AUDET & PARTNERS, LLP
MARK BURTON (SBN 154061)
Email: mburton@audetlaw.com
MICHAEL MCSHANE (SBN 127944)
Email: mmcshane@audetlaw.com
221 Main Street, Suite 1460
San Francisco, CA 94105
(415) 568-2555
(415) 568-2556

ZIMMERMAN REED LLP
CALEB MARKER (SBN 269721)
Email: caleb.marker@zimmreed.com
2381 Rosecrans Ave., #328
Manhattan Beach, CA 90245
(877) 500-8780 Telephone
(877) 500-8781 Facsimile

Attorneys for Plaintiff and for the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MICHAEL GONZALES, individually, and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

UBER TECHNOLOGIES, INC., a Delaware corporation; UBER USA, LLC, a Delaware limited liability company; RAISER-CA. LLC, a Delaware limited liability company; and, DOES 1 to 10, inclusive,

Defendants.

Case No. 3:17-cv- 02264-JSC

Assigned for all purposes to the Honorable Jacqueline Scott Corley

PLAINTIFF'S RESPONSE IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S CLASS ACTION COMPLAINT

Hearing Date: August 31, 2017
Time: 9:00 a.m.
Courtroom: F-15th Floor

Date Action Filed: April 24, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Other Authorities

Regulations

INTRODUCTION

Make no mistake, this is a case about industrial espionage. Defendants (hereinafter collectively referred to as "Uber") did not record publicly broadcast information; Uber hacked into its competitor's computer systems and accessed confidential data, including the identities and real-time locations of Lyft drivers, without their knowledge, consent, or authorization. Plaintiff and the Class intended to broadcast their availability for work and current location only to nearby Lyft customers seeking rides, through Lyft's proprietary and protected computer systems. Through hacking and trickery, Uber was able to disguise its identity, intercept, and siphon off these confidential communications by tricking Lyft's systems into providing the same communications to Uber. Uber then used that restricted information to gain a competitive advantage, improve the Uber platform and harm the Lyft platform, diminishing the earnings of Lyft drivers. Compl. ¶6.

In this case, a group of Uber employees designed software that deceived Lyft's computer systems into thinking it was a large number of Lyft customers in need of rides. In response, Lyft securely transmitted confidential information to the fake customers, in violation of the Lyft *Terms of Service* that Uber attempts to use in its motion. Paragraph 9 of the standard terms that Lyft, its drivers and customers entered into, captioned "Restricted Activities" makes clear that all agreed that the data was private information and Uber's attempt to access it and "surreptitiously intercept or expropriate any system, data or personal information" through its impersonation was strictly prohibited. *See* Lyft Terms of Service ¶9 (a, d, g, h, i, j l, m, n, p). Uber too agreed to these terms, when disguising itself as Lyft riders and establishing the phony accounts.

Uber's conduct is similar to early telephone phreaking and computer hacking, where the goal is to breach defenses and exploit weaknesses in a computer system or network. Uber succeeded in hacking Lyft's computer system. (See, Defendants' Memorandum of Points and Authorities in support of Motion to Dismiss, Doc. 17, hereinafter "Mot." or "Motion"). Uber then used the information obtained through its clandestine efforts to direct ride-share business to Uber and away from Lyft and Lyft drivers. Compl. ¶¶58-59. Uber's conduct damaged Plaintiff and the Class, because, as described in the Complaint, the information was obtained by Uber under false pretenses and used to Lyft drivers' competitive disadvantage. Compl. ¶¶6, 48-49, 58-59.

FACTUAL BACKGROUND

Uber and Lyft are fierce competitors in the ride-sharing market. Compl. ¶26. Uber and Lyft are the two dominant providers of ride-share services. Compl. ¶¶26, 49. Plaintiff worked as a Lyft driver from 2014 until November 2016 in the San Francisco Bay Area, including San Francisco, San Jose, and San Mateo County. Compl. ¶¶16-17. Plaintiff never worked for Uber. Compl. ¶18.

