thus, while Kochava's customers can see where a given mobile

device has been, they cannot see where a device presently is.

2. Mobile Advertising IDs ("MAIDs")

Mobile Advertising IDs (MAIDs) are unique alphanumeric names that operating systems, such as IOS and Android, assign to mobile devices. Acting as virtual fingerprints, MAIDs are also called "unique persistent identifiers" because they remain unchanged unless proactively reset by device users. *Id.* ¶ 10. In the context of data analytics, MAIDs are used to link a series of otherwise unconnected data points, such as geolocation coordinates, and, hence, reveal the movements of a particular device. In short, by associating data points with MAIDs, analytics companies can identify patterns among specific devices, group devices into categories, and develop targeted marketing campaigns based on that information.

According to the FTC, each set of location coordinates in Kochava's data bank is paired with a MAID. This linking of coordinates to MAIDs, the FTC claims, enables Kochava's customers to plot coordinates on a map and trace a particular device's movements, and in doing so, to "associate each set of coordinates with a specific consumer." *Id.* ¶¶ 8, 20–21. It is this practice of selling both geolocation coordinates and MAIDs that the FTC challenges in this lawsuit.

3. This Lawsuit

The FTC filed this action in August of 2022, seeking a permanent injunction barring Kochava from continuing its sale of "precise location data associated with unique persistent identifiers that reveal consumers' visits to sensitive locations." *Id.* ¶ 36. The Complaint focuses on two components of the data Kochava sells: timestamped geolocation coordinates and MAIDs. According to the FTC, by aggregating and selling both data points, together, without any technical controls to prevent tracking device users to sensitive locations, Kochava violates device users' privacy and exposes them to risks of secondary harm. In doing so, the FTC alleges, Kochava engages in an "unfair . . . act or practice" prohibited by Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1). To prevent Kochava from continuing to violate Section 5(a), the FTC seeks a permanent injunction under Section 13(b), 15 U.S.C. § 53(b).

Instead of filing an answer to the FTC's Complaint, Kochava seeks dismissal under Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief may be granted. Kochava's Motion to Dismiss (Dkt. 7) is fully briefed and the Court heard oral argument on February 21, 2023. As explained below, the Court will grant the motion to dismiss, but will allow the FTC to file an emended complaint in accordance with this Order.

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.

When a court dismisses a complaint under Rule 12(b)(6), it should generally allow the plaintiff to file an amended complaint unless the complaint clearly "could not be saved by any amendment." *Chang v. Chen*, 80 F.3d 1293, 1296 (9th Cir. 1996), overruled on other grounds by *Odom v. Microsoft Corp.*, 486 F.3d 541 (9th Cir. 2007); *see also* Fed. R. Civ. P. 15(a)(2).

ANALYSIS

The FTC's Complaint rests on two provisions of the Federal Trade Commission Act ("FTC Act"). First, Section 5(a) provides the underlying legal proscription the FTC seeks to enforce, prohibiting "unfair . . . acts or practices in or affecting commerce." 15 U.S.C. § 45(a). Second, Section 13(b) provides the

enforcement mechanism the FTC employs, authorizing it to seek injunctions in federal court whenever it "has reason to believe" that a person, partnership, or corporation "is violating, or is about to violate," a law enforced by the FTC. 15 U.S.C. § 53(b).

Kochava offers several reasons why the FTC has failed to make sufficient factual allegations to state a claim under Section 5(a) and 13(b). It also makes several constitutional arguments, asserting that even if the FTC made additional factual allegations, its claim would not survive. Ultimately, the Court agrees that the FTC's complaint lacks sufficient allegations to state a claim under Section 5(a). It is not clear, however, that the deficiencies cannot be cured. The Court will therefore dismiss the Complaint with leave to amend in accordance with this Order.

1. The FTC adequately alleges that it has reason to believe Kochava "is violating, or is about to violate," Section 5(a) of the FTC Act.

Under Section 13(b) of the FTC Act, the FTC may only seek injunctive relief when it "has reason to believe" that a defendant "is violating, or is about to violate, any provision of law enforced by the Federal Trade Commission." 15 U.S.C. § 53(b). In other words, the FTC cannot seek an injunction based only upon past conduct.

Kochava insists that the FTC is only challenging past practices. But in

reading the Complaint so narrowly, Kochava misses the forest for the trees. Although the Complaint does repeatedly reference a data sample that is no longer available, it is replete with present and present perfect tense language clearly alleging that Kochava continues to engage in the same practice of selling geolocation data without restrictions near sensitive locations. *See Compl.* ¶¶ 8, 9, 11, 23, 30, 33, 36, 37 & 39, Dkt. 1; *see also Jones v. Liberty Mut. Fire Ins. Co.*, Civil Action No. 3:04-CV-137-MO, 2008 WL 490584, at *2 (W.D. Ky. Feb. 20, 2008) ("The complaint . . . uses the present perfect tense which can communicate a continuing situation."). Read properly, the FTC's Complaint alleges that Kochava is actively selling location data in violation of the FTC Act. At this stage, that allegation suffices.[2]

2. The FTC need not allege a predicate violation of law or policy to state a claim under Section 5(a) of the FTC Act.

[2] Kochava's passing footnote reference to a new Privacy Block feature does not change the Court's conclusion on this point. It is "well-settled that an action for an injunction does not become moot merely because the conduct complained of was terminated, if there is a possibility of recurrence, since otherwise the defendants would be free to return to [their] old ways." *F.T.C. v. Affordable Media*, 179 F.3d 1228, 1237 (9th Cir. 1999) (internal quotation omitted) (emphasis in original). Kochava offers almost no information about its new Privacy Block feature, nor is it clear why implementation of this feature—a readily reversible step—makes it unlikely that Kochava will resume its former practices in the future. And, at any rate, more factual development is necessary to determine the impact the Privacy Block feature may have on the FTC's request for an injunction.

