UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PAMELA MORENO,

Plaintiff,

v.

SAN FRANCISCO BAY AREA RAPID TRANSIT DISTRICT, et al.,

Defendants.

Case No.17-cv-02911-JSC

ORDER RE: MOTIONS TO DISMISS AND TO STRIKE

Re: Dkt. Nos. 41, 42, 43

Plaintiff Pamela Moreno brings this putative class action alleging that Defendants the San Francisco Bay Area Rapid Transit District ("BART") and Elerts Corporation violated California law through the clandestine collection of cell phone identifiers and location data via the BART Watch mobile application. Defendants have each moved to dismiss the First Amended Complaint ("FAC") for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6) and BART has moved to strike the class allegations under Federal Rule of Civil Procedure 12(f).[1] (Dkt. Nos. 41, 42, 43.) Having considered the parties' briefs and having had the benefit of oral argument on November 9, 2017, the Court GRANTS the motions to dismiss with leave to amend and DENIES the motion to strike as moot.

//

//

[1] The parties have consented to the jurisdiction of a magistrate judge pursuant to 28 U.S.C. § 636(c). (Dkt. Nos. 27, 28 & 29.)

BACKGROUND

A. Complaint Allegations

In 2014, BART, through its police department, partnered with Elerts to develop and launch the BART Watch mobile application ("BART Watch App" or "the App") for Android and IOS smartphones. (FAC (Dkt. No. 36) ¶ 25.) The App is marketed in the Google Play store as a way for the public to quickly and discreetly report suspicious activity directly to BART police by "send[ing] pictures, text messages, and locations of suspicious people of activities." (Id. ¶ 26.) An estimated 10,000 to 50,000 people have downloaded the App from the Google Play store. (Id. ¶ 27.)

When a user first downloads the App, the Google Play store advises the user that the App requires access to certain phone functionality to operate. (Id. ¶ 28.) In particular, it lists the following items that the App needs "access to": "location, phone, photos/media/files, camera, and device ID & call information." (Id.) The user must click "Accept" and then the App downloads onto the smartphone. (Id. ¶ 29.) When the user opens the App for the first time, the user must agree to the "Licensed Application End User License Agreement" ("User Agreement"). (Id.) A user cannot begin using the App until he or she has clicked "Yes, I Agree" at the end of the User Agreement. (Id. ¶ 30.) The next screen has a button labeled "Start Using" which the applicant must click before proceeding to actually using the App. (Id.) The "Start Using" screen prompts the user to input contact information so "BART can better assist you in case of an emergency." (Id.; Fig. 5-7.) This information is not required, but the message to this effect is not clear. (Id.) If users provide their contact information, the information is sent with their cellular phones' unique numeric identifier and a unique clientid is created and associated with the contact information. (Id. ¶¶ 33-34.) Even if users do not provide their contact information, their cellular phones' unique numeric identifier is transmitted "with the other tracking data." (Id. ¶ 35.) The App is programmed "to periodically transmit each transit user's clientid and precise location information to [Defendants'] servers." (Id. ¶ 36.) This location data includes "course," "elevation," and "speed." (Id. ¶¶ 37-38.)

The only reference to the collection of location information in the User Agreement is the

following paragraph:

> In addition, when you use the Licensed Application to submit reports, and if you have enabled location services permission for the Licensed Application, the Licensed Application automatically includes your location in the Content transmitted to ELERTS and that location may be used by ELERTS consistent with the rights granted to ELERTS to use Content.

(Id. ¶40.) In another paragraph regarding "Consent to Use of Data" the Agreement states that Defendants "collect unspecified 'technical information about your device, system and application software, and peripherals' for the purpose of 'facilitate[ing] the provision of software updates, product support and other services to you (if any) related to the Licensed Application." (Id. ¶ 42.) The User Agreement does not disclose that the App "secretly collect[s] transit users' unique cellular identifiers, periodically monitor[s] users' locations, and track[s] the identities of anonymous reporters." (Id. ¶ 31.) The App has a separate Privacy Policy that is accessible via a hyperlink at the end of the User Agreement following a paragraph which states that "[t]his Agreement constitutes the entire agreement between you and ELERTS relating to the Licensed Application and supersedes all prior or contemporaneous understandings regarding such subject matter." (Id. ¶ 42.)