A. Uber hacked into Lyft's computer systems using fake rider accounts.

In or around 2014, Uber's competitive intelligence, or "COIN" group secretly developed spyware dubbed "Hell." Compl. ¶49 (9:1-2). The Complaint, incorporating a public news report, describes Hell as follows:

> Hell started like this: Uber created fake Lyft rider accounts and used commonly available software to fool Lyft's system into thinking those riders were in particular locations, according to the person. (That in and of itself is a violation of Lyft's terms of service, which prohibits users from "impersonat[ing] any person or entity," which Lyft riders must agree to when they open the app.)
>
> The spoofed Lyft accounts made by Uber then could get information about as many as eight of the nearest available Lyft drivers who could accommodate a ride request. Uber made sure that in each city where it was competing with Lyft, the fake rider locations were organized in a grid-like format so that it could view the entire city.
>
> In other words, Uber could see, nearly in real time, all of Lyft's drivers who were available for new rides—and where those drivers were located. That also allowed Uber to track the prices Lyft would offer to riders for certain trips, and how many cars were available to pick up riders at a particular time in one city or another.
>
> * * *
>
> Another goal of the program was to make sure Uber steered rides more reliably to Uber drivers who were also available on the Lyft network than to those who weren't, this person said.

Compl. ¶49 (9:25-10:5, 19-22).[1] In other words, Uber used computer hardware and software to send out fake ride requests to Lyft in order to obtain a list of nearby drivers. Uber created a grid of hundreds or thousands of other fake rider accounts placed throughout major cities like San Francisco that allowed

[1] While in their motion, Defendants refer negatively to the "single online article" which Plaintiff cites in his complaint, other mainstream publications such as CNBC, *Fortune*, and *Vanity Fair*, also reported on Uber's secret Hell program in April 2017. *See* Farber, Uber Reportedly Had a Secret 'Hell' Program to Track Lyft Drivers, Forbes, April 13, 2017, *available at* http://fortune.com/2017/04/13/uber-lyft-hell/ (last visited July 14, 2017); Kharpal, *Uber reportedly used secret software called 'Hell' to track rival Lyft drivers*, CNBC, April 13, 2017, *available at* http://www.cnbc.com/2017/04/13/uber-lyft-hell-software-track-drivers.html (last visited July 14, 2017); Kosoff, *Uber Used A Secret Program Called "Hell" To Track Rival Drivers*, Vanity Fair, April 15, 2017, *available at* http://www.vanityfair.com/news/2017/04/uber-used-a-secret-program-called-hell-to-track-rival-drivers (last visited July 14, 2017).

Uber to monitor Lyft drivers around entire cities with its net of fake Lyft accounts, and then used that information to Uber's competitive advantage and Lyft drivers' disadvantage.

B. The hacked system contained sensitive, private information.

The data hacked by Uber contained sensitive, private information that Uber was not authorized to use. Lyft's standard Terms of Service that all Lyft drivers and Lyft riders agree to confirms that information shared through the Lyft platform is private and absolutely not to be used for the types of activities Uber engaged in. *See* Lyft Terms of Service (Ex. 1) ¶9 (a, d, g, h, i, j l, m, n, p).[2] The allegations in the Complaint confirm that Uber violated these terms. The Terms of Service also confirms that Uber's conduct impersonating Lyft drivers to mine data on the Lyft platform to Lyft's and Lyft drivers' detriment was a "restricted activity." *Id.* ("With respect to your use of the Lyft Platform and your participation in the Services, you agree that you will not…(a.) impersonate any person or entity; …(h.) manipulate identifiers… (i.) ..'frame' or 'mirror' any part of the Lyft Platform… (l.) …use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, scrape, 'data mine', or in any way reproduce or circumvent the navigational structure or presentation of the Lyft platform or its contents.").[3] Uber itself agreed to these terms when it clandestinely signed up as Lyft riders in order to operate the Hell spyware program.

Of considerable value to Uber was Plaintiff and the Class' real-time GPS location, the fact they worked for Lyft, their unique Lyft ID, and that they were available to work (collectively, the "Sensitive Geolocation Data" or "SGD"). This information was confidentially provided by class members to Lyft in order to obtain rides from Lyft's customers and earn money.

> Location Information. Lyft is all about connecting Drivers and Riders. To do this, we need to know where you are. *When you open Lyft on your mobile device, we receive your location.* We may also collect the precise location of your device when the app is running in the foreground or background. *If you label certain locations, such as "home" and "work," we receive that information, too.*

[2] Plaintiff agrees with Uber that it is proper for the Court to consider Lyft's Terms of Service, along with other documents such as Lyft's privacy policy and Uber's terms, are authentic and integral to the Complaint. *See e.g. Chesapeake Bay Found., Inc. v. Severstal Sparrows Point, LLC*, 794 F. Supp. 2d 602, 611 (D. Md. 2011). In addition, Plaintiff has attached exhibits such as motions, declarations, and an order resulting from Uber's challenge to a government subpoena for its driver lists which the Court may properly take judicial notice of as a matter of public record.

