UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

DAVID GREENLEY,

Plaintiff,

v.

KOCHAVA, INC.,

Defendant.

Case No. 22-cv-01327-BAS-AHG

ORDER:

1. **GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS (ECF No. 11); AND**

2. **DENYING DEFENDANT'S MOTION FOR VENUE TRANSFER (ECF No. 21)**

Pending before the Court are two motions. First, Defendant moves to dismiss the action pursuant to Federal Rule of Civil Procedure ("Rule") 12(b)(1), asserting a lack of standing, and Rule 12(b)(6), asserting a failure to state a claim upon which relief may be granted. (MTD, ECF No. 11.) Second, Defendant moves to transfer venue pursuant to 28 U.S.C. § 1404(a). (Mot. Venue, ECF No. 21.) Having considered the parties' filings, the Court **GRANTS IN PART** and **DENIES IN PART** Defendant's Motion to Dismiss (ECF No. 11) and **DENIES** Defendant's Motion for Venue Transfer (ECF No. 21).

BACKGROUND

I. Factual Background

Defendant is a "data broker[]" that provides a software developer kit ("SDK") to software application ("app") developers "to assist them in developing their apps." (Am. Compl. ¶ 6, ECF No. 10.)[1] In return, the app developers allow Defendant to "surreptitiously intercept location data" from an app user ("user") via its SDK. (*Id.*) Defendant then sells "customized data feeds to its clients"—such as Airbnb, Disney+, and Kroger—to "assist in advertising and analyzing foot traffic at stores or other locations." (*Id.* ¶¶ 7, 83.) In other words, Defendant coded its SDK for data collection and embedded it in third-party apps; the SDK secretly collected app users' data; and then Defendant packaged that data and sold it to clients for advertising purposes.

Defendant is "able to deliver targeted advertising . . . by in essence 'fingerprinting' each unique device and user, as well as connecting users across devices and devices across users." (*Id.* ¶ 75.) The data links longitude and latitude coordinates with these fingerprints, which can be "easily de-anonymized." (*Id.* ¶¶ 7–8.) In addition to geolocation, Defendant collects "search terms, click choices, purchase decisions and/or payment methods." (*Id.* ¶ 125.) This data collection allows Defendant to deliver "targeted advertising . . . while tracking [users'] locations, spending habits, and personal characteristics" and share this "rich personal data simultaneously with untold numbers of third-party companies." (*Id.* ¶ 75.)

Plaintiff is a California resident filing a putative class action suit on behalf of similarly situated California residents. (*Id.* ¶¶ 1, 35.) Plaintiff has installed and used apps that have integrated Defendant's SDK. (*Id.* ¶¶ 36–37.) As a result, Defendant has collected "personal information," geolocation data, and communications from his cellular telephone. (*Id.* ¶ 23.) This geolocation data includes visits to "sensitive locations." (*Id.*

[1] These facts are taken from the Amended Complaint. The Court accepts as true all nonconclusory allegations set forth therein for the purpose of the Motion to Dismiss. *See Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004).

¶ 24.) Other data includes advertisement clicks; "specific communications from [] SDK-installed apps such as consumer's usernames, customer emails and customer IDs on their Apple or Android cellular telephone devices"; "search terms used by a device user"; and "a user's activities within an app after it has been installed." (*Id.* ¶¶ 76, 78–80.)

Plaintiff avers Defendant's own conduct and statements demonstrate its wrongdoing. In response to pressure from the Federal Trade Commission ("FTC"), Defendant announced a "new feature that allegedly now blocks the gathering of private, sensitive, location data related to health care facilities." (*Id.* ¶ 105.) This "Privacy Block" removes "health services location data from the Kochava Collective marketplace." (*Id.*) Plaintiff claims this new feature evidences that "Defendant recognizes the damage it has done to California consumers." (*Id.*)

In addition, Plaintiff alleges that Defendant has circumvented attempts to safeguard users' privacy. (*Id.* ¶¶ 71–73.) For example, Apple, Inc. ("Apple"), in response to growing privacy concerns, created a framework that requires users to "affirmatively opt-in to allowing Defendant and others to track their device unique identification number for advertisers on their iPhones." (*Id.* ¶¶ 68–69.) After Apple implemented this framework, Defendant advertised that it collects identifying data "even after a consumer thinks [he has] disabled all tracking by apps on an iPhone." (*Id.* ¶ 73.)

II. Litigation Background

On August 12, 2022, Defendant filed a federal lawsuit against the FTC in the District of Idaho. (Ex. A to Mariam Decl., ECF No. 21-4.) Defendant sought declaratory relief that it did not violate any laws. (*Id.*) On August 29, 2022, the FTC filed a Complaint against Defendant also in the District of Idaho. (Ex. B to Mariam Decl., ECF No 21-5.) One week later, Plaintiff filed this lawsuit against Defendant. (ECF No. 1.) Plaintiff alleges violations of the California Constitution, California Computer Data Access and Fraud Act ("CDAFA"), California Invasion of Privacy Act ("CIPA"), California Unfair Competition Law ("UCL"), and common law principles of unjust enrichment. (Am. Compl.) Defendant then filed the present Motion to Dismiss. (MTD.)

Five months after Plaintiff filed his Complaint in this district, Cindy Murphy, a Washington resident, filed a putative class action against Defendant in the District of Idaho alleging unjust enrichment and violations of the Washington Consumer Protection Act. (Ex. C to Mariam Decl., ECF No. 21-6.) After Ms. Murphy filed her lawsuit, Defendant filed the present Motion to Change Venue in this action. (Mot. Venue.)

STANDING

I. Legal Standard

Article III of the Constitution limits federal courts' jurisdiction to the "resolution of 'Cases' and 'Controversies.'" *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021). This limitation means the plaintiff must have standing to sue. *Id.* A plaintiff establishes standing by showing (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief. *Id.* (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992)).

Under Rule 12(b)(1), a party may move to dismiss a claim based on lack of subject matter jurisdiction, including the absence of standing. *Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1123 (9th Cir. 2010). A Rule 12(b)(1) challenge to jurisdiction may be facial or factual. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). Defendant's Motion to Dismiss is facial, positing the allegations in the complaint itself are insufficient to invoke federal jurisdiction. *See id.* at 1039; (MTD.) As a result, the presumption of truthfulness attaches to the allegations in the complaint, and the court is limited to the four corners of the pleading in determining whether it has jurisdiction over the matter. *Thornhill Publ'g Co. v. Gen. Tel. Elec.*, 594 F.2d 730, 733 (9th Cir. 1979). To survive a Rule 12(b)(1) facial challenge, "the plaintiff must 'clearly . . . allege facts demonstrating' each element [of standing]." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

II. Analysis

Defendant asserts Plaintiff fails to plausibly allege any of the standing requirements—injury in fact, causation, and redressability. The Court analyzes each prong and concludes that Plaintiff has adequately pled all three.

A. Injury in Fact

"To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). A "concrete" injury "must be '*de facto*'; that is, it must actually exist." *Id.* at 340 (citing Black's Law Dictionary 479 (9th ed. 2009)). Although "the most obvious" concrete harms are tangible—e.g., physical or monetary, "various intangible harms can also be concrete." *TransUnion*, 141 S. Ct. at 2204. These include injuries "with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," such as "reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.*

"A right to privacy 'encompass[es] the individual's control of information concerning his or her person.'" *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 598 (9th Cir. 2020) (quoting *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017)). Violations of this right fall into the category of traditionally recognized harms. *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019) (recognizing the "common law roots of the right to privacy"). As a result, intrusions into privacy can constitute an injury in fact.