Kochava argues that, to sue under Section 5(a), the FTC must identify some "underlying predicate violation" of law or public policy. The Court disagrees because neither the statutory language nor case law support adding such an element to Section 5(a).

Congress enacted the FTC Act to prohibit "unfair" and "deceptive" business practices that harm competitors and consumers. If those terms seem broad, they are intentionally so. Indeed, Congress "explicitly considered, and rejected, the notion that it reduce the ambiguity . . . by enumerating the particular practices to which [Section 5(a)] was intended to apply." *F.T.C. v. Sperry & Hutchinson Co.*, 405 U.S. 233, 239–40 (1972) (citing S. Rep. No. 63-597, at 13 (1914)). Instead, Congress authorized the FTC to use its expertise in guiding the law's application and development in different contexts.

For the first eighty years after enacting the FTC Act, Congress remained mostly on the sidelines and let the FTC develop the meaning of unfairness through policy statements and agency adjudications. But in 1994, spurred by growing criticisms of the FTC's liberal use of Section 5(a), Congress amended the FTC Act and added Section 5(n) to limit the FTC's authority to deem acts and practices "unfair" under Section 5(a). FTC Act Amendments of 1994, Pub. L. No. 103-312, § 9, 108 Stat. 1691, 1695 (1994). Namely, Section 5(n) prohibits the FTC from

declaring an act or practice unfair unless "the act or practice [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."

Kochava now asks this Court to hold that an act or practice cannot be unfair under Section 5(a) unless it also violates some other existing law or public policy. For support, Kochava cites a recent Eleventh Circuit case: *LabMD, Inc. v. F.T.C.*, 894 F.3d 1221 (11th Cir. 2018). There, the FTC claimed that a medical laboratory engaged in an unfair act or practice by failing to implement adequate data-security measures. *Id.* at 1225. The lab responded, as Kochava does here, by arguing that the Section 5(a) claim must be dismissed because the FTC had not identified any underlying violation of law or public policy. *Id.* at 1227. The Eleventh Circuit agreed, concluding that "an act or practice's 'unfairness' must be grounded in statute, judicial decisions—*i.e.*, the common law—or the Constitution." *Id.* at 1229.[3] Based on that conclusion, the court foraged for some existing legal standard

[3] It is worth noting that other federal circuit courts have come to the opposite conclusion. In *F.T.C. v. Accusearch Inc.*, for example, the Tenth Circuit rejected the premise that "a practice cannot be an unfair one unless it violates some law independent of the FTCA" because "the FTCA imposes no such constraint." 570 F.3d 1187, 1194 (10th Cir. 2009). On the contrary, the court explained, "the FTCA enables the FTC to take action against unfair practices that have not yet been contemplated by more specific laws." *Id.*

to apply. Boiling the FTC's complaint down to its "gist," the court thought it "apparent" that the FTC was essentially claiming negligence. *Id.* at 1231. Applying the negligence standard, the court concluded that the FTC's complaint was sufficient to state a claim under Section 5(a). *Id*.

For two reasons, this Court declines Kochava's invitation to follow the Eleventh Circuit and add a predicate-violation requirement to Section 5(a). First, that approach is inconsistent with Ninth Circuit precedent. *See F.T.C. v. Amazon, Inc.*, Case No. C14-1038-JCC, 2016 WL 10654030, at *6 (W.D. Wash. July 22, 2016) ("The three-part test for whether a practice is 'unfair' under the FTC Act, found in the statute itself, is followed without embellishment by courts in this Circuit."). In at least two cases, the Ninth Circuit has identified the elements of a Section 5(a) unfairness claim by simply stating the three-part test set forth in Section 5(n). In *F.T.C. v. Neovi, Inc.*, for example, the court declared that "an unfair practice or act is one that" satisfies each of the three elements set forth in Section 5(n). 604 F.3d 1150, 1155 (9th Cir. 2010), *as amended* (June 15, 2010); *see also Davis v. HSBC Bank Nevada*, 691 F.3d 1152, 1168 (9th Cir. 2012) (same). The court did not reference any additional requirement for a predicate violation of

law or public policy.[4] Nor is this Court aware of any Ninth Circuit decision suggesting that such a requirement exists.