Plaintiff Pamela Moreno downloaded the App in 2016 onto her Samsung Galaxy S7 and regularly uses it as part of her commute. (Id. ¶ 50.) When she first downloaded the App she was not aware that the App was designed to (and actually did) collect her smartphone's unique identifier and physical location and then transmit that information to Defendants. (Id. ¶ 51.) Plaintiff would not have downloaded the App or consented to collection and transmission of this information had she known. (Id. ¶¶ 52-53.)

B. Procedural History

Plaintiff filed this putative class action on May 22, 2017 alleging claims under (1) the Cellular Communications Interception Act, Cal. Gov't Code § 53166; (2) the Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750, et seq.; (3) the right to privacy under the California Constitution, Article I, Sec. 1; and (4) intrusion upon seclusion. (Dkt. No. 1.) Plaintiff attached the User Agreement and the Privacy Agreement as Exhibits A and B to the complaint,

respectively. (Dkt. Nos. 1-1 & 1-2.) BART thereafter filed a motion to dismiss and after Elerts appeared, the parties filed a stipulation for a consolidated briefing schedule on each Defendant's motion to dismiss. (Dkt. No. 30.)

While those motions were pending, Plaintiff filed her FAC. (Dkt. No. 36.) The FAC pleads class claims under (1) the Cellular Communications Interception Act, Cal. Gov't Code § 53166; (2) the California Constitution, Article I, Sec. 1, right to privacy; (3) intrusion upon seclusion; and (4) Cal. Pen. Code § 637.7. (Dkt. No. 36.) Although the FAC states that the User Agreement is attached as Exhibit A, it was not resubmitted. The FAC does not purport to reattach the Privacy Agreement. Both Defendants thereafter filed motions to dismiss the FAC for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6) and BART filed a motion to strike the class allegations under Federal Rule of Civil Procedure 12(f). (Dkt. Nos. 41, 42, 43.) Those motions are fully briefed.

DISCUSSION

Although each Defendant has filed its own motion to dismiss, the issues raised are largely the same. First, Defendants insist that Plaintiff's claims are barred because she consented to the very conduct she complains of here. Second, Defendants argue that Plaintiff cannot state a claim under California Penal Code § 637.7. Third, the Defendants maintain, albeit for different reasons, that California's Cellular Communications Interception Act does not apply to them. Fourth, Defendants contend that Plaintiff has failed to adequately plead her constitutional and common law privacy claims. Finally, BART separately moves to strike the class allegations as insufficiently pled. The Court addresses each argument in turn.

A. Plaintiff did not Consent to all of the Activity Alleged Here

As a threshold matter, Defendants insist that Plaintiff's claims fail because she consented to transmission of the at-issue information when she clicked "I agree" at the end of the User Agreement. Defendants rely primarily on language in the Privacy Policy to support their argument; however, on this record, and drawing all inferences in Plaintiff's favor, the Court cannot conclude as a matter of law that Plaintiff consented to the Privacy Policy.

In Nguyen v. Barnes & Noble Inc., 763 F.3d 1171 (9th Cir. 2014), the Ninth Circuit

outlined the contractual differences between "click-wrap" or "click-through" agreements and "browse-wrap" agreements. Id at 1176. The former requires the user to affirmatively assent to the terms of the agreement by clicking an "I Agree" button, whereas the latter "does not require the user to manifest assent to the terms and conditions expressly ... [a] party instead gives his assent simply by using the website." Id. (internal citation omitted). Id. The User Agreement is a click-wrap agreement—requiring the user to affirmatively check a box that says "Yes, I Agree" before accessing the App. The only reference to the Privacy Policy, however, is a single hyperlink to the Privacy Policy at the end of the User Agreement directly after a paragraph which states that the User Agreement "constitutes the entire agreement." (Compare FAC ¶ 30; Fig. 5-6 with FAC ¶ 42; Fig. 12.) Thus, a user could reasonably infer that by clicking "I Agree," the user is not agreeing to the Privacy Policy.