The Ninth Circuit's recent opinion in *In re Facebook* is instructive. 956 F.3d 589. The issue was whether Facebook-users had standing to sue Facebook, Inc. ("Facebook") for tracking their browsing histories after they had logged out of Facebook. *Id.* at 595–96. The Ninth Circuit reasoned that Facebook's practices enable it to "amass a great degree of personalized information . . . without affording users a meaningful opportunity to control or prevent the unauthorized exploration of their private lives." *Id.* at 599. Quoting

the Third Circuit, the Ninth Circuit conclusively rejected the argument that the collection of private data is not an injury in fact: "In an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collected private data . . . is untenable." *Id.* (quoting *In re: Google Inc. Cookie Placement Consumer Priv. Litig.*, 934 F.3d 316, 325 (3d Cir. 2019)). For this reason, the Ninth Circuit upheld standing. *Id.* at 598–99.

Here, Plaintiff alleges Defendant collected his personal information in violation of the California Constitution and various California statutes. (Am. Compl. ¶ 1.) Among the collected data are his "geolocation, . . . communications related to his personal characteristics, mode of living, purchase decisions, personal choices, app selections, spending habits, and click choices." (*Id.* ¶ 38.) As in *In re Facebook*, Plaintiff's inability to "control or prevent the unauthorized exploration" of his private affairs is the root of the alleged injury. *See* 959 F.3d at 599. Thus, on first blush, the Court finds no pleading deficiencies.

Defendant counters with three arguments: the Amended Complaint fails to allege (1) that Defendant's actions affected Plaintiff in particular, (2) that the collection of data diminished the economic value of Plaintiff's data, and (3) that there was a lack of consent to data collection. (MTD 19–23.) None is persuasive.

First, the Complaint plausibly alleges Defendant collected Plaintiff's data. To be sure, Plaintiff's injury must be "specific to [him]." *See Gaos v. Google Inc.*, No. 5:10-cv-4809 EJD, 2012 WL 1094646, at *3 (N.D. Cal. Mar. 29, 2012). There is, in other words, no standing if Plaintiff fails to allege that Defendant collected *his* data. But in this case, the Complaint adequately pleads an injury specific to him. The Complaint alleges, "Defendant openly acknowledges that its software development kit (SDK), made available to and inserted by other companies as a plug-in to their own smartphone applications, intercepts and reads massive amounts of consumer data using its technology in order to identify unique consumers and report on their travel and habits for marketing,

verification, and other purposes." (Am. Compl. ¶ 67.) Plaintiff further alleges that he "owns, carries, and regularly uses a cellular device that contains Defendant's Kochava monitoring and intercepting SDK" embedded in apps (*id.* ¶ 36); "regularly uses his cell phone to access these application(s) in which Defendant utilizes its embedded SDK to track his geolocation, and to monitor and intercept communications" (*id.* ¶ 38); and "did not know until recently that his purchase decisions, his movements, and his locations, were being tracked by Defendant to market, sell, and advertise to him" (*id.* ¶ 40). This is enough for the Court to reasonably infer that Defendant collected and sold Plaintiff's data.

Second, there is no constitutional requirement that Plaintiff demonstrate lost economic value. Indeed, the Ninth Circuit explicitly rejected this argument in *In re Facebook*, reversing the lower court's holding to the contrary. 959 F.3d at 599. The Ninth Circuit reasoned, "California law recognizes a right to disgorgement of profits resulting from unjust enrichment, even where an individual has not suffered a corresponding loss." *Id.* Because California law recognizes "an entitlement to unjustly earned profits," to establish standing, plaintiffs must only establish a stake in the profits garnered from their personal data and that it is unjust for the defendant to retain those profits. *Id.* at 600. Plaintiff here does so. The Amended Complaint alleges, "Plaintiff and members of the Class conferred a benefit on Defendant through the use and dissemination of Plaintiff's and Class members' personal information, geolocation data, and communications . . . which Defendant used and disseminated for its own monetary benefit." (Am. Compl. ¶¶ 237–38.) Thus, under Ninth Circuit precedent, Plaintiff has carried his pleading burden.[2]

[2] Some of Plaintiff's claims may require an economic injury as an element of the claim, but such a "statutory standing" requirement does not eliminate constitutional standing. *See Salmon Spawning & Recovery All. v. Gutierrez*, 545 F.3d 1220, 1225 (9th Cir. 2008) ("If a plaintiff has shown sufficient injury to satisfy Article III, but has not been granted statutory standing, the suit must be dismissed under Federal Rule of Civil Procedure 12(b)(6), because the plaintiff cannot state a claim upon which relief can be granted."). As a result, statutory standing elements are not relevant to Defendant's Rule 12(b)(1) challenge. Additionally, the Court notes that Defendant's citation to CIPA is misleading. Defendant

Third, Plaintiff alleges he did not consent to Defendant's collection of his data. Defendant argues that users consented to its data practices in two ways: (1) they consented to sharing their location with a third-party app developer when they downloaded the application and (2) they failed to opt-out by contacting Defendant and requesting data deletion. (MTD 18, 23.) Neither constitutes consent.

To begin, Defendant's argument requires the Court to make inferences in its favor. The Amended Complaint does not directly allege that Plaintiff consented to sharing his location with a third-party app developer or that he had the opportunity to opt out of location sharing. Rather, Plaintiff copies and pastes FAQ-type information from Defendant's website into the Amended Complaint:

> **Can data be deleted upon request?**
> User data may be deleted from Kochava, so long as the request comes directly from the user.

(*Id.* ¶ 67.) And Plaintiff includes a section of Defendant's complaint against the FTC:

> Even if an injury to the consumer did indeed occur, it is reasonably avoidable by the consumer themselves by way the opt-out provision to allow the data collection. In other words, the consumer agreed to share its location data with an app developer. As such, the consumer should reasonably expect that this data will contain the consumer's locations, even locations which the consumer deems is sensitive.

(*Id.* ¶ 104.) On a facial challenge to standing, the Court must draw all reasonable inferences in favor of the non-moving party. *See Wolfe v. Strankman*, 392 F.3d 358, 362

---

points out that CIPA allows "[a]ny person who has been injured" to recover damages and suggests that this language requires economic loss. (MTD 20.) But Defendant cherry-picks the language. The statute specifically provides, "It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." Cal. Penal Code § 637.2.

(9th Cir. 2004). Thus, the Court accepts that, as alleged in the Amended Complaint, Defendant made these statements; but the Court cannot rely on the substance of the statements to grant a facial standing challenge.[3]

Even if the Court accepts that Plaintiff consented to a third-party app developer collecting his data and that he could have contacted Defendant to request the deletion of his data, Defendant's argument is still deficient. "Consent is . . . generally limited to the specific conduct authorized." *Javier v. Assurance IQ, LLC*, No. 4:20-cv-02860-JSW, 2021 WL 940319, at *2 (N.D. Cal. Mar. 9, 2021); *see also In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 824 (N.D. Cal. 2020) (finding that consent to data collection does not extend to data disclosure). Plaintiff gave consent for data collection to app developers, but not to Defendant. Defendant then "surreptitiously intercepts and collects Plaintiff's and Class Members' activity while using smartphone applications that have installed its SDK." (Am. Compl. ¶ 76.) Even if Plaintiff gave full consent to third-party app developers to collect his data, consent to that specific conduct does not extend to Defendant's collection of Plaintiff's data through backdoors built into apps or to Defendant's dissemination of that information for profit.

Likewise, the failure to opt-out does not demonstrate consent, particularly when users are unaware of the data collection practices. Again, the Amended Complaint quotes from Defendant's own statements that it deletes user data "so long as the request comes directly from the user." (*Id.* ¶ 67.) Defendant latches onto this allegation to argue that Plaintiff's failure to request the deletion of his data constitutes consent. But the SDK siphons data "unbeknownst to consumers," who have "no way of discovering that Defendant intercepted and recorded [their] telephonic digital communications without Class Members' knowledge or consent." (*Id.* ¶¶ 5, 148.) In short, without disclosure, the

[3] Based on the Court's experience and common sense, it may assume that third-party apps included privacy policies or terms of service, but it will not assume the content of those policies or terms.

opportunity to opt-out cannot create consent. Here, Plaintiff was not only unaware of his ability to opt-out, but also unaware of Defendant's data collection altogether.

