UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL GONZALES,

Plaintiff,

v.

UBER TECHNOLOGIES, INC., et al.,

Defendants.

Case No. 17-cv-02264-JSC

ORDER RE MOTION TO DISMISS FIRST AMENDED COMPLAINT

Re: Dkt. No. 38

Plaintiff Michael Gonzales brings this action on his own behalf and as a putative class action for Lyft drivers whose electronic communications and whereabouts were allegedly intercepted, accessed, monitored, and/or transmitted by Defendants Uber Technologies, Inc., Uber USA LLC, and Raiser-CA (together, "Uber"). Now pending before the Court is Defendants' motion to dismiss Plaintiff's First Amended Complaint ("FAC"). (Dkt. No. 38.) Having carefully reviewed the parties' briefing and having had the benefit of oral argument on January 11, 2018, the Court GRANTS Defendants' motion with leave to amend.

FIRST AMENDED COMPLAINT ALLEGATIONS

A. The Lyft App

"Lyft provides technology that operates similar to a taxi company's dispatch system." (Dkt. No. 34 ¶ 3.) "A rider requests a ride using a software application on his or her phone (the 'Lyft App')." (*Id.*) After a rider logs on to the Lyft App, the App sends a Hypertext Transfer Protocol ("HTTP") request to Lyft's servers. (*Id.* ¶ 65.) The HTTP request contains the passenger's Lyft ID and GPS coordinates. (*Id.* ¶ 66.) Lyft's servers respond to the Lyft App's request with a list of nearby drivers who are logged in and who have affirmatively indicated they are available for work; the list includes the drivers' Lyft IDs and GPS coordinates. (*Id.* ¶ 67.) The

list is transmitted to riders through Lyft's servers. (*Id*.) "The locations of nearby Lyft drivers are displayed to the rider as dots on a map, along with the estimated price and wait time for arrival once the ride request is submitted." (*Id*. at ¶ 3.)

"Drivers also use the Lyft App." (*Id*. ¶ 4.) "When a driver is ready to accept work, the driver swipes a switch on the Lyft App, directing the Lyft App to continuously transmit the driver's geolocation data and his or her willingness to accept work to servers maintained by Lyft." (*Id*.) Lyft drivers used the Lyft App to communicate with Lyft servers by transmitting and receiving "packets" of information. (*Id*. ¶ 55.) "A packet is analogous to a physical letter mailed from one address to the other, and the protocol used to transmit the packet is analogous to the physical envelope that holds the letter." (*Id*.) "While traditional envelopes use physical postal addresses, . packets use computer Internet Protocol (IP) addresses." (*Id*. ¶ 70.) The digital letter transmitted from the driver to Lyft's servers in response to a rider's HTTP request includes (1) the driver's unique identifier, (2) the driver's precise geolocation data, (3) the driver's affirmation that the driver is available to provide rides for Lyft users, and (4) an estimated price for the rider's requested ride. (*Id*. ¶ 72.) Lyft, acting as the driver's agent, forwards a driver's geolocation and willingness to drive to those requesting a ride. (*Id*. ¶ 4.)

B. Uber's Hell Spyware

Uber offers technology that competes with the Lyft App and operates in the same geographic regions as Lyft. (*Id*. ¶¶ 5, 6.) Some drivers perform transport services through the two platforms simultaneously. (*Id*. at ¶ 6.) Lyft's and Uber's systems store the location of every driver, whether on duty or off duty, every few seconds. (*Id*. ¶¶ 87, 88.) "[N]either Uber nor Lyft ever delete the geolocation data they collect from drivers, at least in part because they consider it valuable to their respective businesses." (*Id*. ¶ 90.)

Starting in 2014 or earlier and continuing into 2016, Uber secretly used 'Hell spyware' to access servers and smartphones owned and operated by Plaintiff, Class Members, and Lyft. (*Id*. ¶ 52.) The "spyware extracted information from Lyft by posing as Lyft customers in search of rides." (*Id*. ¶ 7.) These fake Lyft riders sent forged requests to Lyft's servers. (*Id*.) When Lyft's servers received "a request from a forged rider account, they believed that the ride requests were

coming from actual Lyft riders, not the Hell spyware." (*Id.* ¶ 77.) As a result, Lyft's servers transmitted a response to Uber's fake Lyft requesters containing the IDs, on duty status, pricing, and exact locations of nearby Lyft drivers. (*Id.*) "The data transmitted was provided by Lyft drivers and was only intended to be delivered to actual nearby Lyft riders." (*Id.*)