As a result, Defendants' argument prevails only if the Privacy Policy satisfies the requirements for a browse-wrap agreement that the user either had "actual notice" of its terms or "if the [App] puts a reasonably prudent user on inquiry notice of the terms of the contract." Nguyen, 763 F.3d at 1176-77. Where, as here, "a website makes its terms of use available via a conspicuous hyperlink ... but otherwise provides no notice to users nor prompts them to take any affirmative action to demonstrate assent" there is no constructive notice notwithstanding the "close proximity of the hyperlink to relevant buttons users must click on." Id. at 1178-79. Again, as alleged, the only reference to the Privacy Policy is a single hyper-link at the end of the User Agreement and it follows a paragraph which states that the User Agreement is the entire agreement; these words and format fail to put the user on either actual or constructive notice that the terms of the Privacy Policy are part of the User Agreement or that the user otherwise is agreeing to the Privacy Policy terms. See, e.g., In re Yahoo Mail Litig., 7 F. Supp. 3d 1016, 1029 (N.D. Cal. 2014) (concluding that users consented to both the terms of service and the privacy policy, which was accessible via a hyperlink, because the create account button followed the statement: "I agree to the Yahoo Terms and Privacy.").[2]

[2] Defendants' reliance on Yingling v. eBay, Inc., No. C 09-01733 JW, 2009 U.S. Dist. LEXIS 131776 (N.D. Cal. Nov. 4, 2009), is misplaced. The court there did not analyze whether the

Accordingly, the Court cannot conclude on this record that Plaintiff consented to the conduct alleged here.

B. California Penal Code § 637.7 Claim

California Penal Code § 637.7, adopted in 1998, 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.

Any person injured by a violation of this section, among others, may bring an action against the person who committed the violation for the greater of $5000 per violation or three times the actual amount of damages. Cal. Penal Code § 637.2.

Plaintiff alleges that the App is an "electronic tracking device" because it "causes electronic signals (i.e., internet traffic) to be transmitted from a smartphone to Defendants' servers, which include commuters' specific location information." (FAC ¶ 91.) Defendants argue that the BART Watch App is not a "device" under the statute, and even if it were, Plaintiff has not adequately alleged that the App can be used to determine the location or movement of a person. The Court agrees.

First, Plaintiff does not plausibly allege that the App determines Plaintiff's location or movement. The FAC alleges that a user's optional contact information is associated with a user's unique clientid (Dkt. No. 36 ¶ 33), and that the App is programmed to "periodically transmit each transit user's clientid and precise location information to their servers." (Id. ¶ 36.) But Plaintiff does not allege that she provided her contact information. (Id. ¶¶ 50-53.) Thus, there is no plausible allegation that the App tracked *Plaintiff's* location as opposed to some anonymous

---

plaintiff consented to the "final value fees" terms, and instead, just concluded that it was part of the agreement. Consent—the critical issue here—was never discussed.

clientid that is not matched to any particular person.

Second, Plaintiff does not plausibly allege that the App is an electronic tracking device within the meaning of the statute. Cal. Penal Code § 637.7(d). In interpreting a California statute, federal courts apply California rules of construction. 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. Southern Cal. IPA Med. Group, Inc., 86 Cal. App. 4th 919, 776 (2001). To determine that intent, a court looks first to the statute's language and gives effect to its plain meaning. California Teachers Assn. v. Governing Bd. of Rialto Unified School Dist., 14 Cal. 4th 627, 632–633 (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." People v. Snook, 16 Cal. 4th 1210, 1215 (1997). But language that appears unambiguous on its face may be shown to have a latent ambiguity; if so, a court may turn to customary rules of statutory construction or legislative history for guidance. Stanton v. Panish, 28 Cal.3d 107, 115 (1980).

