UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE GOOGLE LOCATION HISTORY LITIGATION

Case No. 5:18-cv-05062-EJD

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS

Re: Dkt. No. 87

Plaintiffs Napoleon Patacsil, Richard Dixon (and his minor child L.D.), Najat Oshana, Mark Carson, Nurudaaym Mahon, and Aichi Ali bring this putative class action alleging that Defendant Google LLC violated California law by tracking and storing geolocation data via its various applications, *i.e.* Google Maps, Chrome, etc. Having considered the Parties' briefs and having had the benefit of oral argument on November 21, 2019, the Court **GRANTS** Defendant's Motion to Dismiss.

I. BACKGROUND

A. Factual Background

Plaintiffs bring this putative class action and allege that Defendant violated California statutory, constitutional, and common law by secretly tracking and storing the geolocation and other personal data of its users. Consolidated Class Action Complaint ("Compl.") ¶ 1, Dkt. 80. Allegedly, Defendant "misled people who use[d] its products and services" by "telling them that if they activate or deactivate certain settings it [would] prevent Google from tracking their movements and storing a record of their geolocations." *Id.*

Plaintiffs discuss two privacy settings: Location History and Web & App Activity. *See id.*

¶¶ 5, 8–9, 11, 13–14, 16, 18, 20–21, 23–24, 26–27, 29, 38–39, 40–50, 61–70, 72–75, 77–80, 86–87, 106, 109–10. Location History is a setting that "saves where you go with every mobile device." *Id.*, Ex. 26 at ECF 352. "Location History is turned off by default . . . and can only be turned on if [the user] opt[s] in." *Id.* The Web & App Activity setting is different—it is "on" by default and saves certain information about a user's "activity on Google sites and apps to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services." *Id.*, Ex. 27 at ECF 356. Notably, Web & App Activity is triggered only when one uses Google-controlled features, like the Google Maps app or conducts searches using Google's web-search service. *Id.* ¶ 47. This is narrower than the general geolocation tracking which occurs if Location History is turned "on."

Plaintiffs contend that while the two settings are distinct, they reasonably thought that the "Location History" setting allowed users to prevent Google from tracking and storing geolocation information. *Id.* ¶¶ 8–9, 13–14, 18, 21, 24, 27, 69. They allege that Defendant erroneously told users they could "turn off Location History at any time" and that, with Location History off, "the places you go are no longer stored." *Id.* ¶¶ 5, 40. In reality, turning "off" Location History only prevented general geolocation tracking. As reported by the Associated Press and corroborated by academic cybersecurity researchers at Princeton University, even when "Location History" was "off," Defendant captured and kept a record of Plaintiffs' location information. *Id.* ¶ 4.

Plaintiffs allege Defendant violated the California Invasion of Privacy Act ("CIPA"), the right to privacy under the California Constitution, and the common-law tort of Intrusion Upon Seclusion by the unauthorized surveillance and storage of geolocation data. ¶¶ 118–42. Plaintiffs declined to "recite" the "precise locations" where they took their mobile devices with the Location History setting "off," but allege that if one knew those locations, one could learn things about Plaintiffs like their eating, shopping, and exercise habits, medical or psychological care, involvement in the activities of their children (if any), social life, personal residence and/or friends' residences, recurring appointments, religious services, and political affiliations. *Id.* ¶¶ 11, 16, 20, 23, 26, 29.

B. Procedural History

On May 28, 2019, Defendant filed a Motion to Dismiss Plaintiffs' Consolidated Complaint. Motion to Dismiss Plaintiffs' Consolidated Complaint ("Mot."), Dkt. 87. Defendant also filed a Request for Judicial Notice with this motion. Request for Judicial Notice ("RJN"), Dkt. 88. On July 2, 2019, Plaintiffs filed an opposition to Defendant's motion to dismiss. Opposition/Response re Motion to Dismiss ("Opp."), Dkt. 93. Plaintiffs also filed an opposition to Defendants' request for Judicial Notice as to Exhibit 1. Opposition to Request for Judicial Notice ("Opp. RJN"), Dkt. 94. Defendant submitted a reply to this opposition on July 30, 2019. Reply in Support of Request for Judicial Notice ("Reply RJN"), Dkt. 100.

On July 30, 2019, Defendant filed its Reply. Reply re Motion to Dismiss ("Reply"), Dkt. 98. Defendant submitted another request for judicial notice with its reply. Request for Judicial Notice re Reply ("RJN 2"), Dkt. 99. Plaintiffs submitted an opposition to this request on August 13, 2019. Plaintiffs' Opposition to Google's Supplemental Request for Judicial Notice ("Opp. RJN 2"), Dkt. 103.

II. JUDICIAL NOTICE

Defendant asks this Court to take judicial notice of Exhibits 1, 2, 3A–3D, 4, 5, and 6 attached to the Declaration of Christina Lee (the "Lee Declaration"). RJN at 1. Defendant also asks this Court to take judicial notice of Exhibits 1–3 attached to the Declaration of Bright Y. Kellogg (the "Kellogg Declaration"). RJN 2 at 1.