Uber used the fraudulently received geolocation data and driver identifiers "to create grid-like detection nets over cities including San Francisco, Los Angeles, and New York." (*Id.* ¶ 80.) For instance, a forged rider account would transmit a request indicating that the rider was at the Philip Burton Federal Building with specific GPS coordinates. (*Id.*) In response, Lyft's servers "would transmit back information for all nearby Lyft drivers." (*Id.*) The Hell spyware would simultaneously also send another set of requests indicating that a different fake Lyft rider was a few blocks north on O'Farrell Street with specific geolocation data . (*Id.*) This process was repeated with a large number of fake Lyft accounts, "allowing Uber to obtain complete geographic coverage of entire metropolitan areas, and the exact locations of all Lyft drivers and other information." (*Id.*) "Uber repeated this process millions of times using the Hell spyware from 2014 through 2016." (*Id.* ¶ 8.)

Uber used the data collected in conjunction with other databases "to learn personal details about Lyft drivers including, but not limited to, the drivers' full names, their home addresses, when and where they typically work each day and for how many hours, and where they take breaks." (*Id.* ¶ 83.) "Uber was able to use this data to determine the identities of the drivers' rider customers." (*Id.*)

"Uber combined the data harvested by Hell [spyware] with Uber's internal records, including historical location data, to identify Lyft drivers who also worked for Uber." (*Id.* ¶ 9.) "Uber used the information gleaned from Hell to direct more frequent and more profitable trips to Uber drivers who also used the Lyft App." (*Id.* ¶ 101.) "By inundating these drivers [with] Uber rides, Uber was able to discourage drivers from accepting work on the Lyft platform, reducing the effective supply of available Lyft drivers." (*Id.* ¶ 101.) "With the supply of Lyft drivers reduced, Lyft customers faced longer wait times." (*Id.* ¶ 102.) As a result, Lyft riders would cancel the ride requested with Lyft and request a new ride from Uber, and Lyft drivers experienced decreased

earnings. (*Id*. ¶¶ 9, 102.) "Over time, this would reduce the effectiveness of the Lyft App, thus harming drivers such as Plaintiff and absent Class Members." (*Id*. ¶ 102.)

PROCEDURAL HISTORY

Plaintiff filed an initial complaint seeking injunctive relief and damages based on four claims: (1) Federal Wiretap Act as amended by the Electronic Communications Privacy Act (the "ECPA"), (2) the California Invasion of Privacy Act ("CIPA"), (3) the California Unfair Competition Law (the "UCL"), and (4) common law invasion of privacy. (Dkt. No. 1.) Defendants moved to dismiss all four claims. (Dkt. No. 17.) The Court granted Defendants' motion with leave to amend. (Dkt. Nos. 27.)

Plaintiff then filed a First Amended Complaint seeking the same relief under the same causes of action with two additional claims: (1) the Federal Stored Communication Act (the "SCA") and (2) the California Computer Fraud and Abuse Act (the "CFAA"). (Dkt. No. 34.) Thereafter, Defendants filed the now pending motion to dismiss. (Dkt. No. 38.)

DISCUSSION

I. Federal Claims

A. The Wiretap Act

The Federal Wiretap Act makes it unlawful to "intentionally intercept [ ] ... any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). "Intercept" "means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Plaintiff's Wiretap Act claim fails because he has not alleged and cannot allege that Uber "intercepted" the "contents" of a communication.

1. *Contents of a Communication*

Plaintiff alleges that when he activates the Lyft App he sends Lyft his unique Lyft driver identification, his precise geolocation data, his affirmation that he is willing to provide rides to drivers, and an estimated price for the ride (presumably only when there is a rider request). (FAC ¶ 72.) With the possible exception of the estimated price, this information does not qualify as the "contents" of a communication within the meaning of the Wiretap Act.

The Act defines "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). "'[C]ontents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014). Record information includes the "name," "address," and "subscriber number or identity" of a subscriber or customer. *Id.* (citing 18 U.S.C. § 2702(c)(2)). For example, data about a telephone call, including the number from which it was made, the time it was made, the number called, and the length of the call does not fall within the Wiretap Act because it is not the content of the communication, it is data about the communication. *United States v. Reed*, 575 F.3d 900, 917 (9th Cir. 2009). Similarly, an individual's Facebook ID and the url of the webpage the individual was viewing are not the contents of a communication when that information is automatically generated when the individual clicks an app or game icon. *In re Zynga Privacy Litig.*, 703 F.3d at 1107-09. It follows, then, that Plaintiff's IP address and unique Lyft driver ID are not the contents of a communication within the meaning of the Act.