Thus, Defendant's arguments are unavailing, and the Court finds that Plaintiff plausibly pleads an injury in fact.

B. Causation

To establish standing, plaintiffs must also show "a causal connection between the injury and the conduct complained of—the injury has to be 'fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third party not before the court." *Lujan*, 504 U.S. at 560 (quoting *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 40–42 (1976)). The Ninth Circuit has instructed that the "Article III causation threshold" is "less rigorous" than proximate causation. *Canyon Cnty. v. Syngenta Seeds, Inc.*, 519 F.3d 969, 974 n.7 (9th Cir. 2008). Plaintiff need not demonstrate that Defendants were the "sole source" of his injury. *Barnum Timber Co. v. E.P.A.*, 633 F.3d 894, 901 (9th Cir. 2011). Rather, he must only "establish a line of causation' between [D]efendants' action and [his] alleged harm that is more than 'attenuated.'" *See Maya v. Centex Corp.*, 658 F.3d 1060, 1070 (9th Cir. 2011).

Defendant suggests it is third-party app developers' actions, and not Defendant's actions, that caused Plaintiff's alleged injury. (MTD 23.) But it is Defendant's interception, packaging, and reselling of Plaintiff's data that constitute the privacy violations in this case. Third-party apps are merely the vessel for Defendant's SDK to collect data. (Am. Compl. ¶ 5 ("App developers embed SDKs into their app [] and may not know the full extent and functions of the code in the SDK.").) Moreover, even if third-party app developers were the primary cause of the collection of data, Defendant is the sole cause of the repackaging and sale of the data. (*Id.* ¶ 170.) Thus, the third-party app developers' actions do not sever the causal connection between Defendant's actions and Plaintiff's alleged injury.

C. Redressability

Finally, a plaintiff must sufficiently plead a likelihood that the injury will be "redressed by a favorable decision." *Simon*, 426 U.S. at 38. Plaintiff has done so here. He alleges Defendant's data collection practices are ongoing and consumers are "unable to take reasonable steps to avoid" the resulting intrusions to privacy. (Am. Compl. ¶ 102.) The data collection is "opaque to consumers, who typically do not know who has collected their data and how it is being used," and Defendant sells the data to companies with which the consumers have never interacted. (*Id.* ¶¶ 101–102.)

Defendant argues that injunctive relief cannot redress the alleged harm because Defendant's own actions have already provided relief. (MTD 23–24.) Defendant introduced a new "Privacy Block" capability, "which removes health services location data from the Kochava Collective marketplace." (Am. Compl. ¶ 105.) Generally, a defendant's "voluntary cessation" of the challenged conduct does not moot the case or eliminate standing. *See Friends of the Earth, Inc. v. Laidlaw Environmental Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) (explaining justification of voluntary cessation doctrine). As a result, the "Privacy Block" does not necessarily shield Defendant from suit. Moreover, even if this new capability partially redressed the harm, its coverage is limited. The "Privacy Block" protects only health services location data. Plaintiff complains of a broader injury, including tracking consumers to "sensitive locations," like places of worship, domestic abuse shelters, temporary housing shelters, and "places inferring LGBTQ+ identification." (*Id.* ¶ 86.) Therefore, the "Privacy Block" does not eliminate redressability.

For these reasons, the Court concludes Plaintiff plausibly alleges standing and accordingly **DENIES** Defendant's Motion to Dismiss pursuant to Rule 12(b)(1).

VENUE TRANSFER

Defendant also moves to transfer this action to the United States District Court for the District of Idaho, Northern Division, under 28 U.S.C. § 1404(a).

I. Legal Standard

"For the convenience of parties and witnesses, in the interest of justice, a district court may transfer any civil action to any other district . . . where it might have been brought[.]" 28 U.S.C. § 1404(a). Section 1404 "place[s] discretion on the district court to adjudicate motions for transfer according to an individualized, case-by-case consideration of convenience and fairness." *Stewart Org., Inc. v. Ricoh Corp.*, 487 U.S. 22, 29 (1988). District courts employ a two-step framework to resolve a transfer motion. A court first asks whether the plaintiff could have originally brought the action in the proposed transferee forum. *See Hoffman v. Blaski*, 363 U.S. 335, 344 (1960). If the action could have been brought there, then the court weighs "a number of case-specific factors" based in convenience and fairness. *Stewart Org.*, 487 U.S. at 29–30.

II. Analysis

A. Availability of Alternative Forum

The parties do not dispute that this action "might have been brought" in the District of Idaho, but the Court must nonetheless address the issue. *See In re Bozic*, 888 F.3d 1048, 1053 (9th Cir. 2018) (requiring courts to consider the issue *sua sponte*). "The phrase where an action 'could have been brought' is interpreted to mean that the proposed transferee court would have subject matter jurisdiction, proper venue, and personal jurisdiction." *Peregrine Semiconductor Corp. v. RF Micro Devices, Inc.*, No. 12-cv-911-IEG-WMC, 2012 WL 2068728, at *2 (S.D. Cal. June 8, 2012).

Subject Matter Jurisdiction: The Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), provides the Court with subject matter jurisdiction. CAFA requires that the "matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs" and that at least one member of the class is "a citizen of a State different from any defendant." *Id.* Plaintiff's allegations account for an amount in controversy exceeding $5,000,000 (Am. Compl. ¶ 31), and Plaintiff is a citizen of California, while Defendant is a citizen of Idaho and Delaware (*id.* ¶ 30). Thus, based on the pleadings, the federal court in the District of Idaho has subject matter jurisdiction.

Venue: Venue is proper in "a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located." 28 U.S.C. § 1391(b)(1). Here, there is only one Defendant, and its principal place of business and registered agent are in Idaho. (Am. Compl. ¶¶ 40–41.) Therefore, venue is proper in the District of Idaho.

Personal Jurisdiction: Idaho courts have personal jurisdiction over this matter. For corporations, general jurisdiction exists where the Defendant's principal place of business sits. *See Daimler AG v. Bauman*, 571 U.S. 117, 137 (2014) ("With respect to a corporation, the place of incorporation and principal place of business are 'paradig[m] . . . bases for general jurisdiction.'" (quoting *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 924 (2011))). Because Defendant's principal place of business sits in Idaho, the Idaho courts have personal jurisdiction over the matter.

Accordingly, the transfer rests on the case-specific factors and the Court's discretion.

B. Convenience and Fairness Factors

When an action could have been brought in the potential transferee court, a district court must decide whether transfer is appropriate. *Williams v. Bowman*, 157 F. Supp. 2d 1103, 1105–06 (N.D. Cal. 2001). Section 1404(a) expressly identifies the following considerations: "convenience of the parties," "convenience of . . . witnesses," and "the interest of justice." 28 U.S.C. § 1404(a). Although the statute identifies only these factors, courts deem "*forum non conveniens* considerations [to be] helpful in deciding a § 1404 transfer motion." *Decker Coal Co. v. Commonwealth Edison Co.*, 805 F.2d 834, 843 (9th Cir. 1986). District courts, therefore, consider the following factors to decide a transfer motion: (1) the plaintiff's choice of forum, (2) convenience of the parties, (3) convenience of the witnesses, (4) ease of access to the evidence, (5) familiarity of each forum with the applicable law, (6) feasibility of consolidation of other claims, (7) any local interest in the controversy, and (8) relative court congestion and time to trial in each forum. *See Jones v. GNC Franchising, Inc.*, 211 F.3d 495, 498–99 (9th Cir.