Second, the Eleventh Circuit's approach does not square with the text of the FTC Act. Neither Section 5(a) nor Section 5(n) makes any reference to underlying violations of existing law or policy. *Accusearch Inc.*, 570 F.3d at 1194 ("[T]he FTCA imposes no such constraint."). Congress easily could have added such a requirement when it enacted Section 5(n), but it did not. Instead, it specified that public policy may only serve as "evidence to be considered with all other evidence," but "may not serve as a primary basis," for deeming an act or practice unfair. 15 U.S.C. § 45(n). It is true that the three requirements set forth in Section 5(n) are written as negative limitations on the FTC's authority rather than as an exhaustive list of elements. *See F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 244 (3d Cir. 2015); *but see F.T.C. v. Walmart Inc.*, No. 22 CV 3372, 2023 WL 2646741, at *15–16 (N.D. Ill. Mar. 27, 2023). Nevertheless, what the statute

[4] Numerous district courts within the Ninth Circuit have also described the test under Section 5(a) as containing just three elements, without mentioning any requirement for an underlying violation of law or public policy. *See e.g.*, *F.T.C. v. Johnson*, 96 F.Supp.3d 1110, 1151 (D. Nev. 2015); *F.T.C. v. Elec. Payment Sol. of Am. Inc.*, 482 F.Supp.3d 921, 930 (D. Ariz. 2020); *F.T.C. v. LendingClub Corp.*, Case No.18-cv-02454-JSC, 2020 WL 2838827, at *21 (N.D. Cal. June 1, 2020); *Beaver v. Tarsadia Hotels*, 29 F.Supp.3d 1294, 1314–15 (S.D. Cal. July 2, 2014); *F.T.C. v. D-Link Systems, Inc.*, Case No. 3:17-cv-00039-JD, 2017 WL 4150873, at *5 (N.D. Cal. Sept. 19, 2017).

does definitively prohibit is courts giving mechanical deference to public policy in determining whether acts or practices are unfair. There is simply no support in the statutory text for imposing a predicate-violation requirement under Section 5(a).

In sum, to state a claim under Section 5(a), the FTC need not allege that Kochava's practices violate any underlying law or public policy. It must only allege that those practices (1) cause or are likely to cause substantial injury to consumers (2) that is unavoidable by consumers and (3) is not outweighed by countervailing benefits to consumers. 15 U.S.C. § 45(n).

3. The FTC need not allege that Kochava's practices are immoral, unethical, oppressive, or unscrupulous.

Kochava also argues that Section 5(a) of the FTC Act only prohibits acts and practices that are immoral, unethical, oppressive, or unscrupulous. For this proposition, Kochava relies on two decisions from the 1970s: *F.T.C. v. Sperry & Hutchinson Co.*, 405 U.S. 233 (1972) and *Spiegel, Inc. v. F.T.C.*, 540 F.2d 287 (7th Cir. 1976). But both cases relied upon a 1964 policy statement that the FTC later expressly abandoned in 1980. *Wyndham Worldwide Corp.*, 799 F.3d at 243–44 (citing *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984)). Moreover, as discussed above, neither the statutory text nor Ninth Circuit precedent supports adding elements to the standard set forth in Section 5(n). The FTC therefore need not

allege that Kochava's practices are immoral, unethical, oppressive, or unscrupulous in order to bring its Section 5(a) claim.

4. The FTC has not adequately alleged a likelihood of substantial consumer injury.

To state a claim under Section 5(a), the FTC must allege that Kochava's practices cause or will likely cause "substantial injury to consumers." 15 U.S.C. § 45(n). In its Complaint, the FTC advances two theories of consumer injury. First, it claims that Kochava's geolocation data sales could enable third parties to track consumers' past movements to and from 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. Second, the FTC claims that the disclosure of consumers' sensitive location information itself constitutes substantial injury to consumers' right to privacy. *Id.* ¶ 24.

The FTC's first theory of consumer injury is plausible: a company could substantially injure consumers by selling their sensitive location information and thereby subjecting them to a significant risk of suffering concrete harms at the hands of third parties. But here, the FTC has not alleged that consumers are suffering or are likely to suffer such secondary harms. It only alleges that secondary harms are theoretically possible. The FTC's second theory also fails, but

for a different reason: the purported privacy intrusion is not severe enough to constitute "substantial injury" under Section 5(n).

A. Theory #1: Increased Risk of Secondary Harms

As the FTC claims, ill-intentioned third parties could theoretically use Kochava's geolocation data to identify, track, and harm mobile device users who visit certain "sensitive locations." And by creating the risk of such harms, Kochava may indeed be inflicting a substantial injury on consumers within the meaning of Section 5(a) of the FTC Act. The problem, however, is that the FTC has not attached any degree of probability to those risks. Instead, the FTC claims only that secondary harms "could" occur as a result of Kochava's data sales.[5]

Section 5(n) requires the FTC to allege more than a mere possibility of consumer injury. Rather, the defendant's acts or practices must actually cause or be likely to cause injury. 15 U.S.C. § 45(n). That is not to say that the defendant must be the one actually inflicting the underlying harm on consumers. On the contrary, a defendant can "cause" substantial injury under Section 5(n) merely by creating "a