Plaintiff's geolocation data is also record information rather than the content of a communication; the data is automatically generated when Plaintiff activates the Lyft App. (FAC ¶ 4.) *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) ("the allegedly intercepted electronic communications are simply users' geolocation data. This data is generated automatically, rather than through the intent of the user, and therefore does not constitute 'content' susceptible to interception"); *In re Carrier IQ, Inc.*, 78 F.Supp.3d 1051, 1082 (N.D. Cal. 2015) ("[t]he geographic location of a mobile device at any given time has likewise been deemed to be non-content information."); *Cousineau v. Microsoft Corp.*, 922 F.Supp.2d 1116, 1127 (W.D. Wash. Jun. 22, 2012) ("contents" as used in the Wiretap Act is not broad enough to encompass geolocation data). While a text message stating "I am at 6th and Broadway" would constitute content, the automatic generation of geolocation data is record information.

Plaintiff insists that the geolocation data is content because Uber used it to "(1) locate drivers, (2) identify drivers who also drove for Uber, (3) identify which drivers were available for

new rides, (4) track prices that Lyft would offer for trips, and (5) identify how many cars were available to pick up riders at a particular location." (Dkt. No. 41 at 27.) Assuming as the Court must that these allegations are true, none of that information involves a communication from the Lyft driver, let alone the content of such a communication. Further, nothing in the Wiretap Act suggests that *how* an intercepting party uses a communication determines whether the communication involves "content" within the Act's meaning.

The "content" analysis may be different as to pricing information; however, there are no allegations in the FAC that suggest that Plaintiff *intended* to communicate pricing information. *See In re Zynga Privacy Litig.*, 750 F.3d at 1106 ("Congress intended the word 'contents' to mean a person's intended message to another"). Pricing is discussed twice: paragraphs 3 and 72. Paragraph 72 states: "Lyft drivers who are ready to work send digital letters to Lyft. Each letter has a number of components that are directly analogous to a physical letter" including "an estimated price for the ride." Simply because Plaintiff sends a "letter" to Lyft that includes an estimated price does not mean the Lyft driver *intends* to communicate that price. There are no allegations that the Lyft driver had the ability to set the price of a Lyft ride or how price is determined or even whether the Lyft driver is aware of the price communicated to Lyft's servers. Indeed, paragraph 3 supports an inference that Lyft sets the price or that it is automatically generated by the Lyft App. When a Lyft rider opens the App, "[t]he locations of nearby Lyft drivers are displayed to the rider as dots on a map." (FAC ¶ 3.) In other words, the Lyft rider first sees the cars in her area that are willing to provide rides. Then, after the Lyft rider submits her request, she can see "the estimated price and wait time for arrival." (*Id.*) Accordingly, the FAC does not allege that the driver intended to communicate an estimated price. Thus, it is not the content of a communication by Plaintiff.

At oral argument Plaintiff also argued that the content of the driver's message is "the fact they're available to work." (Dkt. No. 48 at 7:5-7.) In other words, Plaintiff contends that it can be inferred from the driver's toggling on of the App that the driver is available to work. That is one inference that can be drawn; another is that the driver toggled on whether he wants to work or not. The only communication, then, is that the driver toggled on—a communication more akin to

record information than content. In *In re Zynga*, for example, the Ninth Circuit distinguished between the address of a Facebook webpage a user is viewing and a Google search URL that not only shows that a user is using the search engine but also the specific *search terms* the user communicated to Google. 750 F.3d at 1108. The court explained:

> Under some circumstances a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication. But the referer header information at issue here includes only basic identification and address information, not a search term or similar communication made by the user, and therefore does not constitute the contents of a communication.

Id. Under Plaintiff's interpretation of "content," the information as to the webpage the user was viewing is "content" because it could be inferred that the user was communicating he wanted to view that webpage, just as, according to Plaintiff, from the act of toggling on it can be inferred that driver is available to accept rides. But *In re Zynga* rejects such a broad reading of content. In other words, simply opening a webpage or mobile application is not a communication with content.