A. Legal Standard

Generally, district courts may not consider material outside the pleadings when assessing the sufficiency of a complaint under Rule 12(b)(6) of the Federal Rules of Civil Procedure. *Lee v. City of L.A.*, 250 F.3d 668, 688 (9th Cir. 2001). When matters outside the pleadings are considered, the 12(b)(6) motion converts into a motion for summary judgment. *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 998 (9th Cir. 2018); *see also* Fed. R. Civ. P. 12(d). This rule does not apply to the incorporation by reference doctrine and judicial notice under Federal Rule of Evidence 201. *Khoja*, 899 F.3d at 998.

Rule 201 permits a court to take judicial notice of an adjudicative fact "not subject to reasonable dispute," that is "generally known" or "can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). Specifically, a court may take judicial notice: (1) of matters of public record, *Khoja*, 899 F.3d at 999, (2) legislative history, *Anderson v. Holder*, 673 F.3d 1089, 1094 n.1 (9th Cir. 2012), and (3) publicly accessible websites whose accuracy and authenticity is not subject to dispute, *Daniels-Hall v. Nat'l Educ. Ass'n*, 629 F.3d 992, 998–99 (9th Cir. 2010). A court may consider facts contained in the noticed materials. *Barron v. Reich*, 13 F.3d 1370, 1377 (9th Cir. 1994).

B. Discussion

1. Defendant's First Request for Judicial Notice

Plaintiffs only take issue with Exhibit 1 of the Lee Declaration. *See* Opp. RJN. Exhibits 2, 3A–3D, 4, 5, and 6 of the Lee Declaration may be judicially noticed—they are either publicly available websites whose accuracy is not subject to reasonable dispute or legislative history. *See Daniels Hall*, 629 F.3d at 998–99; *Anderson*, 673 F.3d at 1094 n.1. Accordingly, the Court **GRANTS** Defendant's requests for judicial notice for Exhibits 2, 3A–3D, 4, 5, and 6 of the Lee Declaration.

Plaintiffs argue that this Court should not take judicial notice of Exhibit 1 because, although it is a publicly available website, the statements contained therein are unreliable, untrustworthy, and self-serving. Opp. RJN at 2–3. But, when a court takes judicial notice, it is not noticing the truth of the statements contained in an exhibit. Rather, the Court "takes judicial notice that [an exhibit] was in the public realm . . . [and] not for the truth of [its] contents." *Diaz v. Intuit, Inc.*, 2018 WL 2215790, at *3 (N.D. Cal. May 15, 2018) (citing *Brodsky v. Yahoo! Inc.*, 630 F. Supp. 2d 1104, 1111 (N.D. Cal. 2009). Here, Defendant is not asking the Court to judicially notice the truth of the statements contained in Exhibit 1. Rather, Defendant requests for this Court to notice that: (1) Exhibit 1 was in the public realm as of May 25, 2019 and (2) that Google publicly disclosed, as of May 25, 2019, to users that Location History is an "opt-in only" feature. Reply RJN. Plaintiffs do not dispute the second proposition. *See* Compl., Ex. 26 at ECF

352. Accordingly, the Court **GRANTS** Defendant's request for judicial notice of Exhibit 1 of the Lee Declaration.

2. Defendant's Second Request for Judicial Notice

Exhibits 1–3 to the Kellogg Declaration are printouts of websites. *See Caldwell v. Caldwell*, 2006 WL 618511, at *3–4 (N.D. Cal. Mar. 13, 2006) (noting that judicial notice of websites and their contents is typically proper if the requesting party provides the court with a copy of the specific web page). Plaintiffs spend most of the brief arguing that judicial notice is improper because the facts presented actually bolster the arguments made in their Complaint. But this is not the inquiry. Plaintiffs next argue that judicial notice is improper because the requests attempt to impermissibly introduce new facts on a reply. Opp. RJN 2 at 2. The information sought to be noticed, however, has to do with disclosures regarding Web & App Activity, which Plaintiffs have already discussed in their Complaint and oppositions. *See, e.g.*, *id.* at 3. Thus, Defendants are not introducing, for the first time, new facts or different legal arguments via the three requested exhibits. *See State of Nev. v. Watkins*, 914 F.2d 1545, 1560 (9th Cir. 1990) ("[Parties] cannot raise a new issue *for the first time* in their reply briefs." (emphasis added)). Accordingly, because the three requested exhibits are publicly available websites, judicial notice is proper, and Defendant's request is **GRANTED.**

III. MOTION TO DISMISS

To survive a Rule 12(b)(6) motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to "state a claim for relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (discussing Federal Rule of Civil Procedure 8(a)(2)). 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. *Id.* The requirement that the court "accept as true" all allegations in the complaint is "inapplicable to legal conclusions." *Id.* If there are two alternative explanations, one advanced by the defendant and the other advanced by the plaintiff, both of which are plausible, the "plaintiff's complaint survives a motion to dismiss under Rule 12(b)(6)." *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011). Dismissal can be based

on "the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1990).