[5] *See Compl.* ¶¶ 20 ("may be used," "it is possible," "it is also possible," "may be used"), 21 ("it is possible"), 22 ("can be used," "can be inferred," "may identify," "may be used"), 24 ("may be used"), 25 ("may be used," "it is possible," "may also be used"), 26 ("could be used"), 27 ("could be used," "could reveal," "could be used"), 28 ("could be used," "could show"), Dkt. 1.

significant risk of concrete harm." *Neovi, Inc.*, 604 F.3d at 1157; *see also id.* at 1156 ("Courts have long held that consumers are injured for purposes of the Act not solely through the machinations of those with ill intentions, but also through the actions of those whose practices facilitate, or contribute to, ill intentioned schemes if the injury was a predictable consequence of those actions."). Here, Kochava arguably creates a foreseeable risk of concrete harm to consumers by aggregating and selling location coordinates and MAIDs which, together, enable third parties to identify and harm device users who visit certain sensitive locations. Yet the FTC's Complaint does no more than claim that such secondary harms are theoretically possible.

The FTC asks the Court to simply infer that consumer injury is probable from its assertion that Kochava is disclosing "sensitive information" about device users. To support such an inference, the FTC points to Ninth Circuit dicta noting that a hypothetical disclosure of "personal facts," such as one's "HIV status, sexual orientation, or genetic makeup," may "lead directly to injury, embarrassment or stigma." *In re Crawford*, 194 F.3d 954, 960 (9th Cir. 1999). But there is an important difference between the hypothetical disclosure of "personal facts" referenced by the Ninth Circuit and this case. Namely, that hypothetical assumes that the disclosed facts are, on their face, tied to particular individuals. That is not

true in our case: the FTC acknowledges that third parties must take additional steps to link Kochava's geolocation data to particular individuals. *See Compl.* ¶ 20, Dkt. 1. Accordingly, Kochava's disclosure of location data, alone, does not give rise to an inference 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. *Neovi, Inc.*, 604 F.3d at 1157.[6]

In sum, although the FTC's first legal theory of consumer injury is plausible, the FTC has not made sufficient factual allegations to proceed. To do so, it must not only claim that Kochava's practices *could* lead to consumer injury, but that they are *likely* to do so, as required by the statute.

B. Theory #2: Invasion of Privacy

The FTC's second theory of consumer injury raises two questions. First, can an invasion of privacy, alone, constitute "substantial injury" under Section 5(n) of the FTC Act? The Court concludes it can. And second, in this case, is the alleged

[6] The Northern District of California similarly required the FTC to include allegations of probability in *F.T.C. v. D-Link Systems, Inc.*, Case No. 3:17-cv-00039-JD, 2017 WL 4150873 (N.D. Cal. Sept. 19, 2017). There, the FTC brought a Section 5(a) unfairness claim against an internet service provider, claiming that deficiencies in its cybersecurity measures could theoretically enable third parties to commit data breaches. The court dismissed the claim because the FTC had alleged only a "mere possibility of injury at best." *Id.* at *5.

privacy intrusion sufficiently severe to constitute substantial injury to consumers? The Court concludes it is not.

(1) An invasion of privacy may constitute substantial injury under Section 5(n) of the FTC Act.

An act or practice is only unfair under Section 5(a) if it causes "substantial injury" to consumers. 15 U.S.C. § 45(n). The FTC claims that Kochava's data sales injure consumers by violating their privacy. The threshold question, then, is whether an invasion of privacy can constitute "substantial injury" within the meaning of Section 5(n).

Beginning with the plain language the statute, Section 5(n) is not limited to tangible injuries, such as monetary or physical harm. Instead, Congress simply used the word "injury," which is a term of art in the legal field that refers broadly to any "actionable invasion of a legally protected interest." *Injury*, BLACK'S LAW DICTIONARY (11th ed. 2019). "[W]hen Congress borrows terms of art in which are accumulated the legal tradition and meaning of centuries of practice, we presume that Congress knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was taken." *United States v. Ornelas*, 906 F.3d 1138, 1143 (9th Cir. 2018) (quoting *Carter v. United States*, 530 U.S. 255, 264 (2000)). Thus, based on the plain language of Section 5(n), any

tangible or intangible invasion of a legally protected interest may constitute "injury" within the meaning of Section 5(n).

Since our nation's founding, privacy has been a legally protected interest at the local, state, and federal levels. *See Patel v. Facebook, Inc.*, 932 F.3d 1264, 1271–72 (9th Cir. 2019) (quoting *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016)) ("Privacy rights have long been regarded 'as providing a basis for a lawsuit in English or American courts.'"); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) ("Violations of the right to privacy have long been actionable at common law."); *Stasi v. Inmediata Health Croup Cor.*, 501 F.Supp.3d 898, 909 (S.D. Cal. 2020) (collecting cases).[7]

More specifically, privacy protections against the disclosure of certain kinds of sensitive personal information are embedded in countless federal and state statutes, regulations, and common law doctrines. *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989) ("[B]oth the common