Accordingly, Plaintiff has not alleged facts sufficient to satisfy the "contents" prong of the Wiretap Act.

2. *Intercept*

Plaintiff also does not allege facts that plausibly suggest that Uber "intercepted" any of *his* communications. *See* 18 U.S.C. § 2520(a) (any person whose wire, oral or electronic communications were intercepted may bring a civil action). The Wiretap Act defines "intercept" as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). The term "acquisition" is not defined in the statute, but the Ninth Circuit, looking at the term's "ordinary meaning," has defined it as the "act of acquiring, or coming into possession of." *United States v. Smith,* 155 F.3d 1051, 1055 n.7 (9th Cir. 1998). Further, to be "intercepted" it must have been "acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). A narrow definition of "intercept" which requires

acquisition contemporaneous with transmission is most "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" *Konop*, 302 F.3d at 878.

Drawing all reasonable inferences in Plaintiff's favor, the FAC does not allege that Uber intercepted a communication from Plaintiff. Plaintiff alleges that his driver ID and geolocation information were sent to Lyft's servers. (FAC ¶ 56.) Lyft then took the information it received from Plaintiff and other nearby drivers and sent it to Uber (pretending to be an actual Lyft customer). (FAC ¶ 67.) Thus, the communication Uber acquired is a communication from Lyft and not Plaintiff and therefore Lyft did not intercept Plaintiff's communications.

Plaintiff's new "sniffer" allegations do not change the outcome. That Uber used network analyzers to decode TCP packets sent from Lyft's servers to the App is insufficient because Plaintiff has not pled the identity of the person using the Lyft App or that Uber was intercepting TCP packets or other communications that were sent by Plaintiff.

Plaintiff alleges that Uber posed as fake Lyft riders to determine the location of Lyft drivers. These fake accounts sent messages to Lyft, which sent a message back to Uber with nearby Lyft driver locations. The communications occurred directly between Lyft and Uber posing as Lyft riders; there was no contemporaneous transmission between Plaintiff and Lyft that was *stopped* or *interrupted* by Uber. *See Konop,* 302 F.3d at 878. That Uber was pretending to be a legitimate Lyft rider is of no moment; Plaintiff has still not alleged the interception of a communication from *Plaintiff* to a third party.

Plaintiff's reliance on *United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010), is unpersuasive. In *Szymuszkiewicz*, the plaintiff set up a rule in Microsoft Outlook to direct his boss's emails to his account. The Seventh Circuit held that the servers in question make copies of the boss's messages "within a second of each message's arrival and assembly" with no more than an eyeblink in between each message, and therefore the defendant's acquisition of the emails constituted contemporaneous interception. Here, unlike *Szymuszkiewicz*, there were no messages between existing Lyft drivers and Lyft riders that were copied contemporaneously by Uber; instead, as alleged, the acquired messages traveled directly and only between Lyft and Uber acting

as a Lyft rider.

Accordingly, Plaintiff has not plausibly alleged an "interception" under the Wiretap Act.

***

In light of Plaintiff's failure to plausibly plead that Uber intercepted the content of a communication from Plaintiff, the Court declines to consider Uber's other arguments. The federal Wiretap Act is dismissed with leave to amend, but only to the extent Plaintiff can allege consistent with Rule 11 that Uber intercepted the content of a communication from Plaintiff.

B. Stored Communications Act ("SCA")

Uber also argues that Plaintiff fails to state a claim under the Stored Communications Act. "The Stored Communications Act provides a cause of action against anyone who 'intentionally accesses without authorization a facility through which an electronic communication service is provided ... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.'" *Theofel v. Farley-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (citing 18 U.S.C. §§ 2701(a)(1)). The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication." 18 U.S.C. § 2510(17)(A), (B). "[S]ubsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient." *Theofel*, 359 F.3d at 1075. "By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission." *Id*. at 1072-1073.

Plaintiff's SCA claim fails because he has not alleged facts that plausibly suggest that the communications were in "electronic storage"; that is, that the communications were temporary or were in storage for the purpose of back-up protection. Plaintiff alleges that Lyft's and Uber's systems store the location of every driver, whether on duty or off duty, every few seconds and that neither Uber nor Lyft ever delete the geolocation data they collect from drivers. (FAC ¶¶ 87, 88, 90.) Given this information is never deleted, the communications at issue are not stored temporarily and therefore do not fall under section (A). Nor does section (B) apply: Plaintiff has not pled that the communications Lyft stores on its servers is backup information. Indeed,

Plaintiff admits that he has not made any such allegation, but he asserts that he cannot do so without discovery and thus should be excused. The case he relies on to support his argument, *In re Intuit Privacy Litigation*, 138 F. Supp. 2d 1272 (C.D. Cal. 2001), was decided before the United States Supreme Court's decisions in *Bell Atlantic v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 602 (2009), and thus is not persuasive.