[3] *See also* Lyft Terms of Service ¶10(e) ("…you represent, warrant and agree that: …(e) You will not make any misrepresentation regarding…your status as a driver.").

> Your location information is necessary for things like matching Riders with nearby Drivers, determining drop off and pick up locations, and suggesting destinations based on previous trips. Also, if the need ever arises, our Trust & Safety team may use and share location information to help protect the safety of Lyft Users or a member of the public. In addition to the reasons described above, Drivers' location information and distance travelled is necessary for calculating charges and insurance for Lyft rides. If you give us permission through your device settings or Lyft app, we may collect your location while the app is off to identify promotions or service updates in your area.

Lyft Privacy Policy, at 2(B) (emphasis added), attached hereto as Exhibit "2".

The Lyft Privacy Policy confirms that the SGD data unlawfully recorded by Uber includes private information, such as the location of class members on public roadways, but also wherever their smartphone is when the Lyft app is logged in, including their home, work, or other places inside buildings. This is not information one could record by simply standing on a street corner looking for automobiles with Lyft's trade dress decal on the windshield. Hell allowed Uber to see thousands of Lyft drivers at once all across a city, and importantly compare Lyft driver's relative locations and distances so as to be able to exploit that private and proprietary data not for Lyft's exclusive benefit, but rather, for Uber's. Thus, Uber acted to completely undercut the Lyft platform. Unlike Uber's Hell, human beings cannot see through buildings or track a driver once they are out of sight. Only by following every single driver with another human could Uber have amassed the same kind of data, which is all but impossible because it would have required placing humans on every street corner in every major city. Even if Uber had followed every driver, it would not have known if the driver was available for work because the driver has to manually input that information into the Lyft app. Lastly, without Hell, Uber would be unable to follow Lyft drivers into their homes, offices, restaurants, or any other location, while they awaited their next fare. Many class members turn their Lyft app on, mark themselves ready for work while still at home, and then get into their car once they receive their first passenger. Others leave the Lyft app running and indicate they are available for work until they get home. Using this information, Uber could easily discern class members' home addresses and work schedules. If the Lyft driver ever had an Uber account, Uber could cross-reference those locations and determine the identity of the class member or could accomplish the same using public databases containing consumer names and contact information.

In sum, the SGD could contain, at a minimum, the following sensitive information: (1) precise geolocation data of class members' cell phones in 2014, 2015, and 2016; (2) class members' unique

Lyft ID number; (3) that class members' are employed by Lyft; (4) the dates and times that class members' indicated that they were available to work; (5) the locations of class members' homes, offices, and other locations; (6) the full names and identity of class members using geolocation data such as start and stop locations; and (7) the full names and identity of class members using Uber's own location data associated with driver and passenger records.

C. Uber derived a substantial business advantage from the confidential data and inflicted an economic injury on Plaintiff, Lyft, and Members of the Class.

Recruiting drivers to drive for Uber is one of Uber's biggest expenses and the total amount Uber spent recruiting through advertising and marketing may have exceeded $1 billion in 2016. Compl. ¶49 (9:22-24). Having enough drivers is key to Uber's business model as a transportation provider, because when riders wait too long they may cancel their ride request and seek transportation with one of Uber's competitors, such as Lyft, a taxicab, or public transit. Hell was key to this challenge. Uber cross-referenced the known locations of its drivers with the Lyft driver locations obtained with Hell. Uber was then able to determine which Lyft drivers were "dual apping" and working for both Uber and Lyft. Once known, Uber was able to steer more rides to dual Uber/Lyft drivers over standalone Uber drivers through its "privileged dispatch" program, which aimed to "squeeze Lyft's supply of drivers." Compl. ¶¶49 (10:19-25, 58). This resulted in a shortage of Lyft drivers and a surplus of standalone Uber drivers. For consumers, this meant longer wait times for a Lyft driver and shorter wait times for an Uber driver. Compl. ¶¶6, 59. This inherently harmed the Lyft marketplace and drove consumers to rely on Uber instead of Lyft. *Id.* This reduced demand for the services provided by Plaintiff and the Class. In addition to the privileged dispatch, Uber used the data from Hell to direct bonuses, financial incentives in exchange for a minimum number of rides, and other incentives that allowed Uber to: (1) reduce its recruiting and retention costs; and (2) harm the Lyft market, thereby reducing the earnings of Plaintiff and the Class. *Id.*