A. Consent

Defendant first argues that this action must be dismissed because Plaintiffs consented to the geolocation tracking and storage at issue. MTD at 9–11; *see also Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) (noting that effective consent means a plaintiff cannot have a reasonable expectation of privacy). Specifically, Defendant argues that by agreeing to its Terms of Service and Privacy Policies, all Google users consented to having their geolocation data tracked and stored when using a Google application. MTD at 9–10.

Consent is only effective if the person alleging harm consented to "the particular conduct, or to substantially the same conduct" and if the alleged tortfeasor did not exceed the scope of that consent. *Opperman*, 205 F. Supp. 3d at 1072–73 (citation and quotation marks omitted).

Explicit Consent. Defendant first argues that Plaintiffs consented to the use and collection of their location information because the Privacy Policy warned, *before* the Class Period, that "[w]hen you use Google services, we may collect and process information about your actual location." Opp. at 10 (citing Lee Decl., Ex 3D at 3). Defendant thus contends that because Plaintiffs consented to this as part of Google's Terms of Services, they consented to the collection and storage of geolocation data, and thus have no claims against Defendant. *Id.*

Defendant notes that its Privacy Policy informed users that their geolocation data may be collected during the use of Google services and argues nothing overrode or modified this warning. MTD at 11. Defendant next notes that its "Web & App Activity support page makes clear that Google collects location information when those specific services are used" as it states that when this feature is turned on, location data is collected when a user uses Google services. *Id.* (citing Compl., Ex. 29).

This misses the thrust of the allegations within Plaintiffs' Complaint. Plaintiffs argue that even while "Web & App Activity" and "Location History" are distinct, Defendant mislead users into believing that disabling Location History meant geolocation information would not be stored.

See, e.g., Compl. ¶ 8 ("Based upon the terminology used by Google (*e.g.* "Location History"), the context, and representations by Google to the effect that turning "Location History" off would prevent his location information from being stored and that Google would respect his privacy settings, Mr. Patacsil believed that this would prevent Google from storing a record of his location history."); *Id.* ¶ 40 & Ex. 4 (noting that Google's support page formerly stated "With Location History off, the places you go are no longer stored.");[1] *Id.* ¶ 106 (alleging "sophisticated media professionals" were deceived by Google's stated data policy and believed that turning off Location History prevented Google from tracking and storing location data). Plaintiffs argue that the way to disable geolocation storage (the "Web & App Activity" feature) was "deeply-buried and no[t] obvious," such that Plaintiffs were misled about the effect of disabling Location History. *Id.* ¶ 63. Thus, the literal statements within the Privacy Policies and Terms of Service are irrelevant. The relevant inquiry is whether Plaintiffs still consented to geolocation storage *even after* disabling Location History.

Drawing all inferences in favor of Plaintiffs, a reasonable user could believe that disabling Location History prevented Defendant from collecting and storing geolocation data. This conclusion is bolstered by the fact that *many* people were mislead by the effect of disabling Location History. *See, e.g.*, Compl. ¶ 4. Moreover, the support page Defendant points the Court to was created *after* this litigation had already commenced. At the time Plaintiffs' original complaints were filed, the page described Web & App Activity as merely a means to "[s]ave your search activity on apps and in browsers to make searches faster." *Id.*, Ex. 28. The page did not expressly state that geolocation data may be collected.

Implicit Consent. Defendant next argues that by using Google services, like Google Maps, users implicitly consented to Google collecting and using geolocation information.

[1] Defendant makes light of Plaintiffs' failure to specifically plead they read and relied on this statement. *See* Mot. at 11. But Plaintiffs allege that based on Defendant's representations, they believed that by turning off Location History, their geolocation data was no longer stored. *See, e.g.*, Compl. ¶ 5. The Court can plausibly infer that Plaintiffs read and relied on Defendant's representations.

Plaintiffs rebut this by noting that while Google may need to track the location of a user when Google Services are being used, consent to Defendant tracking a user's geolocation location for an immediate, discrete purpose does not parlay into consent for the indefinite storage of such location information. Opp. at 3–4. Plaintiffs allege that by turning off Location History, they gave only ephemeral consent to geolocation tracking and not indefinite consent to the storage of that tracking. Compl. ¶¶ 8, 12, 18, 21, 24, 27.

"[C]onsent is not an all-or-nothing proposition." *In re Google Inc.*, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013). A party may consent to "the interception of only part of a communication or to the interception of only a subset of its communications." *In re Pharmatrak, Inc.*, 329 F.3d 9, 19 (1st Cir. 2003). The Court thus rejects Defendant's contention that by consenting to transitory use, Plaintiffs consented to geolocation collection. To the contrary, it is plausible that Plaintiffs gave a *narrow* consent to geolocation tracking, exclusive of data storage.