Uber also argues that Plaintiff has not plausibly alleged "unauthorized access" to a stored communication. It contends that because Plaintiff alleges that Uber (while pretending to be a legitimate Lyft rider) *requested* the information that Lyft then provided, Uber cannot have engaged in unauthorized access. The Court is unpersuaded. Plaintiff alleges that Uber violated Lyft's terms of service and falsely posed as a Lyft rider to gain access to that information; Uber does not explain how such access is authorized. Indeed, it appears directly analogous to "the busybody who get permission to come inside by posing as meter reader" and is thus trespassing. *Thoefel*, 359 F.3d at 1073.

Uber's lament that Plaintiff has not shown that Lyft's servers qualify as a "facility" under the Stored Communications Act reverses the burden of proof. On Uber's motion to dismiss it is its burden to show that the servers cannot possibly qualify as a "facility." It has not met that burden.

Nonetheless, as Plaintiff has not alleged facts that plausibly suggest that the communications Uber allegedly accessed without authorization are "backups," the Stored Communications Act claim must be dismissed. The dismissal will be with leave to amend to allege facts that show that Uber accessed communications in "electronic storage."

II. State Claims

A. California Invasion of Privacy Act ("CIPA")

The CIPA is California's anti-wiretapping and anti-eavesdropping statute that prohibits unauthorized interceptions of communications in order "to protect the right of privacy." Cal. Penal Code § 630. "The analysis for a violation of CIPA is the same as that under the federal Wiretap Act." *See NovelPoster v. Javitch Canfield Group*, 140 F.Supp.3d 938, 954 (N.D. Cal. Aug. 4, 2014) (citing cases). The FAC alleges violations of two CIPA sections, 632 and 637.7.

Uber argues Plaintiff's CIPA claim fails because (1) Plaintiff "fails to allege Uber 'eavesdropped' on any 'confidential communications' (as required by Section 632") and (2) Plaintiff consented to his smartphone tracking his location, triggering the exception to a Section 637.7 violation. (Dkt. No. 38 at 19:11-14.)

1. *Section 632*

California Penal Code section 632 makes it unlawful to "intentionally and without the consent of all parties to a confidential communication, use[] an electronic amplifying or recording device to eavesdrop upon or record the confidential communication." "California courts interpret 'eavesdrop,' as used in section 632, to refer to a third party secretly listening to a conversation between two other parties." *Thomasson v. GC Services Ltd. P'ship*, 321 Fed. App'x 557 (9th Cir. 2008) (citing *Ribas v. Clark*, 38 Cal.3d 355, 363 (1985); *Rogers v. Ulrich*, 52 Cal.App.3d 894, 899 (1975)); *see also Flanaghan v. Flanaghan*, 27 Cal.4th 766, 775 (2002) (Penal Code section 632 prohibits "unconsented to eavesdropping or recording of conversations"). Plaintiff contends Uber collected data from messages Lyft sent to Uber, acting as a Lyft rider. Plaintiff has not alleged that Uber "eavesdropped" on communications between Lyft drivers and legitimate Lyft riders or between Lyft drivers and Lyft. Accordingly, Plaintiff's Section 632 CIPA claim fails.

Plaintiff's only argument as to why the allegations here somehow constitute eavesdropping is to claim that the Ninth Circuit's decision in *Thomasson* is not good law in light of *Kight v. Cashcall, Inc.*, 200 Cal.App.4th 1377 (2012). But this argument makes no sense. *Kight* did disagree with *Thomasson's* conclusion that a company could not eavesdrop on its own employee's conversations with customers because the employee and employer were considered the same party. *Id.* at 1394. But *Kight* did not hold that section 632 prohibits something other than eavesdropping or recording a communication between two other people. To the contrary, consistent with *Thomasson* and the other California cases cited above, *Kight* held that section 632 "expressly prohibits surreptitious monitoring without the consent of 'all parties' to the conversation and specifically imposes liability on a corporation for improper eavesdropping." *Id.* at 1393. Plaintiff has not alleged any such conduct; accordingly, the section 632 claim fails.