D. Lyft drivers had an expectation of privacy in their confidential data.

The information contained in the SGD, with a potentially infinite amount of historical waypoints that Uber intercepted and amassed in real time over several years, paints a vivid, intimate portrait of one's life. While class members may expect their whereabouts to be known by Lyft as well

as by individual customers during single trips, they have no expectation that Uber could monitor their locations continuously . In 2012, the FTC noted that:

> The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both *sensitive information* (*e.g.*, health information, *precise geolocation information*) and less sensitive information (*e.g.*, purchase history, *employment history*) to unauthorized third parties.[4]

The FTC further explained that there are many known and unknown uses that could violate the privacy of smartphone users, such as the Class:

> The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. … The Wall Street Journal has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique ID associated with a particular mobile device – that can then be used to track and predict consumer behavior.2 Not surprisingly, consumers are concerned: for example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.

FTC Rep., at 33. The FTC noted that the public comments it received from consumers and industry "reflect a general consensus that information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data is sensitive and merits heightened consent methods," and that "before collecting such data, companies should first obtain affirmative express consent from consumers." FTC Rep., at 58-59. Of course Uber obtained no such consent. Compl. ¶¶55, 67.

The surveys cited by the FTC show that the U.S. public is greatly concerned with their location being tracked and logged. Nielsen notes that "most mobile app downloaders … are concerned about privacy when it comes to sharing their location via mobile phone[], with 59 percent reporting they have privacy concerns compared to 52 percent of male app downloaders."[5] One survey shows that 65% of smartphone users are concerned or very concerned about their location being tracked.[6] Likewise, courts

[4] F.T.C. Rep., Protecting Consumer Privacy in an Era of Rapid Change (Mar. 2012) ("FTC Rep.") (emphasis added), at 8, *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. (Ex. 3).

[5] *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NielsenWire Blog (Apr. 21, 2011), *available at* http://www.nielsen.com/us/en/insights/news/2011/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location.html/ (Ex. 4).

[6] Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* (Mar. 2011), at 8, *available at*

in this District routinely find that individuals have an expectation of privacy in their historical geolocation data.[7] Here, Plaintiff and the Class had an expectation that their SGD would not be intercepted and recorded by Uber and used in the way that it was. Compl. ¶¶8, 53, 90, 91.

E. Lyft's driver lists and employment data are confidential trade secrets.

Plaintiff and the Class believe that Lyft's list of drivers and the drivers' SGD is a confidential trade secret (but still subject to discovery). Uber agrees. It has been fighting the efforts of the City of San Francisco to turn over its driver lists, which is a small piece of what Uber was able to obtain from Lyft using Hell. In opposing San Francisco's subpoena, Uber argued that the City's subpoena violated the driver's privacy rights.[8] In arguing against disclosure, Uber relied in part on the declaration of its Operations Manager, Michael Colman, who attested to the following:

> 8. Following the launch of the Uber App, other competitors have emerged that utilize a business model similar to Uber. I believe these competitors closely monitor Uber's present and past business strategies, including the number of drivers using the Uber App.
>
> 9. Competitors may be interested in the number of drivers using the Uber App for a variety of reasons. For example, they may wish to evaluate the marketplace, including estimated rider and driver wait times. Uber engages in various promotional campaigns, direct advertising, and incentive to attract drivers, and I believe competitors likely do the same based on market demand.
>
> 10. The number of drivers who use the Uber App is proprietary business information that Uber guards through security measures to prevent disclosure to the public. Uber maintains safeguards to prevent disclosure relating to drivers using the Uber App in part because it would put Uber at a competitive disadvantage if this information was publically available.[9]

See also Uber Technologies, Inc.'s Motion to Seal in *City & Cty. of S. F. v. Uber Techs., Inc.*, No. CPF-17-515663, at *2 (Sup. Ct. S. F. Cty.) (filed June 2, 2017) ("Because of these competitive reasons, Uber

---

http://aa-download.avg.com/filedir/other/Smartphone.pdf (reporting that 64% of consumers worry about their location being tracked when using their smartphones) (Ex. 5).

[7] *See In re Application for Tel. Info. Needed for a Criminal Investigation*, 119 F. Supp. 3d 1011 (N.D. Cal. 2015) (on appeal); *United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015), at *6-8 (N.D. Cal. Mar. 2, 2015).

[8] Uber Technologies, Inc.'s Opposition to Motion for Order to Require Uber to Disclose Driver Contract Information, *City and County of San Francisco v. Uber Technologies, Inc.*, No. CPF-17-515663 at *13-15 (Sup. Ct. San Francisco Cty.)(filed June 2, 2017) (Ex. 6).