[7] The Ninth Circuit has also repeatedly held that privacy intrusions may constitute "concrete injury" for purposes of Article III standing. *See, e.g., Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1041–43 (9th Cir. 2017) (finding "concrete injury" where plaintiffs claimed that unsolicited telemarketing calls "invade the privacy and disturb the solitude of their recipients"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020) (finding "concrete injury" where Facebook allegedly tracked users' "personally identifiable browsing history" on third party websites); *Patel*, 932 F.3d at 1275 (finding "concrete injury" where plaintiffs claimed Facebook's facial-recognition technology violated users' privacy rights).

law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."). To name just a few: tort law in many states allows lawsuits based on the public disclosure of private facts; a host of federal statutes and regulations forbid the unauthorized disclosure of personal health information, *see, e.g.*, Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 201 *et seq.*; numerous federal statutes protect internet users' privacy, *see, e.g.*, Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6505; and the Fourth Amendment to the United States Constitution bars the federal government from violating reasonable expectations of privacy, *see Carpenter v. United States*, 138 S.Ct. 2206, 2217–18 (2018). In short, privacy is—and has always been—a legally protected interest in many contexts, including specifically with regard to sensitive personal information.

Stepping back and connecting the dots, then: if injury is the invasion of a legally protected interest, and privacy is a legally protected interest, then an invasion of privacy may constitute injury. Thus, under the plain language of the FTC Act, a defendant whose acts or practices violate consumer privacy may be said to inflict an "injury" upon consumers within the meaning of Section 5(n).

Looking beyond the statutory text, neither legislative history nor case law contradicts the plain meaning of Section 5(n). *See F.T.C. v. Roca Labs, Inc.*, 345

F.Supp.3d 1375, 1395 (M.D. Fla. 2018) ("[N]either the legislative history nor the current law requires proof of tangible harm to the exclusion of intangible harm."). As the Ninth Circuit has explained, consumer injury can occur in "a variety of ways." *Neovi, Inc.*, 604 F.3d at 1156. Thus, although Congress has noted that consumer injury often involves monetary harm, and that mere "[e]motional impact and other more subjective types of harm" are ordinarily insufficient, these generalizations do not limit Section 5(n)'s reach only to tangible harms. S. Rep. No. 103-130, at 13, 1993 WL 322671 (1993). If Congress had intended such a limitation, it could have easily included one in the statute.

Neither the text of Section 5(n), the legislative history, nor case law indicates that a severe invasion of privacy cannot constitute substantial injury giving rise to liability under Section 5(a) of the FTC Act.

(2) The alleged privacy intrusion is not sufficiently severe to constitute substantial injury.

The next question is whether the privacy intrusion alleged by the FTC constitutes substantial injury to consumers. The Court concludes it does not.

The FTC claims that Kochava's data sales reveal "sensitive and private characteristics of consumers" and therefore "pose an unwarranted intrusion into the most private areas of consumers' lives." *Compl.* ¶¶ 24 & 29, Dkt. 1. It explains that "much can be inferred about the mobile device owners" by plotting their devices'

timestamped location coordinates on a map. For example, using publicly available services like Google Maps, anyone with access to Kochava's data feeds can determine where a given device user lives, works, worships, and seeks medical treatment. *Id.* ¶ 22. To illustrate, using data it obtained from one of Kochava's free data samples, the FTC identified a particular device user who visited a women's reproductive health clinic, spent nights at a certain residence, and visited another location on at least three evenings in the same week. *Id.* ¶ 25.

The privacy concerns raised by the FTC are certainly legitimate. Disclosing where a person has been every fifteen-minutes over a seven-day period could undoubtedly reveal information that the person would consider private, such as their travel habits, medical conditions, and social or religious affiliations. Be that as it may, the Court's job is to apply the law as it is, regardless of whether the Court thinks the law is too strict or not strict enough. The FTC Act only prohibits acts and practices that cause "substantial injury" to consumers. Where, as here, a privacy intrusion is the alleged injury, the Court must determine whether the privacy intrusion is sufficiently severe to constitute "substantial" injury.

Here, at least three factors lessen the severity of the alleged privacy injury. First, the data Kochava sells is not, on its face, sensitive or private. On the contrary, any private information that is revealed in Kochava's data bank can be

ascertained only by inference. But inferences are often unreliable. For example, geolocation data showing that a device visited an oncology clinic twice in one week could reveal that the device user suffers from cancer. Or it may instead reveal that the person has a friend or family member who suffers from cancer. Or that the person is a pharmacist or is in the business of selling or maintaining medical devices. The point is that the FTC does not actually claim that Kochava is disclosing private information, but rather that it is selling data from which private information might be inferred. Although this distinction does not eliminate all the privacy concerns voiced by the FTC in this lawsuit, it does lessen the severity of the alleged privacy injury.

Second, the information that can be inferred from Kochava's geolocation data is generally accessible through other, lawful means. A third party may, for example, observe a person's movements on public streets and sidewalks as they go to and from home or a medical facility. A third party may also discover a person's home address by reviewing publicly accessible property records. Privacy interests in the kind of location data Kochava sells are therefore weaker than, for example, privacy interests in confidential financial or medical information which is not otherwise publicly accessible. *See, e.g., Wyndham Worldwide Corp.*, 799 F.3d at 240.