2. *Section 637.7*

Section 637.7 prohibits the "use [of] an electronic tracking device to determine the location or movement of a person," but there is no violation if the "owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle." *Id*. § 637.7(a)–(b). Plaintiff alleges that he consented to the use of his smartphone as a tracking device with respect to whatever vehicle he is using when he signed up to be a Lyft driver. (Dkt. No. 34 ¶ 93.)

Plaintiff argues his 637.7 claim cannot be dismissed because consent is an affirmative defense. However, the language regarding consent is found in the statute itself, under Section 637.7(b):

> (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.

In any event, even if it is an affirmative defense on which Uber bears the ultimate burden of proof, Uber has met that burden based on Plaintiff's own allegations. (Dkt. No. 34 ¶ 93.)

Plaintiff next urges that no valid consent was "transferred" to Uber. The statute's plain language, however, does not require consent be given to the person doing the tracking; instead, it says that the statute does not apply if the vehicle's owner, lessor or leseee "consented to the use of the electronic tracking device with respect to that vehicle." Cal. Penal Code § 637(b). The only case Plaintiff cites to support his argument, *People v. Barnes*, 216 Cal.App.4th 1508 (2013), does not address the issue here: consent to one party and not to a third party (Uber) under Section 637.7. Instead, *Barnes* concerned the victim of a theft who consented to Sprint and police officers to track her phone to apprehend the person who stole the victim's phone. 216 Cal.App.4th at 1511-1512. The *Barnes* court concluded there is no Fourth Amendment violation when the information generated by the GPS, with the owner's consent, is only a part of the objective reasons leading to the decision to detain. *Id*., 216 Cal.App.4th at 1519. *Barnes* is thus inapposite.

The plain language of Section 637.7 states that the statute does not apply when the owner of a vehicle consents to the use of the tracking device with respect to the same vehicle. The statute

does not distinguish to whom consent is given and this Court is unaware of any authority that holds consent is limited to particular parties. Plaintiff consented to the tracking of his vehicle through his cellphone when he signed up to be a Lyft driver. Accordingly, Plaintiff's Section 637.7 claim fails and shall be dismissed without leave to amend.

B. Computer Data Access and Fraud Act ("CDAFA")

The California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502, "expand[s] the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." *Id.* § 502(a). Plaintiff alleges Uber violated subdivisions (c)(1)–(3), (5), and (7). In particular, parroting the language of the subsections, Plaintiff conclusorily alleges that Uber:

- knowingly accesses and without permission used data, or a computer, or a computer system, or a computer network, in order to wrongfully control or obtain money, property, or data, contrary to Cal. Penal Code § 502(c)(1)
- knowingly accessed and without permission took, copied, or made use of data from a computer, computer system, or computer network, or took or copied and supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network, contrary to Cal. Penal Code § 502(c)(2)
- knowingly [and without permission] used or caused to be used computer services, contrary to Cal. Penal Code § 502(c)(3)
- knowingly and without permission disrupted or caused the disruption of computer services or denied or caused the denial of computer services to an authorized user of a computer, computer system, or computer network, contrary to Cal. Penal Code § 502(c)(5)
- knowingly and without permission provided or assisted in providing the a means of accessing a computer, computer system, or computer network in violation of Cal. Penal Code § 502, contrary to Cal. Penal Code § 502(c)(7).

(Dkt. No. 34 ¶¶ 125-129.)

These boilerplates allegations do not survive Rule 8. Did Uber use data, a computer or a computer system to wrongfully obtain money? How did Uber disrupt or deny the use of computer services? What was it that it did without permission? Neither Uber nor the Court should have to guess how Plaintiff contends these subsections were violated. Further, the Act provides that "the

owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief." Cal. Penal Code § 502(e)(1). Thus, Plaintiff must allege that Uber accessed *Plaintiff's* computer, computer system, etc. He has not done so.

Accordingly, Plaintiff' claim under the California Comprehensive Computer Data Access and Fraud Act is dismissed with leave to amend to the extent Plaintiff can allege facts that plausibly suggest Uber violated a particular subsection of the Act.

C. Invasion of Privacy

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 state a claim under the California constitutional right to privacy, a plaintiff must allege 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. The California Supreme Court recently held that while less sensitive than medical history or financial data, home contact information is generally considered private. *Williams v. Superior Court*, 3 Cal.5th 531, 554 (2017).