Assuming that a cellphone qualifies as "a vehicle or other movable thing," the App is not "attached to" the cellphone. The ordinary meaning of "to attach" in this context is "to join or fasten (something) to something elese." See Attach, Oxford English Dictionary Online (http://www.oed.com/view/Entry/12698) (2017); Wasatch Property Management v. Degrate, 35 Cal.4th 1111, 1122 (2005) ("When attempting to ascertain the ordinary, usual meaning of a word, courts appropriately refer to the dictionary definition of that word."). The App is not "attached" to the cellphone; it is downloaded by the user into the cellphone.

Similarly, Plaintiff has not plausibly alleged that the App is a "device" within the meaning of section 637.7(d). A common meaning of "device" is "a thing made or adapted for a particular purpose, especially a piece of mechanical or electronic equipment." Google Dictionary, www.google.com/search?q=Dictionary (last visited December 14, 2017). Merriam-Webster defines "device" in relevant part as "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function," for example, "smartphones and other electronic devices or a "hidden recording device." See Device, Mirriam-Webster Online, (https://www.merriam-webster.com/dictionary/device) (2017). See Pope v. Superior Court, 136

Cal.App.4th 871, 876-77 (2006) (consulting online dictionary sources). A device could be "attached to" a moveable object, but software, such as the App, cannot.

The legislative history confirms that the statute governs electronic tracking devices placed on vehicles or other movable things (like a boat or plane) and not on software installed in mobile devices.[3] For example, the "purpose" of the bill was to "make it a misdemeanor to place an electronic tracking device on an automobile without the permission of the owner." (Dkt. No. 44-1 at 3.) Likewise, the bill analysis contains repeated references to regulat[ing] the placing of electronic tracking devices on automobiles." (Dkt. No. 44-3 at 2.) Plaintiff's only response to this history argues that "[t]he legislative history reveals a much broader scope of applicability than merely attaching tracking devices to cars; rather, the law's purpose was to generally "protect[] individuals from having their movements tracked by other private individuals.'" (Dkt. No. 46 at 28, n.7 (citing the same legislative history as referenced above, see Dkt. No. 44-3).) It is true that the statute is not limited to attaching devices to cars, but it is limited to attaching a device to a moveable object. Such facts are not alleged here.

Accordingly, Defendants' motion to dismiss the Penal Code § 637.7 claim is granted.

C. Cellular Communications Interception Act Claim

Next, Defendants maintain that Plaintiff also cannot state a claim under the Cellular Communications Interception Act. The Act, Cal. Gov't Code § 53166, enacted in January 2016, requires "[e]very **local agency** that operates **cellular communications interception technology"** to do the following:

> (1) Maintain reasonable security procedures and practices, including

[3] Elerts requests judicial notice of three documents reflecting the legislative history of Senate Bill 1667 (which became Penal Code § 637.7): (1) Senate Committee on Public Safety Analysis, Privacy: Electronic Tracking Device, SB 1667; (2) Office of Senate Floor Analysis, Statement on SB 1667 – Electronic Tracking Devices; and (3) Assembly Republican Bill Analysis, SB 1667. (Dkt. No. 44.) Pursuant to Federal Rule of Evidence 201, "[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." See also Territory of Alaska v. American Can Co., 358 U.S. 224, 226-27 (1959) (holding that courts, when interpreting statutes, may take judicial notice of "legislative history"). Plaintiff here has not objected to Elert's request for judicial notice. Accordingly, the Court GRANTS the Request for Judicial Notice as to Exhibits 1-3 which are part of the public record and easily verifiable.

> operational, administrative, technical, and physical safeguards, to protect information gathered through the use of cellular communications interception technology from unauthorized access, destruction, use, modification, or disclosure.
>
> (2) Implement a usage and privacy policy to ensure that the collection, use, maintenance, sharing, and dissemination of information gathered through the use of cellular communications interception technology complies with all applicable law and is consistent with respect for an individual's privacy and civil liberties. This usage and privacy policy shall be available in writing to the public, and, if the local agency has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site...