Accordingly, a material factual dispute remains as to whether Plaintiffs consented to a Privacy Policy "authorizing the very conduct they complain of," see Reply at 3, *or* whether Plaintiffs reasonably believed, based on Defendant's representations, that they revoked consent to geolocation storage by disabling "Location History." *Starr*, 652 F.3d at 1216 (noting that if two alternative plausible explanations exist, the plaintiff's versions should be followed at the motion to dismiss stage). It is plausible that Plaintiffs only consented to transitory use tracking and revoked any consent to the storage of their geolocation history. It is also plausible that they did *not* revoke such consent. The Court cannot conclude either way—factual disputes remain. "This is an issue for the jury." *Opperman*, 205 F. Supp.3d at 1073 (holding that the plaintiffs produced sufficient evidence showing they did not consent to the defendants' actions). For these reasons, the Court holds Plaintiffs have plead sufficient facts to show they did not consent to the storage of their geolocation information.

B. California Invasion of Privacy Act ("CIPA") Claim

California Penal Code § 637.7 provides in relevant part:

(a) No person or entity in this state shall use an electronic tracking device to determine the

location or movement of a person.

(b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.

(c) This section shall not apply to the lawful use of an electronic tracking device by a law enforcement agency.

(d) As used in this section, "electronic tracking device" means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.

Plaintiff alleges that Google services constitute an "electronic tracking device" because Defendant used "devices" (GPS hardware, the cellular radio, and/or the WiFi chip) attached to or located within a "moveable thing" to "reveal[] its location or movement by the transmission of electronic signals." Compl. ¶ 123. Plaintiffs argue, in the alternative, that their mobile devices are "electronic tracking devices," which when placed or attached on or within moveable things (cars, buses, backpacks, clothing, etc.) reveal a device's "location or movement by the transmission of electronic signals." *Id.* ¶ 124. Defendant argues that Plaintiffs' CIPA claim fails as a matter of law because the subject-matter at issue is outside CIPA's reach. Mot. at 12. The Court agrees.

Federal courts apply California rules of statutory construction when interpreting a California statute. *Lares v. West Bank One (In re Lares)*, 188 F.3d 1166, 1168 (9th Cir. 1999). "The touchstone of statutory interpretation is the probable intent of the Legislature." *Hale v. S. Cal. IPA Med. Grp., Inc.*, 103 Cal. Rptr. 2d 773, 776 (Ct. App. 2001). The first step in determining that intent is to "scrutinize the actual words of the statute, giving them a plain and commonsense meaning." *Cal. Teachers Ass'n v. Governing Bd. of Rialto Unified Sch. Dist.*, 927 P.2d 1175, 1177 (Cal. 1997). A court may use customary rules of statutory construction or legislative history to resolve any facial or latent ambiguity in the statute. *Hale*, 103 Cal. Rptr. 2d at 776. If no ambiguity exists, however, such tools of statutory construction are unnecessary. *Cal. Fed. Sav. & Loan Ass'n v. City of L.A.*, 902 P.2d 297, 300 (Cal. 1995); *People v. Snook*, 947 P.2d 808, 811 (Cal. 1997) ("If there is no ambiguity in the language, we presume the Legislature meant

what it said and the plain meaning of the statute governs.").

First, there is a fundamental problem with the way Plaintiffs plead their CIPA claim—they take issue not with the "determination [of] the[ir] location or movement," but with the *collection* and *storage* of that geolocation data. CIPA does not apply to the storage of geolocation data; it only applies to unconsented geolocation tracking. *See* Cal. Penal Code § 637.7(b). Plaintiffs concede in their opposition brief that "in some applications, contemporaneous *use* of location information may be appropriate . . . [like] to receive 'driving directions' or 'showtimes for movies playing near[by].'" Opp. at 3.[2] Hence, Plaintiffs issue is not with Defendant tracking them during application use, rather their issue is with the *storage* of that data. *See* Opp. at 3–4 ("[I]n accepting the transitory use of location information for an immediate, discrete purpose, Plaintiffs in no way consented to indefinite storage of their daily locations and movements . . . ."). For this reason, Plaintiffs' CIPA claim fails as a matter of law because CIPA, by its plain terms, is not concerned with data storage but focuses on unconsented data tracking, which is not at issue.

Second, assuming some type of unconsented tracking was occurring, Defendant's services are not a "device" within the meaning of Section 637.7(d). In *Moreno v. San Francisco Bay Area Rapid Transit Dist.*, Judge Corley determined that an "electronic tracking device" did not include "software installed in mobile devices." 2017 WL 6387764, at *5 (N.D. Cal. Dec. 14, 2017). Software like Google Maps, Chrome, etc. are not "devices" within the meaning of CIPA because they are not "equipment." *Id.* Plaintiffs do not contest this. Opp. at 8. Instead, they argue that their allegations do not hinge on software because the word "software" does not appear in the CIPA count. Opp. at 8.