Finally, the FTC has not even generally indicated how many device users may suffer privacy intrusions. This omission is important because the substantiality of a consumer injury depends, in part, on the number of consumers injured. *Neovi, Inc.*, 604 F.3d at 1157 (internal quotation omitted) ("An act or practice can cause substantial injury by doing a small harm to a large number of people."). The FTC concedes that Kochava's geolocation data can only be linked to particular device users if third parties take additional steps—steps requiring access to external, or "offline," information. But a consumer whose geolocation data is used only for analytics but never tied back to him cannot be said to have suffered any privacy injury. Ultimately, the FTC claims only that third parties *could* tie the data back to device users; not that they have done so or are likely to do so.

Although an invasion of privacy could theoretically constitute consumer injury under Section 5(a), the intrusion alleged by the FTC is not sufficiently severe to constitute "substantial" injury.

C. Conclusion

In sum, the FTC's first theory of consumer injury is plausible, but the FTC has not adequately alleged that Kochava's data sales "cause or are likely to cause" the purported secondary harms. Put another way, the FTC has not alleged that Kochava's practices create a "significant risk" of concrete harm. *Id.* at 1157. This

deficiency may, however, be cured through additional factual allegations in an amended complaint. The FTC's second theory of consumer injury fails because It has not adequately alleged how the privacy intrusion creates a "substantial injury" to consumers. Although the Court is somewhat skeptical that this deficiency can be cured through an amended complaint, it will give the FTC an opportunity to try. The Court will therefore dismiss the Complaint but give the FTC an opportunity to file an amended complaint in accordance with this Order.[8]

5. The FTC has adequately alleged that the purported injury is unavoidable by consumers themselves and not outweighed by countervailing benefits.

To state a claim under Section 5(a), the FTC must also allege that the consumer injury is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits. *See* 15 U.S.C. § 45(n). Kochava challenges the sufficiency of the Complaint on both grounds.

First, "[i]n determining whether consumers' injuries were reasonably avoidable, courts look to whether the consumers had a free and informed choice." *Neovi, Inc.*, 604 F.3d at 1158. The FTC claims that Kochava's "collection and use" of consumers' location data is "opaque to consumers" who "have never heard of or

[8] Because the FTC is granted leave to amend, the Court will address Kochava's remaining arguments for dismissal.

interacted with" Kochava and have "no insight into how Kochava uses their data." *Compl.* ¶ 31, Dkt. 1. Conceding that device users initially consent to the collection of their data by other companies, the FTC claims that consumers are nevertheless unaware that their data will be aggregated, linked to MAIDs, and sold to the public. At this stage, the FTC has adequately alleged that consumers lack the information necessary to make informed choices and avoid the harms allegedly caused by Kochava's practices.

Second, in conducting the cost-benefit analysis under Section 5(n), courts consider "the potential costs that the proposed remedy would impose on the parties and society in general." *Am. Fin. Servs. Ass'n v. F.T.C.*, 767 F.2d 957, 975 (D.C. Cir. 1985). Here, the FTC seeks only an injunction requiring Kochava to "implement safeguards to remove data associated with sensitive locations from its data feeds." *Compl.* ¶ 32, Dkt. 1. Kochava responds by emphasizing the societal benefits of geolocation data, generally, but overlooks the narrowness of the FTC's requested remedy, which would only bar the disclosure of coordinates near certain "sensitive locations."[9] At this stage, the FTC has adequately alleged that the

[9] Kochava also argues that the terms of the FTC's requested injunction are "vague and uncertain on [their] face." *Def.'s Memo. in Supp.* at 21, Dkt. 7-1. But at this stage, the Court must only determine whether the FTC has stated a plausible claim against Kochava. The precise terms of the injunction—if the FTC ultimately obtains one—is a matter for another day.

purported injury to consumers is not outweighed by the countervailing benefits of that relatively narrow subset of data.

6. Kochava had fair notice that unrestricted sales of geolocation data could fall within Section 5(a) of the FTC Act.

"A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required." *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). This principle, grounded in the concept of due process, is violated whenever a law "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." *Id.* at 253 (quoting *United States v. Williams*, 553 U.S. 285, 304 (2008)).[10]

Kochava claims it lacked fair notice that its sale of geolocation data without restrictions near sensitive locations could violate Section 5(a) of the FTC Act. In response, the FTC correctly points out that the standard for fair notice is especially low in cases, like this one, involving civil statutes regulating economic activities.

---

[10] The standard for fair notice varies depending on whether an agency is enforcing its own regulation, filling statutory gaps, or simply enforcing a statute, as written. *Wyndham Worldwide Corp.*, 799 F.3d at 250–53. Here, the FTC seeks to enforce Section 5(a) of the FTC Act, as written. The Court will therefore apply the ordinary fair notice standard governing civil statutes that regulate economic activities.

Such laws are only void for vagueness if they create a standard "so vague and indefinite as really to be no rule or standard at all." *Boutilier v. INS*, 387 U.S. 118, 123 (1967). A statute is not overly vague, however, if it "prohibits conduct according 'to an imprecise but comprehensible normative standard.'" *Botosan v. Paul McNally Realty*, 216 F.3d 827, 836 (9th Cir. 2000) (quoting *Coates v. City of Cincinnati*, 402 U.S. 611, 614 (1971)).