Cal. Gov't Code § 53166(b)(1) & (2) (emphasis added). An individual harmed by a knowing violation of this statute is entitled to the greater of actual damages or liquidated damages of not less than $2500.00. Id. at § 53166(d).

1. Local Agency

The Act defines a "local agency" as "any city, county, city and county, special district, authority, or other political subdivision of the state, and includes every county sheriff and city police department." Id. § 53166(a)(2). Elerts insists that it is not a "local agency" as defined by the statute. Plaintiff does not attempt to argue that Elerts is a local agency, but instead maintains that Elerts should be treated as an extension of the government itself because it "participates in the provision and management of core government functions—in this case, public safety on public transportation." (Dkt. No. 46 at 21:11-14 (citing Amalgamated Food Emps. Union Local 590 v. Logan Valley Plaza, Inc., 391 U.S. 308, 318 (1968); Fashion Valley Mall, LLC v. N.L.R.B., 172 P.3d 742, 754 (Cal. 2007)). Even if this principle were to extend to this context—of which the Court is skeptical—the FAC is devoid of allegations that Elerts has taken on provision and management of core functions. To the contrary, the FAC alleges that BART paid Elerts approximately $300,000 to develop the BART Watch App. (FAC ¶ 25.) Plaintiff's alternative suggestion that Elerts could be held liable under a theory of vicarious liability is no more availing as there are similarly no allegations which would give rise to vicarious liability or agency relationship. Finally, even if there were, Plaintiff has failed to point to anything which suggests that Section 53166 allows for vicarious liability. Accordingly, Elerts motion to dismiss the

Section 53166 claim must be granted.

2. Knowing Violation of the Statute

The statute provides a private right of action against a person "who knowingly caused a violation" of the statute. Gov't Code § 53166(d). Plaintiff insists that its allegation that "Defendants' targeting and collection of unique cellular identifiers is not incidental to usage of any part of the App but reflects Defendants' intentional and out of the ordinary programming choice" is sufficient to satisfy its obligation to allege that BART knowingly violated the statute. Not so. Plaintiff alleges that Bart paid Elerts "$300,000 for the development of the BART Watch App." (Dkt. No. 36 at ¶ 25.) There are no allegations that plausibly suggest that BART had any knowledge of the functionality alleged by Plaintiff. See Starr v. Baca, 652 F.3d 1202, 1216 (9th Cir. 2011) (holding that a claim is facially plausible when it "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.").

Accordingly, BART's motion to dismiss the Section 53166 claim likewise must be granted.

D. Constitutional and Common Law Privacy Claims

1. Constitutional Privacy Claim

The California Constitution creates a privacy right that protects individuals from the invasion of their privacy by private parties. Am. Acad. of Pediatrics v. Lungren, 16 Cal. 4th 307, 327 (1997). To establish a claim under the California Constitutional right to privacy, a plaintiff must first demonstrate three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 35–37 (1994). "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." Id. at 37.

Here, Plaintiff alleges that (1) she has a "legally protected privacy interest in preventing government agencies (and the private companies helping them) from collecting without consent their unique cellular numeric identifiers and locations" (FAC ¶ 69); (2) that she did not consent to

collection of this information (id. ¶ 74); and (3) Defendants' secret collection and transmission of unique cellular numeric identifiers and locations violates her right to privacy pursuant to Article I, Section 1 of the California Constitution (id. ¶ 75.)