Such an argument places form over substance and is rejected. The Court agrees with Defendant's contention that "Plaintiffs' allegations are centrally focused on Google's software." Reply at 7. The gravamen of Plaintiffs' Complaint is that they turned off "Location History"—a

[2] Moreover, Plaintiffs own allegations make clear that indefinite tracking was not occurring as they all claim to have switched Location History "off." With Location History off, Defendant cannot track users unless they open a Google application. Plaintiffs do not allege such indefinite tracking was occurring.

software setting—believing this disabled Google's applications, *i.e.* Google Maps, etc., from storing geolocation data. Compl. ¶ 122; *see also id.* ¶¶ 5, 8–9, 11, 13–14, 16, 18, 20–21, 23–24, 26–27, 29, 38–39, 40–50, 61–70, 72–75, 77–80, 86–87, 106, 109–10 (describing Location History and/or Web & App Activity software settings). Just as in *Moreno*, where Judge Corley concluded the Bay Area Rapid Transit ("BART") Watch mobile application was software, Google applications, much like the BART application, are software downloaded onto smartphones. *See* 2017 WL 6387764 at *1, 5. The lack of the word "software" in the Complaint does not change the basic structure of Defendant's services.

Plaintiffs argue in the alternative that even if Defendant's services constitute "software," the GPS hardware, cellular radios, and WiFi chips embedded in mobile devices constitute "electronic tracking devices" within the meaning of Section 637.7. Admittedly, Section 637.7 defines "electronic tracking device" broadly; it reaches any device that "determine[s] the location or movement of a person." Despite the expansive language of Section 637.7, Plaintiffs' argument fails because Plaintiffs provide no facts from which the Court can infer GPS hardware, cellular radios, and/or WiFi chips actually determine the location of movement of a person. *See* Compl. ¶ 123. The Court need not accept Plaintiffs' bare conclusion that GPS hardware, cellular radios, and WiFi chips qualify as "electronic tracking devices." *See Ashcroft*, 556 U.S. at 678 (noting that a court need not accept legal conclusions as true); *see also* Reply at 8 (arguing GPS hardware and WiFi chips are not electronic tracking devices based on case law that states WiFi chips and GPS hardware only receive, but do not transmit, satellite signals). Moreover, this argument collapses into the software argument detailed above. *See supra*. Indeed, as noted above, the gravamen of Plaintiffs' allegations is not that GPS hardware in the phones tracked Plaintiffs, but that Plaintiffs believed by disabling certain software settings Defendants could no longer store their geolocation data. *See* Compl. ¶ 142 (only paragraph about "GPS hardware, cellular radios, and/or WiFi chips" out of a 142-paragraph complaint).

Finally, Defendant argues that Plaintiffs have not shown that they "attached" an "electronic tracking device" to "a vehicle or other moveable thing." Plaintiffs contend that they have pled

Defendant "attached" an electronic tracking device to "moveable things," including "cars, buses, trains, bicycles, [] other forms of transportation . . . . [and] clothing, purses, briefcases, and backpacks." Compl. ¶ 124; Opp. at 10. Plaintiffs argue CIPA's "attach" does not require Defendant to have personally "placed" something on a moveable thing because it only requires some association with a moveable thing. Opp. at 12. The Court disagrees. These arguments push CIPA beyond its plain meaning and transform the statute into something unrecognizable. *See* Reply at 6 (arguing Plaintiffs arguments create a "CIPA windfall").

As Judge Corley noted in *Moreno*, the ordinary meaning of "attach," is to "join or fasten (something) to something else." 2017 WL 6387764, at *5 (citing *Attach*, OXFORD ENGLISH DICTIONARY ONLINE, https://www.oed.com/view/Entry/12698 (last visited November 26, 2019)); *Wasatch Prop. Mgmt. v. Degrate*, 112 P.3d 647, 653 (Cal. 2005) ("When attempting to ascertain the ordinary, usual meaning of a word, courts appropriately refer to the dictionary definition of that word."). Plaintiffs advocate for a definition of attach that requires *no* literal attachment to a moveable thing. *See* Opp. at 12–13. They define "to attach" as an "association." *Id.* But, such definitions of the term apply to familial or personal attachments, not the attachment of devices. For instance, under Plaintiffs definition, smartphones[3] would have to "join (someone or something) without being invited" or "bring [themselves] into an association" with a vehicle or other moveable thing." *See* Reply at 10 (analyzing Plaintiffs' definitions). This is nonsensical and contrary to the words and history of the statute. Indeed, the bill denotes that "attach" requires some affirmative act by the wrongdoer. *See* RJN, Ex. 5 at ECF 96 ("[T]his bill . . . would not allow *a private investigator to place* a device on the automobile of an individual he or she is trying to follow." (emphasis added)). Simply associating with a "moveable object" with an "electronic tracking device" is insufficient. Accordingly, the Court rejects Plaintiffs definition of "attach."