2000); *Barnes & Noble, Inc. v LSI Corp.*, 823 F. Supp. 2d 980, 993 (N.D. Cal. 2011). "This list is non-exclusive, and courts may consider other factors, or only those factors which are pertinent to the case at hand." *Martin v. Glob. Tel*Link Corp.*, No. 15-cv-00449-YGR, 2015 WL 2124379, at *2 (N.D. Cal. May 6, 2015).

1. Plaintiff's Choice of Forum

A court may afford "great weight" to the plaintiff's choice of forum, especially "when the plaintiff has chosen to file the lawsuit in its home forum." *Lou v. Belzberg*, 834 F.2d 730, 739 (9th Cir. 1987). The deference to the plaintiff's choice is reduced (1) in a class action spanning multiple states and (2) when the plaintiff does not reside in or have significant connections to the forum. *See id.* at 739 (class action); *Llevat v. True N. Brands, LLC*, No. 21-cv-656-BAS-AGS, 2021 WL 5449033, at *7 (S.D. Cal. Nov. 22, 2021) (plaintiff's out-of-forum residence); *Heredia v. Sunrise Senior Living LLC*, No. 18-cv-00616-HSG, 2018 WL 5734617, at *5 (N.D. Cal. Oct. 31, 2018) (significant connections). Finally, when there is no evidence of forum-shopping, courts generally afford at least some deference to the plaintiffs' choice of forum. *See Urista v. Wells Fargo & Co.*, No. 20-cv-01689-H-AHG, 2020 WL 7385847, at *2–3 (S.D. Cal. Dec. 16, 2020) ("[E]ven though this is a class action, [the plaintiff's] choice is entitled to deference because there is no evidence that [the plaintiff] engaged in forum shopping and both [the plaintiff] and [the defendants] have significant contacts with the [forum], including those that gave rise to this action.").

Here, Plaintiff and all putative Class Members reside in California, and a substantial part of the injury occurred in the Southern District of California. (Am. Compl. ¶¶ 35, 138.) Although Plaintiff does not reside in this district, on balance, the Court does not discern evidence of forum shopping. As such, Plaintiff's choice of forum deserves significant weight, only slightly reduced by the class action status and Plaintiff's out-of-district residence.

2. Convenience of the Witnesses

"In determining the convenience of the witnesses, the Court must examine the materiality and importance of the anticipated witnesses' testimony and then determine their accessibility and convenience to the forum." *Gherebi v. Bush*, 352 F.3d 1278, 1304 n.33 (9th Cir. 2003), *vacated on other grounds,* 542 U.S. 952 (2004). In considering the convenience factor, courts should consider "not only the number of witnesses located in the respective districts, but also the nature and quality of their testimony in relationship to the issues in the case." *Kannar v. Alticor, Inc.*, No. C-08-5505 MMC, 2009 WL 975426, at *2 (N.D. Cal. Apr. 9, 2009). Indeed, "to show inconvenience to witnesses, the moving party should state the witnesses' identities, locations, and content and relevance of their testimony." *Meyer Mfg. Co. v. Telebrands Corp.*, No. CIV. S-11-3153 LKK/DAD, 2012 WL 1189765, at *6 (E.D. Cal. Apr. 9, 2012) (citing *Florens Container v. Cho Yang Shipping*, 245 F. Supp. 2d 1086, 1092–93 (N.D. Cal. 2002)); *see also Cochran v. NYP Holdings, Inc.*, 58 F. Supp. 2d 1113, 1119 (C.D. Cal. 1998). Further, not all witnesses are treated equal: "[I]n balancing the convenience of the witnesses, primary consideration is given to third part[ies], as opposed to employee witnesses." *Hawkins v. Gerber Prod. Co.*, 924 F. Supp. 2d 1208, 1215 (S.D. Cal. 2013) (quoting *Kannar*, 2009 WL 975426, at *2).

Here, Defendant, the moving party, fails to provide the "witnesses' identities, locations, and content and relevance of their testimony." *See Meyer Mfg. Co.*, 2012 WL 1189765, at *6. The Court accepts the contention that the "majority" of Defendant's officers and employers are "based and/or located in Sandpoint, Idaho." (Manning Decl. ¶ 9, ECF No. 21-2.) But Defendant also has offices in Dublin, Ireland and Portland, Oregon. (*Id.* ¶ 6.) It is not clear how many witnesses are in Idaho or what the "nature and quality" of their testimony would be. *See Kannar*, 2009 WL 975426, at *2. Moreover, Defendant does not name or indicate any inconvenience to third-party witnesses, and it is not Plaintiff's burden to do so. As a result, the Court discerns no inconvenience to non-

party witnesses, and Defendant does not provide enough information for the Court to estimate the inconvenience to employee-witnesses.

Accordingly, Defendant has not carried its burden to establish this factor weighs in favor of transfer.

3. Familiarity of Each Forum with Applicable Law

Plaintiff alleges violations of California law. Although courts within the District of Idaho are competent to apply California law, "[a] California district court is more familiar with California law than district courts in other states." *In re Ferrero Litig.,* 768 F. Supp 2d 1074, 1081 (S.D. Cal. 2011). In some cases, the application of law is "not especially complex or specialized." *See Barnstormers, Inc. v. Wing Walkers, LLC*, No. 09-cv-2367 BEN (RBB), 2010 WL 2754249, *3 (S.D. Cal. July 9, 2010). But the Court cannot conclude that California's data privacy statutory regime is "not especially complex or specialized." As demonstrated in the analysis below on Defendant's Motion to Dismiss pursuant to Rule 12(b)(6), the issues are a tangle of law and fact. This factor, therefore, weighs against transfer.

4. Local Interest in the Controversy

"[T]his factor takes into account the current and transferee forum's interest 'in having localized controversies decided at home[.]'" *Hangzhou Chic Intelligent Tech. Co. v. Swagway, LLC*, No. 16-cv-04804-HSG, 2017 WL 1425915, at *4 (N.D. Cal. Apr. 21, 2017) (quoting *Decker Coal Co.*, 805 F.2d at 843).

California has a demonstrated interest in the privacy of its residents. To begin, Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, *and privacy*." Cal. Const. art. I, § 1 (emphasis added). The words "and privacy" were added by California voters via ballot initiative on November 7, 1972. *See Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 15 (1994). With respect to the amendment, the California Supreme Court concluded: "The principal focus of the

Privacy Initiative is readily discernible. The Ballot Argument warns of unnecessary information gathering, use, and dissemination by public and private entities—images of 'government snooping,' computer stored and generated 'dossiers' and '"cradle-to-grave" profiles on every American' dominate the framers' appeal to the voters." *Id.* at 21. The initiative's "primary purpose" was "to afford individuals some measure of protection against this most modern threat to personal privacy." *Id.*[4]

Moreover, the California Legislature has demonstrated the forum's interest in consumer protection and data privacy. California's privacy statutes have both breadth and depth. Indeed, the statutes at issue in this case exemplify this complex regime. For instance, California's UCL, a consumer protection statute, has expansive scope:

> [T]he Legislature . . . intended by this sweeping language to permit tribunals to enjoin on-going wrongful business conduct in whatever context such activity might occur. Indeed, . . . the section was intentionally framed in its broad, sweeping language, precisely to enable judicial tribunals to deal with the innumerable new schemes which the fertility of man's invention would contrive.

Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co., 20 Cal. 4th 163, 181 (1999) (internal quotation marks omitted). Other statutes are narrower but carry a bigger stick. For instance, CDAFA applies only to "computers, computer systems, and computer data," but allows for compensatory damages, punitive damages, and attorneys' fees. Cal. Penal Code § 502(a), (e). Even more severe, persons injured by, *inter alia*, the electronic collection of confidential communications are entitled to $5,000 per violation or treble damages (if any actual damages were sustained). Cal. Penal Code §§ 632, 637.2(a). These statutes evidence California's serious concern with consumer protection and data privacy.[5]

---

[4] By contrast, a constitutional amendment adding a "right to privacy" was rejected by Idaho voters in 1970. *See Planned Parenthood Great Nw. v. State*, 522 P.3d 1132, 1148 (Idaho 2023).