Plaintiff alleges that Uber used the data collected from Lyft in conjunction with other databases to learn personal details about Lyft drivers including, but not limited to, drivers' full names, when and where they typically work, where they take breaks, and the drivers' home addresses. (Dkt. No. 34 ¶ 83, 92.)

Plaintiff has sufficiently pled a protected privacy interest as to home addresses, *see Williams*, 3 Cal.5th at 554, and arguably precise geolocation data. *See U.S. v. Jones*, 565 U.S. 400, 411 (concluding the GPS tracking device of a vehicle, and the subsequent use of that device to monitor the vehicle's movements on public streets, was a search within the meaning of the

Fourth Amendment requiring a warrant). Plaintiff, however, offers no authority to support his argument that the other information Uber allegedly obtained is generally considered private - Lyft ID number, working as a Lyft driver, and full names. The Court concludes it is not.

The second element, a reasonable expectation of privacy under the circumstances, is not met. "A 'reasonable' expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill,* 7 Cal.4th at 37. The decision "must take into account any 'accepted community norms,' advance notice to [Plaintiff] ..., and whether [Plaintiff] had the opportunity to consent to or reject the very thing that constitutes the invasion." *TBG Ins. Servs. Corp. v. Superior Court,* 96 Cal.App.4th 443 (2002). The plaintiff in an invasion of privacy action must have conducted himself or herself in a manner consistent with an actual expectation of privacy, i.e., he or she must not have manifested by his or her conduct a voluntary consent to the invasive actions of defendant. *Hill,* 7 Cal.4th at 26. The "community norms" aspect of the "reasonable expectation of privacy" element means that "the protection afforded to the plaintiff's interest in his privacy must be relative to the customs of the time and place, to the occupation of the plaintiff and to the habits of his neighbors and fellow citizens." *TBG Ins. Servs. Corp.*, 96 Cal.App.4th at 450.

Plaintiff consented to the sharing of his geolocation data with perfect strangers (Lyft riders); thus, under the circumstances he did not have a reasonable expectation of privacy in such information. (Dkt. No. 34 ¶ 93.)

Plaintiff may have toggled on from home and thus, since Uber was allegedly tracking the location of Lyft drivers, Uber could have determined Plaintiff's home address. (Dkt. No. 34 ¶ 92.) However, under the circumstances the drivers did not have a reasonable expectation of privacy in their home location. Most Lyft users, both drivers and riders, can expect that their home addresses will be shared with other users on the platform when using the Lyft App. As such, users cannot reasonably expect that this information will remain private.

Plaintiff argues his consent was limited to Lyft and therefore Plaintiff had a reasonable expectation that only Lyft would have access to his information. However, "the case law suggests that in determining whether a plaintiff has satisfied the elements of the claim, a plaintiff's lack of

consent does not matter so much as the nature of the information in which he or she alleges a privacy interest." *See In re Yahoo*, 7 F.Supp.3d at 1040-1041; *see also In re iPhone Application Litig.*, 844 F.Supp.2d at 1063 ("[e]ven assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure [of information including device identifier number, personal data, and geolocation information] does not constitute an egregious breach of social norms").

Nor is the third element, a serious invasion, met. "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. Thus, the extent and gravity of the invasion is an indispensable consideration in assessing an alleged invasion of privacy." *Hill*, 7 Cal. at 37. "The California Constitution sets a high bar for establishing an invasion of privacy claim." *In re Yahoo Mail Litigation*, 7 F.Supp.3d 1016, 1038 (N.D. Cal. Aug. 12, 2014) (citing *Belluomini v. Citigroup, Inc.*, No. CV 13–01743 CRB, 2013 WL 3855589, at *6 (N.D. Cal. July 24, 2013)). "Even disclosure of very personal information has not been deemed an 'egregious breach of social norms' sufficient to establish a constitutional right to privacy." *Id.* (citing *In re iPhone Application Litig.*, 844 F.Supp.2d at 1063) (holding that the disclosure to third parties of unique device identifier number, personal data, and geolocation information did not constitute an egregious breach of privacy sufficient to prove a serious invasion of a privacy interest); *Ruiz v. Gap, Inc.*, 540 F.Supp.2d 1121, 1127–28 (N.D. Cal. Mar. 24, 2008), *aff'd*, 380 Fed.Appx. 689 (9th Cir. 2010 (unpublished) (holding that the theft of a retail store's laptop containing personal information, including the social security numbers, of job applicants did not constitute an egregious breach of privacy and therefore was not sufficient to state a claim).