The Court also rejects Plaintiffs' expansive definition of "other moveable things." Plaintiffs contend that "other moveable things" means anything that moves, like "belt holsters and

[3] Smartphone comprises the GPS hardware, cellular radios, and WiFi chips that Plaintiffs argue constitutes an "electronic tracking device" as they are all components of the phone.

phone cases." This, however, ignores foundational statutory interpretation principles. "[W]hen words 'are associated in a context suggesting that the words have something in common, they should be assigned a permissible meaning that makes them similar.'" *Friends of Animals v. U.S. Fish & Wildlife Serv.*, 879 F.3d 1000, 1008 (9th Cir. 2018) (citation omitted); *see also People v. Prunty*, 355 P.3d 480, 487 (Cal. 2015) (interpreting "group" in "organization, association, or group" as requiring a meaning "generally similar to—and at least no broader than" the preceding terms). Here, "vehicle" precedes (and thus modifies) "other moveable thing." "The meaning of vehicle, thus, informs the meaning of "other moveable things." *Prunty*, 355 P.3d at 487 ("[A] word literally 'is known by its associates.'" (citation omitted)). Hence, "other moveable things" cannot mean "anything that moves." A contrary finding would ignore and render "vehicle" surplusage. *Cf. id.* ("[W]e must stop short of construing [a statute] so expansively that we render the other terms 'unnecessary or redundant . . . ." (citation omitted)). Therefore, "other moveable things" refers to things like boats, planes, or other comparable motorized machines. *See* RJN, Ex. 5 at ECF 95 ("The purpose of this bill is to prohibit the placing of an electronic tracking device on an *automobile* by a person who is not the registered owner."); *see also id.* at ECF 95–96 (referring to "automobiles" in describing the purpose of the bill). "Other moveable things" does *not* refer to moving persons, their belts, or their smartphones.

Hence, Plaintiffs arguments that Defendants "attached" an "electronic tracking device" to a "moveable thing" are rejected. The Court holds that "attach" requires the wrongdoer to "place," "put," or "join" an electronic tracking device to a moveable thing. *See* RJN, Ex. 5 at ECF 96 ("[T]his bill . . . would not allow *a private investigator to place* a device on the automobile of an individual he or she is trying to follow." (emphasis added)). The Court further holds that the definition of "other moveable things" does not include persons, their belts, or their smartphones. Plaintiffs' theory that any mobile device in any moveable thing satisfies CIPA is rejected. Accordingly, because Plaintiffs have not plead sufficient facts showing that Defendant "attached" a tracking device to a "moveable thing," see *supra*, Defendant's motion to dismiss Plaintiffs' CIPA claim is **GRANTED.** The Court does not grant leave to amend as it finds that amendment

would be futile because Plaintiffs neither can show that CIPA reaches the software at issue nor that Defendants were intentionally placing electronic tracking devices on vehicles or other comparable moveable things. *Cahill v. Liberty Mut. Ins. Co.*, 80 F.3d 336, 338 (9th Cir. 1996) (dismissal with prejudice permissible if amendment would be futile).

C. Constitutional and Common-Law Privacy Claims

Plaintiffs allege that Defendant violated their right to privacy under Article I, Section 1 of the California Constitution by intentionally intruding on and into Plaintiffs' solitude, seclusion, right of privacy, and/or private affairs by intentionally tracking their location. Compl. ¶¶ 136–42. Plaintiffs also allege Defendant violated the common law intrusion upon seclusion. *Id.* ¶¶ 128–35.

The California Constitution creates a privacy right that protects individuals' privacy from intrusion by private parties. *Am. Acad. Of Pediatrics v. Lungren*, 940 P.2d 797, 810 (Cal. 1997); *see also Hill v. NCAA*, 865 P.2d 633, 644 (Cal. 1994). To establish an invasion of privacy claim, a plaintiff must demonstrate: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill*, 865 P.2d at 654–655. These elements are not a categorical test but rather are "threshold elements" that allow courts to "weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale*, 927 P.2d 1200, 1230 (Cal. 1997). "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill*, 865 P.2d at 655.

A common law intrusion upon seclusion claim must allege: "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998). Analysis of these respective prongs is effectively identical, and the Parties analyzed the constitutional and common law claims together under *Hill*'s three elements. Opp. at 14; *see also In re Vizio, Inc. v. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1232 n.11 (C.D. Cal. 2017). The Court examines the claims together.