[5] Other statutes further highlight the forum's interest. In 2018, California passed "the nation's most far-reaching consumer protection privacy law: the California Consumer Privacy Act of 2018."

Thus, California's strong interest in these issues is readily apparent, and the local interests in the controversy weigh against transfer.

5. Feasibility of Consolidation of Other Claims

The main countervailing weight against transfer is judicial economy. "An important consideration in determining whether the interests of justice dictate a transfer of venue is the pendency of a related case in the transferee forum." *Hawkins*, 924 F. Supp. 2d at 1214 (quoting *Callaway Golf Co. v. Corp. Trade, Inc.*, No. 09-cv-384 L(POR), 2010 WL 743829, at *7 (S.D. Cal. Mar. 1, 2010)). In such cases, transfer is preferable because of "the positive effects it might have in possible consolidation of discovery and convenience to witnesses and parties." *Id.* (quoting *Callaway Golf*, 2010 WL 743829, at *7).

A court in the District of Idaho is hearing three related cases: Defendant's suit against the FTC, the FTC's suit against Defendant, and Washington residents' class action against Defendant. (Mariam Decl. ¶¶ 4–6.) Although the FTC cases may be distinguishable by their administrative nature, the Washington residents' class action largely resembles the issues here. The Court acknowledges that judicial economy may be served by consolidating discovery in these cases. Although the governing law at issue is distinct, the factual issues will largely overlap.

Several considerations, however, detract from the weight of this factor. First, Plaintiff filed his case *before* the Washington class action commenced. In the cases cited by Defendant, the transferee court transferred the later-filed case to the court with the first-to-file plaintiffs. (Mot. Venue 13.) Second, the Court cannot be certain that the later-

---

Sanford Shatz & Susan E. Chylik, The California Consumer Privacy Act of 2018: A Sea Change in the Protection of California Consumers' Personal Information, 75 Bus. Law. 1917, 1917 (2020).

filed class action will reach discovery or that the FTC suits can feasibly be consolidated. Third, the risk of inconsistent judgments is low. The Court has ruled on Defendant's standing challenge—a necessary step to continuing to exercise jurisdiction. All other judgments will be specific to the claims at issue, which almost exclusively fall under California law. The Idaho court, by contrast, will be applying Washington law and federal regulations and statutes. As a result, differing judgments would be less inconsistent than distinguishable. Thus, this factor favors transfer but has diminished weight.

6. Other Factors

The Court finds the other factors to be neutral or insignificant in this case. The convenience of the parties cancels—Idaho is more convenient for Defendant, while California is more convenient for Plaintiff and Class Members. The evidence likely is predominantly electronic and, therefore, easily transported. And finally, the relative court congestion and time of trial in each forum does not significantly move the needle.

* * *

In conclusion, the Court gives significant credence to argument for judicial economy but ultimately finds that the fairness and public policy arguments win the day. The Plaintiff's choice of forum, this Court's familiarity with California law, and California's interest in data privacy and consumer protection outweigh the potential convenience of consolidating the cases in the District of Idaho. Accordingly, the Court **DENIES** Defendant's Motion for Transfer.

FAILURE TO STATE A CLAIM

I. Legal Standard

A motion to dismiss pursuant to Rule 12(b)(6) tests the legal sufficiency of the claims asserted in the complaint. *Navarro v. Block*, 250 F.3d 729, 731 (9th Cir. 2001). "A Rule 12(b)(6) dismissal may be based on either a 'lack of cognizable legal theory' or 'the

absence of sufficient facts alleged under a cognizable legal theory.'" *Johnson v. Riverside Healthcare Sys., LP*, 534 F.3d 1116, 1121 (9th Cir. 2008) (quoting *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990)).

A complaint must plead sufficient factual allegations to "state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up). The court must accept all factual allegations pleaded in the complaint as true and must construe them and draw all reasonable inferences in favor of the nonmoving party. *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 337–38 (9th Cir. 1996). The court, however, need not accept conclusory allegations as true. Rather, it must "examine whether conclusory allegations follow from the description of facts as alleged by the plaintiff." *Holden v. Hagopian*, 978 F.2d 1115, 1121 (9th Cir. 1992) (citations omitted). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678.

II. Analysis

The Amended Complaint alleges violations of the California Constitution, CDAFA, CIPA, UCL, and common law principles of unjust enrichment. Defendant now moves to dismiss each of these causes of action.

A. Invasion of Privacy

Plaintiff's first cause of action alleges invasion of privacy, *inter alia*, under the California Constitution. Defendant argues Plaintiff's allegations do not sustain the cause of action—that is, they do not amount to a "sufficiently serious" invasion of privacy "to constitute an egregious breach of the social norms underlying the privacy right." *See Hill*, 7 Cal. 4th at 37. Plaintiff counters that the seriousness of the invasion is a question for the finder of fact, not appropriate for the pleadings stage. The Court agrees with Plaintiff.

The right to privacy is neither static nor objective. "[A]dvances in technology can increase the potential for unreasonable intrusions into personal privacy." *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1272 (9th Cir. 2019). In this way, the right is dynamic

against new threats to privacy. It is also measured against the social norms of the day: "questions of whether conduct is 'egregious,' 'offensive,' or violates 'social norms' tend by their very nature to be subjective determinations about which reasonable jurists may differ." *See Mastel v. Miniclip SA*, 549 F. Supp. 3d 1129, 1139 (E.D. Cal. 2021).

Intrusions on privacy exist on a spectrum: "Courts have been hesitant to extend the tort of invasion of privacy to the routine collection of personally identifiable information as part of electronic communications. . . . By contrast, collection of intimate or sensitive personally identifiable information may amount to a highly offensive intrusion." *In re Vizio, Inc., Consumer Priv. Litig.*, 238 F. Supp. 3d 1204, 1233 (C.D. Cal. 2017). The seriousness of a privacy invasion "requires a holistic consideration of factors such as the likelihood of serious harm to the victim, the degree and setting of the intrusion, the intruder's motives and objectives, and whether countervailing interests or social norms render the intrusion inoffensive." *In re Facebook*, 956 F.3d at 606. For this reason, courts hesitate to decide the issue at the pleadings stage. *See id.* ("The ultimate question of whether Facebook's tracking and collection practices could highly offend a reasonable individual is an issue that cannot be resolved at the pleading stage."); *Mastel*, 549 F. Supp. 3d at 1139 ("[T]hese questions are typically more appropriately resolved by a jury.").

Here, the Court finds an egregious breach plausible. Far from the "routine collection of personally identifiable information," Plaintiff alleges the surreptitious collection information that could reveal, for instance, a person's religious affiliation, sexual orientation, and medical condition. (Am. Compl. ¶ 11.) The Ninth Circuit's decision in *In re Facebook* is, again, instructive. The *In re Facebook* plaintiffs were Facebook users alleging common law and statutory privacy violations.[6] 956 F.3d at 596.

[6] *In re Facebook* primarily examines common law invasion of privacy. The common law tort of invasion of privacy is distinct from invasion of privacy under the California Constitution. But in articulating the test for invasion of privacy under the California Constitution, the California Supreme Court borrowed from common law to define "serious violations" of the expectation of privacy. *See Hill*, 7 Cal. at 270. "Because of the similarity of the tests, courts consider claims together." *In re Facebook*,

They alleged that Facebook surreptitiously "tracked their browsing histories after they had logged out of the Facebook application." *Id.* Facebook collected the Uniform Resource Locator ("URL") accessed by the users and the search terms used to find the URL. *Id.* The Ninth Circuit emphasized, "Facebook's tracking practices allow it to amass a great degree of personalized information." *Id.* at 599.