Section 5(a)'s prohibition of "unfair and deceptive acts or practices" is not an island of its own. If it were, Kochava's void-for-vagueness argument might hold more water. On the contrary, Congress limited the meaning of the term "unfair" in 1994 when it added Section 5(n) to the FTC Act, which sets forth the three elements discussed above.[11] Admittedly, Section 5(n) is somewhat imprecise, using undefined terms like "substantial injury," "reasonably avoidable," and "countervailing benefits." Nevertheless, it is comprehensible and sets forth a normative cost-benefit analysis for companies to use in assessing their compliance with the law. *See Wyndham Worldwide Corp.*, 799 F.3d at 255; *see also Sperry &*

[11] Additionally, for more than a century, federal courts have been clarifying the meaning of Section 5(a)'s prohibition of "unfair or deceptive acts or practices." *C.F.P.B. v. D & D Mktg*, Case No. CV 15–9692 PSG (Ex), 2016 WL 8849698, at *6 (C.D. Cal. Nov. 17, 2016) ("The FTCA is now more than a century old and Courts have given shape to the meaning of its ban on 'unfair or deceptive acts or practices.'").

Hutchinson Co., 405 U.S. at 244; *Walmart Inc.*, 2023 WL 2646741, at *22–24. Ultimately, applying the standard set forth in Section 5(n), Kochava could have reasonably foreseen that selling substantial quantities of precise geolocation data without restrictions near sensitive locations could be construed as injurious—and therefore unfair—to consumers.[12]

Indeed, even the 2014 FTC press release that Kochava offers as an exhibit bolsters this conclusion. FTC Testifies on Geolocation Privacy, *Exhibit A*, Dkt. 7-3. That release, published in June of 2014, highlighted "concerns raised by the tracking of information about consumers' location," reiterated that the FTC is "the federal government's leading privacy enforcement agency," and confirmed that the FTC had already "used its enforcement authority under Section 5 of the FTC Act to take action against companies engaged in unfair or deceptive practices involving geolocation information." *Id.* at 1. If anything, that press release provided Kochava with additional notice that unrestricted sales of geolocation data and associated MAIDs could be construed as violating the FTC Act.

---

[12] Kochava cites a 2012 White House release on Consumer Data Privacy which directed that "data brokers and other companies that collect personal data without direct consumer interactions . . . should seek innovative ways to provide consumers with effective individual control." The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting privacy and Promoting Innovation in the Global Digital Economy*, Feb. 23, 2021, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf. The Court is not persuaded that this release lends any support to Kochava's fair notice argument.

In sum, given the low bar for fair notice in this context and the comprehensible standard set forth in sections 5(a) and 5(n) of the FTC Act, Kochava had fair notice.

7. Section 13(b) of the FTC Act does not violate the separation of powers.

Kochava next argues that Section 13(b) of the FTC Act violates the separation of powers by giving executive litigation authority to an agency whose members are not removable at-will by the president. The Court rejects Kochava's position for two reasons. First, the Ninth Circuit has squarely rejected this argument and upheld the constitutionality of Section 13(b). And second, even if the FTC Act's removal protections did violate the separation of powers, invalidating Section 13(b) would not be the proper remedy.

The power to enforce the law is vested in the President of the United States. U.S. CONST. art. II, § 1. But because one person cannot be everywhere at once, it is "expected that the President w[ill] rely on subordinate officers for assistance." *Seila Law LLC v. C.F.P.B.*, 140 S.Ct. 2183, 2191 (2020). To ensure that the buck stops in the oval office, however, the president generally has "the authority to remove those who assist him [or her] in carrying out his [or her] duties." *Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 513–14 (2010).

One notable exception to the president's removal power was carved out in

Humphrey's Executor v. United States, 295 U.S. 602 (1935). There, the United States Supreme Court upheld the constitutionality of Congress's for-cause removal protections for officers of the multi-member FTC who performed "quasi-legislative" and "quasi-judicial" functions. *Id.*

Kochava asserts that, since the time *Humphrey's Executor* was decided in 1935, Congress has expanded the FTC's toolbelt to include quintessentially executive powers. Namely, a 1973 amendment added Section 13(b) which authorizes the FTC to enforce the FTC Act by seeking injunctive relief in federal court. In passing that amendment, Kochava argues, Congress impermissibly granted executive enforcement power to an agency governed by officials who are not removable at-will by the president. As a result, Kochava contends, the FTC no longer falls within the narrow exception carved out in *Humphrey's Executor*.

For support, Kochava relies primarily upon a recent Supreme Court decision involving the president's power to remove the director of the Consumer Financial Protection Bureau (CFPB). *Seila Law LLC*, 140 S.Ct. 2183. In *Seila Law LLC v. C.F.P.B.*, the Court determined that the exception outlined in *Humphrey's Executor* did not apply to the CFPB due to several important differences between the single director of the CFPB and the multi-member commission governing the

1935-era FTC.[13] Kochava would have this Court follow the same path by distinguishing the modern-day FTC from the 1935-era FTC. For two reasons, however, the Court will not do so.