"The California Constitution sets a 'high bar' for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (quoting *Belluomini v. Citigroup, Inc.*, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013). "Whether a legally recognized privacy interest is present in a given case is a question of law to be decided by the court." *Hill*, 865 P.2d at 657. Whether a plaintiff has a reasonable expectation of privacy in the circumstances and whether a defendant's conduct constitutes a serious invasion of privacy are mixed questions of law and fact. *Id.*

Legally Protected Privacy Interest. California law recognizes two classes of legally protected privacy interests. *Id.* at 654. "[P]rivacy interests do not encompass all conceivable assertions of individual rights." *Id.* "Legally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference ('autonomy privacy')." *Id.*

Plaintiffs argue they have established a "legally protected privacy interest," see Opp. at 14, because they allege that Defendant violated their (1) informational privacy rights by "misus[ing] [their] sensitive and confidential [location] information," *id.* at 15 n.5 (second and third alteration in original) and (2) autonomy privacy rights as the comprehensive cataloging of users' movements restricted users' ability to "mak[e] intimate personal decisions . . . without observation [or] intrusion." *Id.* (alteration in original) (quoting *Hill*, 865 P.2d at 648). Defendant argues Plaintiffs have not established an invasion of such privacy rights because Plaintiffs do not allege that Defendant misused or disseminated sensitive and confidential information *or* observed, intruded, or interfered with the making of intimate personal decisions. Mot. at 16.

As a starting matter, Plaintiffs argue "that Google not only tracked Plaintiffs *continuously* in their cars, but also in every other aspect of their lives." Opp. at 18; *see also* Compl. ¶¶ 10, 15, 19, 22, 25, 28 ("[Plaintiff] carried his mobile device virtually everywhere he went throughout the day, including when traveling by vehicle or otherwise on public thoroughfares and when entering

commercial spaces, medical care providers, private offices, and private residences."). But this mischaracterizes the factual background of the Complaint. Plaintiffs' Complaint is premised on the allegation that Defendant mislead them into believing that by turning "off" Location History, the geolocation data collected during ***use*** of Google's services would not be stored. *See* Compl. ¶ 47 ("Contrary to Google's representations, even when 'Location History' is turned off, whether at the Google Account level or the individual device level, a user's location is stored and, on information and belief, continues to be stored, every time Google-controlled features on her mobile device are active . . . ."). They never allege that even with Location History "off," Defendant was still tracking their geolocation data. Thus, continuous geolocation tracking is not at issue.

The Court returns to the issue of consent. As discussed above, see *supra* III.A., a factual issue remains about the scope of Plaintiffs' consent. However, it is clear that even while Plaintiffs may not have consented to "Google's storage of their location information," they did consent to *some* type of geolocation tracking. *Compare* Compl. ¶ 114(c) (stating Plaintiffs did not consent to storage of geolocation data), *with* Opp. at 3 ("To be clear, Plaintiffs acknowledge that in some applications, contemporaneous use of location information may be appropriate—for example, to receive "driving directions" or "showtimes for movies playing near[by]."). Indeed, consent to geolocation tracking is corollary to the use of a Google service, like Google Maps. Hence, as clarified above, the issue in dispute is not geolocation tracking but the storage of that geolocation information. *See* Opp. at 3. This is something Plaintiffs acknowledge in their Consolidated Complaint. *See, e.g.*, Compl. ¶ 8 (arguing Plaintiff Patacsil turned "off" his Location History to protect Defendant and others from "record[ing]" and accessing his location over time). Despite this, Plaintiffs collapse geolocation tracking and geolocation storage into the same allegation. *See* Opp. at 16. The Court rejects this. The issue is not the "systematic tracking of movements over time" but the storage of that information. *Id.*; *see also* Compl. ¶ 40 ("Google misrepresented that "the places you go are no longer *stored*" when Location History is disabled . . . .").

Having narrowed the issue, the Court turns to the main issue—whether the collection and

storage of geolocation information interferes with autonomy and/or information privacy. *Hill*, 865 P.2d at 654. While the California Constitution protects autonomy, it does not "create an[] unbridled right of personal freedom of action that may be vindicated in lawsuits." *Id.* California courts have discussed autonomy privacy in cases "alleging *bodily* autonomy." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1039; *see also e.g.*, *Comm. to Def. Reprod. Rights v. Myers*, 625 P.2d 779, 792 (Cal. 1981) (noting constitutional right of privacy in woman's "personal bodily autonomy"); *Smith v. Fresno Irrigation Dist.*, 84 Cal. Rptr. 2d 775, 785 (Ct. App. 1999) (discussing autonomy privacy in the context of drug testing through use of a urine sample). Plaintiffs do not argue in their Opposition that *Myers* or *Fresno Irrigation District* should be extended to geolocation information. *See* Opp. at 15 n.5 (only places "autonomy privacy" is discussed). Instead, Plaintiffs spend most of their Opposition arguing that informational privacy is at stake. The Court does not find sufficient cause to extend the bodily autonomy line of cases to data autonomy.