Similarly, in this case, the Amended Complaint outlines a data collection system that compiles "rich personal data," including the "[i]dentification of sensitive and private characteristics of consumers from the location data sold." (Am. Compl. ¶¶ 75, 99.) In both cases, the defendants "fingerprinted" users and correlated a vast amount of personal information without users' knowledge. (*Id.* ¶ 75 ("Defendant is able to deliver targeted advertising . . . by in essence 'fingerprinting' each unique device and user, as well as connecting users across devices and devices across users.")); *In re Facebook*, 956 F.3d at 599 ("Facebook gained a cradle-to-grave profile without users' consent."). Thus, the type of information amassed is similarly revealing, and the method is similarly secretive. These factors allow the Court to plausibly infer Defendant's data-collection practices amount to an egregious breach of social norms.

At this stage, Plaintiff has alleged enough to survive the Motion to Dismiss. Accordingly, the Court **DENIES** Defendant's Motion to Dismiss with respect to Plaintiff's invasion of privacy claim.

B. CDAFA

Under CDAFA, a person who knowingly accesses a computer system or computer data may be guilty of a public offense. Section 502(c) states in relevant part:

---

956 F.3d at 601. Thus, the logic of *In re Facebook* extends to both common law invasion of privacy and invasion of privacy under the California Constitution.

> [A]ny person who commits any of the following acts is guilty of a public offense:
>
> (1) Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> * * *
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

Cal. Penal Code § 502(c)(1)–(2), (7).

Each of these subsections requires a plaintiff to demonstrate that the defendant acted "without permission." Defendant argues the Amended Complaint fails to do so in two ways: (i) Plaintiff and Class Members consented to Defendant's data collection and (ii) "without permission" means the circumvention of a computer's barrier to access, which is not alleged. (MTD 17–19.) The Court disagrees.

First, Plaintiff and Class Members did not "consent" to Defendant's data collection so as to grant "permission" under CDAFA. Defendant argues that Plaintiff consented through voluntarily installing the SDK-embedded third-party apps on their phones, receiving a "disclaimer or warning," and bypassing the opportunity to opt-out of data collection. Just as Defendant's standing consent argument failed, its CDAFA consent argument likewise fails. Defendant's consent argument rests on allegations in the Amended Complaint which quote from Defendant's own statements. Like a facial challenge under Rule 12(b)(1), a Rule 12(b)(6) challenges requires the Court to make all reasonable inferences in Plaintiff's favor. *Cahill*, 80 F.3d at 337–38. As a result, the Court cannot assume that the content of Defendant's quotes is true.

Moreover, the Defendant carries the ultimate burden of proving a consent defense. *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1063 (N.D. Cal. 2021). To establish consent under CDAFA, a defendant must "explicitly notify users of the practice at issue." *Id.* As a result, consent is limited to the specific disclosures provided to the user, and the disclosures must have "only one plausibly interpretation for a finding of consent." *Id.* In other words, if the disclosure does not specifically and unambiguously inform the user of the data collection practices, then the consent defense fails.

Even if the Court assumes that the "consumer agreed to share its location data with an app developer," (MTD 27 (quoting Am. Compl. ¶ 104)), the limitations of the disclosures are fatal to Defendant's argument. Nowhere does the Amended Complaint suggest that consumers were aware of Defendant's involvement, when they purportedly consented to data collection. Indeed, Plaintiff alleges the opposite: "Plaintiff and Class members were not aware and could not have reasonably expected that [an] unknown third party would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiff's and Class members' personal information with other parties." (Am. Compl. ¶ 157.) To reiterate, "[c]onsent is . . . generally limited to the specific conduct authorized." *Javier*, 2021 WL 940319, at *2. As such, a user's consent to a third-party app developer collecting location data does not extend to Defendant's undisclosed collection of data.

To be clear, Defendant is not arguing that (1) Plaintiff consented to third-party app developers collecting and disseminating his data and (2) Defendant received the data from the third-party app developers. Nor could it. The Amended Complaint specifically alleges that Defendant's hidden software collected Plaintiff's data directly, skipping the middleman. Indeed, the app developers "may not know the full extent and functions of the code in the SDK." (Am. Compl. ¶ 5.) Thus, consent to third-party app developers does not confer consent to Defendant. From these allegations, Plaintiff has plausibly stated a lack of consent.

Second, the phrase "without permission" is not limited to conduct that circumvents a device barrier or "hacks" a computer system. Defendant relies on *Facebook, Inc. v. Power Ventures, Inc.* to support its narrow reading of "without permission." No. C08-05780 JW, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010). But California courts have more recently broadened their interpretation of "without permission": "Nothing in the *Power Ventures* decision held that overcoming 'technical or code-based barriers' designed to prevent access was the *only* way to establish that the Defendant acted without permission." *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1099 (N.D. Cal. 2015) (emphasis in original); *see also Synopsys, Inc. v. Ubiquiti Networks, Inc.*, 313 F. Supp. 3d 1056, 1073 (N.D. Cal. 2018). The *In re Carrier IQ, Inc.* court reasoned that the plain meaning of "without permission" should govern a consent defense and rejected the *Power Ventures* court's narrower reading of the statute. 78 F. Supp. 3d at 1099. The Court is persuaded by the reasoning of *In re Carrier IQ*. The plain meaning of "without permission" does not require the circumvention of computer barriers. Code hidden in embedded software may plausibly use or take computer data "without permission."

Moreover, even if the narrower interpretation of "without permission" did apply, the Amended Complaint plausibly alleges the circumvention of a device barrier. Apple, Inc. introduced an iPhone Application Tracking Transparency (ATT) framework, which allows an iPhone user to turn off tracking. (Am. Compl ¶¶ 68, 69, 71.) But Defendant boasts an end-run around Apple's privacy framework: it "actively collects [device tracking data], even after a consumer thinks [he has] disabled all tracking by apps on an iPhone." (*Id.* ¶ 73.) Plaintiff is himself an iPhone user. (*Id.* ¶ 72.) At this stage, the Court can plausibly infer that this end-run constitutes "access that circumvents technical or code-based barriers." *See Power Ventures*, 2010 WL 3291750, at *12. Thus, even under Defendant's preferred statutory construction, Plaintiff has carried his pleading burden.

Accordingly, the Court **DENIES** Defendant's Motion to Dismiss with respect to Plaintiff's CDAFA claim.

C. CIPA

Plaintiff alleges violations of three provisions under CIPA. The Court analyzes each below.

As a preliminary matter, Defendant argues that all CIPA claims fail because Plaintiff fails to identify a specific "communication" that was intercepted. But Defendant misunderstands Plaintiff's pleading burden. To survive a 12(b)(6) motion, a plaintiff must plead factual content that "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. Therefore, pleading a CIPA violation does not require identifying a specific communication that was intercepted. Such an inference is reasonable given the detailed allegations of Defendant's practices and Plaintiff's alleged use of SDK-embedded apps.

1. Section 638.51

California law prohibits the installation of a pen register without first obtaining a court order. Cal. Penal Code § 638.51 ("Section 638.51"). The statute defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." *Id.* § 638.50(b).

Defendant argues that its SDK is not a "pen register" but provides no caselaw in support. Indeed, it seems no court has interpreted this provision of CIPA. Traditionally, law enforcement used "pen registers" in investigations to record all numbers called from a particular telephone, and "pen registers" required physical machines. Today, pen registers take the form of software.[7] As a result, private companies and persons have the ability to hack into a person's telephone and gather the same information as law

[7] *See In re Order Authorizing Prospective & Continuous Release of Cell Site Location Recs.*, 31 F. Supp. 3d 889, 898 n.46 (S.D. Tex. 2014) (citing Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 982–89 (1996) (describing the evolution of the pen register from mechanical device to computer code)).

enforcement. Perhaps for this reason, the California legislature does not limit its prohibition on installing pen registers to law enforcement. *Compare* Cal. Penal Code § 638.51 ("[A] *person* may not install or use a pen register . . ." (emphasis added)), *with id.* § 638.52 ("A *peace officer* may make an application to a magistrate for an order . . . authorizing . . . the installation and use of a pen register . . ." (emphasis added)).