In *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4th 986, 992 (2011), the "supposed invasion of privacy essentially consisted of [defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements." The court concluded the defendant's actions were not an egregious breach of social norms but were instead routine commercial behavior. *Id.* Here, similar to *Folgelstrom*, Uber allegedly obtained Plaintiff's name and home address; however, there is no allegation as to what Uber did, if anything, with this

information. Indeed, it appears that Plaintiff is alleging only that Uber could have obtained his home address, not that it in fact intentionally did so. Without more allegations as to what, if anything, Uber did with this information, Plaintiff has not plausibly alleged a serious invasion of privacy.

Plaintiff's reference to his allegation that Uber obtained the names of Lyft's customers is puzzling as he does not explain how that translates into a serious invasion of *Plaintiff's* right to privacy.

Accordingly, the Court grants Defendants' motion to dismiss Plaintiff's constitutional invasion of privacy claim with leave to amend.

D. Unfair Competition Law

California's Unfair Competition Law ("UCL") prohibits, and provides civil remedies for, "unfair competition," defined as "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200 et seq. Its purpose "is to protect both consumers and competitors by promoting fair competition in commercial markets for goods and services." *Kasky v. Nike, Inc.*, 27 Cal.4th 939, 949 (2002).

Private parties can sue under the UCL only if, as a result of unfair competition, they have: (1) suffered an injury in fact, (2) lost money or property, and (3) the economic injury was a "result of" the unfair competition. *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 322, 326 (2011); Cal. Bus. & Prof. Code § 17204. The "lost money or property" requirement means plaintiff "must demonstrate some form of economic injury such as surrendering more or acquiring less in an transaction, having a present or future property interest diminished, being deprived of money or property, or entering into a transaction costing money or property that was unnecessary. *Id*. at 323. "At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice." *Id.* at 27.

Plaintiff alleges that by encouraging drivers to use the Uber platform exclusively, and not also drive for Lyft, that reduced the supply of Lyft drivers thereby increasing wait times and causing Lyft drivers to experience decreased earnings; in particular, the longer wait time would cause a passenger to cancel the Lyft request and request a new ride from Uber. (FAC ¶ 9, 101,

102.) These factual allegations, which the Court must accept as true, are sufficient to satisfy the lost money or property requirement of UCL standing.

Plaintiff also urges that Uber's unauthorized "interception of communications constitutes cognizable injury." (Dkt. No. 41 at 34:10-11.) However, the sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes. *See Campbell v. Facebook*, 77 F.Supp.3d 836, 849 (N.D. Cal. Dec 23, 2014) (concluding the courts "have consistently rejected" a broad interpretation of "money or property" to include personal information); *Archer v. United Rentals, Inc.*, 195 Cal.App.4th 807, 816 (2011) (holding that an invasion of a right to privacy through the collection of private information is not "lost money or property" conferring UCL standing). Nonetheless, he has sufficiently alleged that he lost revenue as a result of Uber's programs to decrease the supply of Lyft drivers. Whether Plaintiff will be able to prove that allegation is a question for another day.

Accordingly, Plaintiff has alleged standing to bring a UCL claim. The Court is unpersuaded that at this stage of the litigation Plaintiff cannot pursue equitable relief.

CONCLUSION

For the reasons described above Uber's motion to dismiss is GRANTED as to all claims except the UCL claim. Plaintiff is granted leave to file an amended complaint as to all claims except the CIPA section 637.7 claim as amendment as to that claim would be futile. Plaintiff is not given leave to add any new claims; leave is only to correct, if possible, deficiencies in the allegations of the claims already pled. The second amended complaint shall be by May 18, 2018. Uber's request for judicial notice of Lyft's terms of service is GRANTED given the document is referenced in the FAC and its accuracy is not reasonably questioned. *See* Fed. R. Evid. 201(b)(2). Plaintiff's request for judicial notice is DENIED given the Jacobs letter from the *Waymo* litigation is not discussed in the FAC nor relevant to this matter.

//

//

//

//

//

This Order disposes of Docket No. 38.

IT IS SO ORDERED.

Dated: April 18, 2018

JACQUELINE SCOTT CORLEY
United States Magistrate Judge

United States District Court
Northern District of California