Plaintiffs' information privacy rights allegation is also rejected. Plaintiffs contend that Defendant's surreptitious collection and storage of comprehensive and highly sensitive location data violates their information privacy rights. Opp. at 15. Even if the collection of granular and specific location data establishes an information privacy interest, Plaintiffs' theory is undercut by the admission that Defendant only tracked and collected data during use of Google services. Accordingly, Defendant's "profile" of a user is only as specific as their use of Google services. *Carpenter v. United States* and *United States v. Jones* do not undercut this conclusion. *Carpenter v. United States* addressed whether the Fourth Amendment required government agents to secure a warrant to access historical cell phone records (cell-site location information). 138 S. Ct. 2206, 2211, 2220 (2018). First, there was no claim that MetroPCS and Sprint, the phone companies holding the cell-site location information, violated the plaintiff's right of privacy by having such robust geolocation records. *Id.* at 2212. The case thus does not stand for the proposition that geolocation collection violates the right of privacy.

Second, the cell-site location information discussed in *Carpenter* was comprehensive—the cell-site location information provided cellular companies with a rough "map" of a customer's

fluid movements. *Id.* at 2211. Such comprehensive data collection is not at issue here; Plaintiffs' geolocation information depends on how often they use Google's services. Defendant's collection of geolocation data is not automatic; it does not happen by the routine "pinging" of a cell-phone tower. *Cf. United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy *in the sum* of one's public movements." (emphasis added)). Here, unlike the continual GPS tracking in *Jones*, not *all* of Plaintiffs movements were being collected, only specific movements or locations. Such "bits and pieces" do not meet the standard of privacy established in *Carpenter* or *Jones*. *Carpenter*, 138 S. Ct. at 2218 ("[A] cell phone . . . tracks *nearly exactly* the movements of its owner . . . . [to] private residences, doctor's offices, political headquarters, and other potentially revealing locales"); *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L.R. 311, 328–29 (2012) (discussing the mosaic theory).

Second, and relatedly, the Court agrees with Defendant that Plaintiffs allegations are far too conclusory and speculative. Without more particular pleading, the Court cannot determine if Defendant extrapolated a "mosaic" from the user data *or* if the data collected is "sensitive and confidential" information. Indeed, "[a] person's general location is not the type of core, value, informational privacy explicated in *Hill*." *Fredenburg v. City of Fremont*, 14 Cal. Rptr. 3d 437, 446 (Ct. App. 2004). It is entirely speculative that geolocation data was ever collected from a Plaintiff while at a sensitive or confidential location. *See* Compl. ¶ 108 ("[Google] *can* track where and when consumers shop, the establishments they pass once or every day, which restaurants they frequent, the doctors they visit, where they pump their gas." (emphasis added)); *see also* Compl. ¶ 11 (not reciting Plaintiff Patacsil's precise location history for privacy reasons, but also only stating that Defendant *could have* determined Patacsil's precise geolocation movements). As the Court discussed above simply carrying a mobile device does not give Defendant the ability to track a user. It is entirely speculative what data Defendant collected. *Cf. Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078, 1091 (N.D. Cal. 2018) (finding information

privacy right after the plaintiff specifically alleged that the defendant collected his home address); *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1040 (requiring specifics as to why email contents were private). Much like *In re Yahoo Mail Litigation*, Plaintiffs claims are too conclusory and the Court cannot assess whether Plaintiffs had a legally protected privacy interest in the specific places they went or even how often their geolocation was accessed. *See* 7 F. Supp. 3d at 1041 ("The problem for Plaintiffs in the instant case, however, is that to the extent Plaintiffs intend to allege that they have a privacy interest in the specific content of their emails, their allegations are fatally conclusory."). Allowing such conclusory and speculative pleading to survive a Rule 12(b)(6) motion to dismiss would obliterate the "high bar" set for establishing an invasion of privacy claim. Because Plaintiffs do not plead sufficient facts to establish a legally protected privacy interest, the Court does not reach the remaining two factors.

Accordingly, since Plaintiffs do not plead sufficient facts to allege an invasion of privacy, Defendant's Motion to Dismiss Plaintiffs' constitutional and common law privacy claims is **GRANTED.** The Court grants leave to amend as it finds amendment would not be futile.

IV. CONCLUSION

For the foregoing reasons, the Court **GRANTS** Defendant's Motion to Dismiss with prejudice as to Plaintiffs' CIPA claim. The Court **GRANTS** Defendant's Motion to Dismiss without prejudice as to Plaintiffs' constitutional and common law privacy claims.

Plaintiffs may file an amended complaint by **January 23, 2020**. Plaintiffs may not add new causes of action or parties without a stipulation or order of the Court under Rule 15 of the Federal Rules of Civil Procedure. Failure to cure the deficiencies addressed in this Order will result in dismissal with prejudice.

IT IS SO ORDERED.

Dated: December 19, 2019

EDWARD J. DAVILA
United States District Judge