Moreover, the Court cannot ignore the expansive language in the California Legislature's chosen definition. The definition is specific as to the type of data a pen register collects—"dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," but it is vague and inclusive as to the form of the collection tool—"a device or process." *See* Cal. Penal Code § 538.50(b). This indicates courts should focus less on the form of the data collector and more on the result. Thus, the Court applies the plain meaning of a "process" to the statute. A process can take many forms. Surely among them is software that identifies consumers, gathers data, and correlates that data through unique "fingerprinting." (Am. Compl. ¶¶ 67, 74.) Thus, the Court rejects the contention that a private company's surreptitiously embedded software installed in a telephone cannot constitute a "pen register."

The Court is perplexed by Defendant's second argument. Defendant argues, "Plaintiff fails to show that the type of data purportedly collected by Kochava requires a court order or a warrant." (MTD 32.) Defendant then cites to *In re Zynga Privacy Litigation* to show that email and IP addresses are often collected without a warrant. (*Id.*) But Defendant misunderstands the elements of Plaintiff's claim. CIPA extends civil liability to the installation of a pen register without a court order. Cal. Penal Code § 638.51. Plaintiff has alleged each necessary element of this claim: Defendant installed a pen register without a court order. The fact that law enforcement can install a warrantless pen register without offending the Fourth Amendment is immaterial. *See In re Zynga Priv. Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014) ("[W]arrantless installation of pen

registers, which capture only the telephone numbers that are dialed and not the calls themselves, does not violate the Fourth Amendment.").

As such, Plaintiff has alleged enough to survive the Motion to Dismiss. Accordingly, the Court **DENIES** Defendant's Motion to Dismiss with respect to Plaintiff's Section 638.51 claim.

2. Section 631

Another CIPA subsection, titled the Wiretapping Act, prohibits surreptitious eavesdropping. It reads:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection . . . with any telegraph or telephone wire, line, cable, or instrument, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit or passing over any wire, line, or cable . . . is punishable [by fine or imprisonment].

Cal. Penal Code § 631(a) ("Section 631").

Section 631 has two clauses: It punishes (1) persons who tap telegraph or telephone wires, lines, cables, and instruments and (2) persons who attempt to learn in an unauthorized manner the contents of communications passing over any wires, lines, and cables. *See id.*; *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *20 (N.D. Cal. Sept. 26, 2013). The first clause applies only to "telegraph and telephone" wires, lines, cables or instruments, while the second clause applies to "any wire, line, or cable." As a result, courts have concluded that the first clause does not apply to internet connections, while the second clause does. *See Licea v. Am. Eagle Outfitters, Inc.*, No. EDCV 22-1702-MWF (JPR), 2023 WL 2469630, at *5 (C.D. Cal. Mar. 7, 2023) (rejecting the argument that the first clause of Section 631 applies to smart phones); *In re Google*, 2013 WL 5423918, at *20 ("[T]he Court finds no reason to conclude that the limitation of 'telegraphic or telephone' on 'wire, line, cable, or instrument' in the first clause of the statute should be imported to the second clause of the statute."). Because

Plaintiff's claim relates to data collected from smartphone apps, only the second clause can sustain the cause of action. With respect to the second clause, Defendant's only argument is that Plaintiff fails to allege that Defendant obtained the "contents" of a communication.

The statute does not provide clarity on the definition of "contents," and so courts have penciled in a dividing line. On one hand, courts have found that the contact information of the communicating parties and the geolocation of the communicating parties are not the "contents" of a communication under Section 631. *See People v. Suite*, 101 Cal. App. 3d 680, 686 (Cal. Ct. App. 1980) (finding the trapping of police emergency lines did not reveal the content of any communication, but "instead only disclosed the telephone numbers of the callers"); *cf. In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) (finding that mere geolocation data is not the "contents" of a communication under the federal Wiretap Act). On the other hand, information about particular activity conducted and search terms used on an app qualify as the "contents" of communication. *See Hammerling v. Google LLC*, No. 21-cv-09004-CRB, 2022 WL 17365255, at *10 (N.D. Cal. Dec. 1, 2022) (finding information regarding "when and how often [users] interact" with third-party apps is not "contents" of communication, but "particular activity on those apps, including products they searched for and services they used within the application," is the "contents" of communication); *In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 WL 17869218, at *11 (N.D. Cal. Dec. 22, 2022) (finding that search terms entered into a website constitute the "contents" of a communication).

The allegations in this case fall on the "contents" of communication side of the line. Plaintiff alleges that Defendant "monitor[s] and intercept[s] communications related to his personal characteristics, mode of living, purchase decisions, personal choices, app selections, spending habits, and click choices, amongst others." (Am. Compl. ¶ 38.) Defendant collects users' "activity while using smartphone applications" (*id.* ¶ 76), "search terms used by a device user which resulted in that user clicking on a particular

advertisement" (*id.* ¶ 78), and "a list of all interactions that user took within the app" (*id.* ¶ 80). Based on these allegations, this case aligns better with *Hammerling* and *In re Meta* than *Suite* and *In re iPhone Application Litigation*. Thus, Plaintiff has adequately pled that Defendant intercepted the "contents" of a communication.

Accordingly, the Court **DENIES** Defendant's Motion to Dismiss with respect to Plaintiff's Section 631 claim.

3. Section 632

"A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device" violates California Penal Code § 632 ("Section 632"). In other words, to prevail on a Section 632 claim, "a plaintiff must prove (1) an electronic recording of or eavesdropping on (2) a 'confidential communication' (3) to which all parties did not consent." *In re Google Inc.*, 2013 WL 5423918, at *22.

Defendant contends Plaintiff fails to allege the second element—the existence of a "confidential" communication. The statute defines a "confidential communication" as a communication "carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto . . . ." Cal. Penal Code § 632(c). The California Supreme Court has further clarified, "[A] conversation is confidential if a party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 768 (2002). The statutes "protects against intentional, nonconsensual recording of telephone conversations regardless of the content of the conversation or the type of telephone involved." *Id.* at 776. As such, the plaintiff need not show an "additional belief that the information would not be divulged at a later time to third parties." *Mirkarimi v. Nevada Prop. 1 LLC*, No. 12-cv-2160-BTM-DHB, 2013 WL 3761530, at *2 (S.D. Cal. July 15, 2013).

California courts have generally applied "a presumption that Internet communications do not reasonably give rise to" an objectively reasonable expectation that the conversation is not being overheard or recorded. *See Revitch v. New Moosejaw, LLC*, No. 18-cv-06827-VC, 2019 WL 5485330, *3 (N.D. Cal. Oct. 23, 2019); *see also Rodriguez v. Google LLC*, No. 20-cv-04688-RS, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021) (applying the same presumption and noting "plaintiffs must plead unique, definite circumstances rebutting California's presumption against online confidentiality"). Moreover, the Ninth Circuit has noted in dicta, "Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).

One court, however, has pushed back on this presumption. *Brown v. Google LLC* concerned Google's alleged collection of data while plaintiffs used their browsers in "private browsing mode." 525 F. Supp. 3d 1049, 1055 (N.D. Cal. 2021). The court pointed out that the presumption rested on cases concerning internet messaging services or emails. *Id.* at 1074. It distinguished these cases for two reasons. First, browsing information "does not involve messages going to another person, who could share the communication with others." *Id.* And second, whereas the defendant's policies in previous cases disclosed that messages could be shared, Google's policies did not. *Id.* Therefore, the Court applied no presumption and concluded that the communications at issue were confidential.