Defendants insist that this conduct is not so egregious as to amount to a violation of social norms relying on two cases in this district which have granted motions to dismiss privacy claims. See, e.g., In re iPhone Application Litig., 844 F.Supp.2d 1040, 1063 (N.D. Cal. 2012); In re Google, Inc. Privacy Policy Litig., 58 F.Supp.3d 968, 988 (N.D. Cal. 2014). In re iPhone Application Litig. involved the disclosure to third parties of a user's unique device identifier number, personal data, and geolocation information. 844 F.Supp.2d at 1063. The court held that "[e]ven assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms." Id. In re Google, Inc. Privacy Policy Litig. involved a challenge to Google's privacy policy which allowed Google to comingle user data across accounts and disclose it to third-parties for advertising purposes. 58 F.Supp.3d at 974.[4]

Plaintiff insists that her case is more analogous to that of Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 973 (N.D. Cal. 2015), where the court likewise granted a motion to dismiss concluding that "defendants' tracking of a vehicle's driving history, performance, or location 'at various times,' is not categorically the type of sensitive and confidential information the constitution aims to protect." Plaintiff maintains that the court dismissed the claim there because—unlike here—the plaintiffs' allegations were not sufficiently detailed with respect to who was collecting the data, how and how often it was collected, and what was collected. Plaintiff contends that her allegations that the App is programmed to collect the data regarding Plaintiff's geographic location and unique cellular identifier at periodic intervals are more detailed. The Court is not persuaded that the allegations here are in fact distinguishable from those in Cahen.

[4] In Opperman v. Path, Inc., 205 F. Supp. 3d 1064, 1078-79 (N.D. Cal. 2016), the court rejected the reasoning of both these cases and held that the plaintiffs' allegations that Yelp surreptitiously obtained access to the plaintiff's address book within their contacts app and reviewed and retained the information therein without the plaintiff's knowledge adequately stated a claim of invasion of privacy. The anonymous data here is different from an address book.

Plaintiff's allegation of monitoring "at periodic intervals" is indistinguishable from *Cahen's* allegation of monitoring "at various times."

Drawing all reasonable inferences in Plaintiff's favor, Plaintiff's allegations are insufficient to satisfy the third element of the constitutional invasion of privacy claim: a reasonable user would find that Defendants' periodic transmitting to their servers of her anonymous clientid (there is no allegation she provided her contact information) and location is an egregious breach of social norms. Plaintiff concedes that prior to downloading the App, she had to accept that the App would have "access to" her "location, phone, photos/media/files, camera, and device ID & call information." (FAC ¶¶ 28-29.) She was thus on notice that BART would be accessing this information. Further, users download the BART Watch App so that they can report suspicious activity happening on BART—it is implicit that the App would need to provide BART police with the user's location to do so. How else would the police know where to go? Indeed, the App clearly states that it will use a user's location to do so even—and especially—in the case of an anonymous report. That BART also "periodically" accesses this information even when the user is not using the App is not an egregious violation of social norms. While Plaintiff suggests that BART does so for a nefarious purpose, she does not allege facts to plausibly support such an inference. Indeed, she does not allege that BART uses the data for any purpose, or even that BART was aware of the data collection. All she alleges is that the App periodically transmits the data to Defendants' servers. In this age of mobile technology the Court cannot conclude that a reasonable user would consider it highly offensive or egregious that a voluntarily downloaded mobile application which utilizes the user's cell phone identifier and location data when the app is in use, also "periodically" accesses that anonymous data while the application is not in use.

The motion to dismiss Plaintiff's constitutional privacy claim is therefore granted.

2. Intrusion on Seclusion Claim

Under California law, a claim for intrusion upon seclusion has two elements: (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), as modified on denial of reh'g (July 29, 1998); see also Restatement (Second) of Torts § 652B (1977) ("One who

intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person").

Plaintiff's allegations with respect to her intrusion on seclusion claim mirror her allegations with respect to her constitutional right to privacy. As such, they fail to adequately allege a claim for intrusion on seclusion for the same reasons. The motion to dismiss this claim is granted as well.

CONCLUSION

For the reasons explained above, Defendants' motions to dismiss are GRANTED with leave to amend. Plaintiff's amended complaint, if any, shall be filed within 30 days of this Order. The motion to strike the class allegations is denied as moot.

This Order disposes of Docket Nos. 41, 42, 43.

IT IS SO ORDERED.

Dated: December 14, 2017

JACQUELINE SCOTT CORLEY
United States Magistrate Judge

United States District Court
Northern District of California