First, Ninth Circuit precedent forecloses Kochava's position. In *FTC v. American National Cellular*, the Ninth Circuit took up precisely the question raised here: whether Section 13(b) violates the "constitutional principle of separation of powers." 810 F.2d 1511, 1513 (9th Cir. 1987). The court concluded that "the FTC's current power to seek injunctive relief pursuant to section 13(b) does not so materially differ from the power to seek cease and desist orders as to render *Humphrey's Executor* inapposite. We hold, therefore, that the enforcement provisions of the Act are constitutional, under *Humphrey's Executor*." *Id.* at 1514. Ultimately, although the Supreme Court expressed some skepticism toward *Humphrey's Executor* in *Seila Law*, this Court is not persuaded that *Seila Law* invalidates the Ninth Circuit's clear holding in *American National Cellular*.[14]

---

[13] It is important to note, however, that although the *Seila Law* Court emphasized the limited scope of *Humphrey's Executor*, the Court expressly refrained from overruling that decision. *Id.* at 2192.

[14] It is also worth noting that both the U.S. Supreme Court and Ninth Circuit have recently entertained lawsuits by the FTC under Section 13(b). *AMG Capital Management, LLC v. F.T.C.*, 141 S.Ct. 1341 (2021); *F.T.C. v. Elegant Solutions, Inc.*, No. 20-55766, 2022 WL (Continued)

Kochava's argument also fails because the requested remedy—invalidation of Section 13(b)—would not follow even if the FTC Act did violate the separation of powers. When removal protections for federal officials violate the separation of powers, courts first ask whether the removal provisions are severable from the remainder of the statute. If severable, those provisions are invalidated while the remainder of the statute—including the grant of agency authority—survives. *See, e.g.*, *Seila Law LLC*, 140 S.Ct. at 2192 (striking only the removal provision of the statute); *Collins v. Yellen*, 141 S.Ct. 1761, 1787–88 & n.23 (2021). The FTC Act's removal provision, 15 U.S.C. § 41, is severable from the remainder of the FTC Act by virtue of the separability clause set forth in Section 17, 15 U.S.C. § 57. *See Walmart Inc.*, 2023 WL 2646741, at *26.[15] Therefore, even if the removal clause violated the separation of powers, the FTC's authority to bring this lawsuit would not be affected.

8. The nondelegation and major questions doctrines do not apply.

2072735, at *2 (9th Cir. June 9, 2022) (affirming the grant of injunctive relief under § 13(b)). Although neither court specifically took up the question of whether the FTC's structure violates the separation of powers, these cases indirectly reinforce the continued vitality of Section 13(b) after *Seila Law*.

[15] Even without the severability clause, the removal provisions of the FTC Act would be severable because the remaining portions of the Act are capable of "functioning independently," and there is no reason to believe that Congress "would have preferred no board at all to a Board whose members are removable at will." *Free Enter. Fund*, 561 U.S. at 509.

Finally, Kochava argues that Section 5(a) of the FTC Act is unconstitutional under both the nondelegation doctrine and the major questions doctrine. At their core, both doctrines limit the amount of legislative authority delegated by Congress to administrative agencies. But neither doctrine applies here.

First, "[t]he nondelegation doctrine bars Congress from transferring its *legislative* power to another branch of Government." *Gundy v. United States*, 139 S.Ct. 2116, 2121 (2019) (emphasis added). It does not, however, limit Congress in granting agencies the authority to seek judicial enforcement of the laws they administer. *See United States v. Bruce*, 950 F.3d 173, 175 (3d Cir. 2020) ("[T]he non-delegation doctrine applies only to delegations by Congress of legislative power; it has no application to exercises of executive power."). Here, the FTC is simply asking a court to interpret and apply a statute, as written. Consequently, there is no relevant delegation of legislative authority to which the Court could apply nondelegation principles.[16]

Relatedly, the major questions doctrine requires "Congress to speak clearly

[16] Even if the FTC's lawsuit was construed as an attempt to "make law" through litigation, the nondelegation doctrine would not require dismissal of this action. When delegating legislative powers, Congress must only provide a "general policy" and "boundaries of . . . authority." *United States v. Melgar-Diaz*, 2 F.4th 1263, 1266–67 (9th Cir. 2021). Section 5(n) of the FTC Act provides both.

if it wishes to assign to an agency decisions of vast 'economic and political significance.'" *Mayes v. Biden*, No. 22-15518 (9th Cir. Apr. 19, 2023) (slip op. at 23) (quoting *Util. Air. Regul. Grp. v. EPA*, 573 U.S. 302, 324 (2014)). As with the nondelegation doctrine, the objective is to avoid "an enormous and transformative expansion in . . . regulatory authority without clear congressional authorization." *Id.* at 23. But here, the FTC is not flexing its regulatory muscles—it is merely asking a court to interpret and apply a statute enacted by Congress. Accordingly, this doctrine, too, is inapplicable.

ORDER

IT IS ORDERED that Defendant's Motion to Dismiss (Dkt. 7) is **GRANTED with leave to amend.** Plaintiff shall file an amended complaint, if at all, within 30 days after entry of this Memorandum Decision and Order.

DATED: May 4, 2023

B. Lynn Winmill
U.S. District Court Judge