Brown, however, is distinguishable in part. Similar to the *Brown*-plaintiffs, Plaintiff here alleges Defendant collected his "search terms" and other communications. (Am. Compl. ¶ 78.) But unlike the *Brown*-plaintiffs, Plaintiff here fails to allege any representations that his search terms would be kept private. In *Brown*, the defendant indicated to users that searches in "incognito" or "private" mode would be protected. 525

F. Supp. 3d at 1057. For instance, the defendant's privacy notice advised users concerned with data collection to browse the web "privately using Chrome in Incognito mode" to "manage your privacy." *Id.* at 1058. No such allegations exist in this case. Thus, *Brown* is distinguishable.

The Amended Complaint does not allow the Court to infer that Plaintiff had an objectively reasonable expectation of privacy, and therefore, the Court cannot conclude Plaintiff has plausibly stated a claim. Accordingly, the Court **GRANTS** Defendant's Motion to Dismiss with respect to Plaintiff's Section 632 claim and **GRANTS** Plaintiff leave to amend.

D. UCL

Under the UCL, civil remedies are available to any "person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Defendant argues Plaintiff fails to allege a cognizable injury under the UCL. The Court agrees.[8]

In essence, the UCL stipulates two injury requirements: (1) an injury in fact and (2) lost money or property. The first injury requirement is coextensive with the constitutional minimum for standing. *See Kwikset Corp. v. Superior Ct.*, 51 Cal. 4th 310, 323 (2011). The second demands more: a plaintiff must show "economic injury." *Id.* Thus, the UCL narrows the class of plaintiffs who may sue to those who suffered economic injury.

To establish "economic injury," a plaintiff may "(1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Id.* In his Opposition, Plaintiff offers three theories of economic loss: the value of his personal data,

[8] Because the Court concludes Plaintiff failed to allege a UCL injury, it does not reach Defendant's alternative argument that Plaintiff fails to allege an "unfair" practice.

the future value of his personal data, and the surrender of more in a transaction. (ECF No. 16 at 26–30.) None is persuasive.

First, Plaintiff "is claiming the economic value of the information that was intercepted by Defendant." (*Id.* at 26.) This economic value, he argues, satisfies the injury requirement. But this argument misses the mark. Courts have consistently found that alleging the economic value of data is not enough, if a plaintiff fails to allege the economic value *to him*. *See Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1040 (N.D. Cal. 2019) (finding that "to merely say the information was taken and therefore it has lost value" does not confer UCL standing); *Ji v. Naver Corp.*, No. 21-cv-05143-HSG, 2022 WL 4624898, at *9 (N.D. Cal. Sept. 30, 2022) ("Courts in this District have held that to proceed on an economic injury theory, data privacy plaintiffs must allege the existence of a market for their data and the impairment of the ability to participate in that market."). The relevant inquiry is not whether Defendants can profit from Plaintiff's personal information, but whether Plaintiff himself can profit from his own data. The Amended Complaint does not allege any opportunity through which Plaintiff might do so. *See Hart v. TWC Prod. & Tech. LLC*, 526 F. Supp. 3d 592, 603 n.4 (N.D. Cal. 2021) (noting that the plaintiff's "location data may have economic value to others but not to him," which "reflects a peculiar feature of the current information economy").

Plaintiff cites only one case to support his theory: *Brown v. Google LLC*. But *Brown* is distinguishable. The plaintiffs in *Brown* alleged not only that the value of the data collected could be "quantified," but also that there was "an active market for such data." 2021 WL 6064009, *15. Indeed, the complaint in *Brown* alleged the defendant, Google, paid internet users "up to $3 per week to add a browser extension that shares with Google the sites they visit and how they use them." *Id.* (internal quotation marks omitted). By contrast, the Amended Complaint here includes no such allegations. Plaintiff contends Defendant's conduct was "more outrageous" than the defendant in *Brown*, but the outrageousness of a defendant's conduct is immaterial to whether Plaintiff

could have profited from his collected data. Without plausibly alleging that the data Defendant collected had value to Plaintiff, the theory fails.

Second, Plaintiff argues that he lost "future property interests." (ECF No. 16 at 28.) For the same reasons that Plaintiff's first theory failed, his second theory likewise fails. Whether alleging present or future economic loss, Plaintiff must allege how his data is economically profitable to him.

Third, Plaintiff posits losing the "benefit of the bargain"—acquiring less in the transaction than he otherwise would have—satisfies the UCL's economic injury element. To be sure, "[c]ourts in California have consistently held that benefit of the bargain damages represents economic injury for purposes of the UCL." *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, No. 3:19-cv-2284-H-KSC, 2020 WL 2214152, at *9 (S.D. Cal. May 7, 2020). But this theory of UCL injury requires the parties to have transacted. When a plaintiff never transacted with a defendant, there can be no benefit-of-the-bargain injury under the UCL. *See In re Google Assistant Priv. Litig.*, 546 F. Supp. 3d at 971 (finding that plaintiffs who did not directly transact with the defendant Google, but rather interacted with non-Google smartphones, did not have a benefit-of-the-bargain injury under the UCL).

Courts are split as to whether plaintiffs must have paid money to a defendant to sustain their benefit of the bargain theory. *Compare id.* (concluding that when a plaintiff "fail[s] to allege that [he] paid any money" to defendants, he "cannot have been injured by overpayment"), *and Cottle v. Plaid Inc.*, 536 F. Supp. 3d 461, 484 (N.D. Cal. 2021) (similar), *with Brown*, 2021 WL 6064009, at *17 ("A party who has provided goods or services in a transaction and has not been paid the fair value of those goods or services has suffered an economic injury even though the party has *received* money instead of paying money."), *and Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 636 (N.D. Cal. 2021) (similar).

But the Court need not to resolve this split today. In this case, Plaintiff did not transact with Defendant at all. Indeed, the Amended Complaint emphasizes the

"surreptitious" nature of Defendant's data collection. (Am. Compl. ¶¶ 6, 8, 12.) By contrast, *Brown*, on which Defendant relies entirely, was a dispute between Google users and Google. 2021 WL 6064009, at *17. Thus, the facts in the *Brown* case are distinguishable from those alleged in this case.

In sum, Plaintiff has "failed to demonstrate how such privacy violation translates into a loss of money or property." *Archer v. United Rentals, Inc.*, 195 Cal. App. 4th 807, 816 (Cal. Ct. App. 2011). Accordingly, the Court **GRANTS** Defendant's Motion to Dismiss with respect to Plaintiff's two UCL claims and **GRANTS** Plaintiff leave to amend.

E. Unjust Enrichment

Plaintiff's final cause of action is for "unjust enrichment," which is not a stand-alone cause of action. *See Hill v. Roll Internat. Corp.*, 195 Cal. App. 4th 1295, 1307 (2011) ("Unjust enrichment is not a cause of action, just a restitution claim."). Accordingly, the Court **GRANTS** Defendant's Motion to Dismiss with respect to Plaintiff's unjust enrichment claim.

CONCLUSION

For the reasons stated, Defendant's Motion for Transfer (ECF No. 21) is **DENIED**. Defendant's Motion to Dismiss (ECF No. 11) is **GRANTED IN PART** and **DENIED IN PART**. The Court dismisses Plaintiff's fifth, sixth, seventh, and eighth causes of action. The Court **GRANTS** Plaintiff leave to amend. If Plaintiff wishes to file an Amended Complaint, he must do so on or before **August 11, 2023**. If Plaintiff elects not to amend by August 11, 2023, Defendant's response to the remaining counts shall be due on or before **September 1, 2023**.

IT IS SO ORDERED.

DATED: July 27, 2023

Hon. Cynthia Bashant
United States District Judge