[9] Decl. of Michael Colman in *City &Cty. of S. F. v. Uber Techs., Inc.*, No. CPF-17-515663, at *13-15 (Sup. Ct. S. F. Cty.)(filed May 24, 2017) (Ex. 7).

protects the information about the number of drivers and keeps it confidential….If the information were to be publically available, the harm to Uber would be substantial. Specifically, it would expose information that provides it certain competitive advantages Uber enjoys in many markets across the globe. There would be no way for Uber to mitigate the potential harm if the information becomes publically available.").[10]

Uber's representations and sworn testimony in *City & Cty. of S. F.* conclusively establish that the very data at issue here is confidential and protected. Shockingly, through the Uber Hell program, Uber intentionally acted to secretly obtain the very same sensitive data that it claimed was protected and would cause unmitigatable harm were it to fall into the hands of a competing ride-share service.

In turn, there is no dispute that Lyft's list of drivers, which Lyft considers its software licensing customers, is not known or readily ascertainable, cannot be derived from public sources, and could not be reproduced regardless of the investment. Confidential customer lists are trade secrets in California. *See, e.g., Abba Rubber Co. v. Seaquist,* 235 Cal. App. 3d 1, 21 (Cal. Ct. App. 1991). Moreover, California law dictates that the customer lists of employer customers with job orders with an employment agency, here Lyft, constitutes a trade secret and confidential information. Cal. Bus. & Prof. Code § 16607(a). Uber acted in bad faith to obtain such data.

F. Uber was not authorized to access the SGD.

Uber unconvincingly argues that the data it accessed was publically available, on the theory that class members broadcast the SGD with a megaphone. Not true. Lyft's Privacy Policy informs class members that "[w]hen you open Lyft on your mobile device, [Lyft] receive[s] your location." (Ex. 2.) First, Uber is not Lyft. Second, it is the comparative distances between Lyft drivers and Lyft riders that is sensitive and protected, while on the other hand of value to Uber. Third, Uber's team of hackers violated Lyft's Terms of Service by pretending to be hundreds or thousands of fake Lyft riders. This was not public information as Uber itself recognizes in *City & Cty. of S. F.*. Instead, as shown above, Uber's conduct plainly violated Paragraphs 9 and 10 of Lyft's Terms of Service. The SGD was

[10] While ultimately the court determined that disclosing the identities of Uber's drivers to the tax authority did not violate the driver's right to privacy, that does not alter Uber's admission that the type of data it took from Lyft was proprietary and private. Order dated June 22, 2017 (Ex. 8); Motion to Seal (Ex. 9).

intended to be used to pair available drivers and customers, and securely transmitted to nearby riders. Uber tricked Lyft's systems into believing that it was legitimate riders and was then able to intercept communications sent to actual riders in the vicinity. Lyft intended to securely broadcast this information to the next nearby customer, but Uber used Hell to intercept the data that was being sent to Lyft customers. Uber's access into Lyft's computer systems was illegal, surreptitious, and unauthorized. Compl. ¶52-53.

Passengers using the Lyft app do not receive the exact GPS coordinates of eight nearby drivers, nor do they receive their unique Lyft IDs. Rather, consumers only see a map of the nearby area with small icons of vehicles moving around the area. Presumably, the placement of those vehicle icons is dictated by coordinates transmitted by Lyft to a customer's phone, which is the vulnerability that Uber likely took advantage of to gain access to this information.

Lastly, none of the "Other Sharing" exceptions listed in Section 4(b) of Lyft's Privacy Policy apply here. Lyft's platform and ride-sharing services are not open to members of the general public: one must have a Lyft account which includes a username and password and agreement to be bound by the Terms of Service. In order to create a Lyft account, you must agree to and adhere to Lyft's terms. As discussed below, Uber's Hell spyware violated more than half of them. Lyft's Terms clearly prohibited Uber from hacking into its computer systems and posing as fake Lyft riders:

> With respect to your participation in the Local Partnerships Program, you agree that you will not:
>
> a. impersonate any person or entity;
> b. stalk, threaten, or otherwise harass any person, or carry any weapons;
> c. violate any law, statute, rule, permit, ordinance or regulation;
> d. interfere with or disrupt the Lyft Platform or the servers or networks connected to the Lyft Platform;
> f. post information or interact in a manner which is false, inaccurate, misleading (directly or by omission or failure to update information), defamatory, libelous, abusive, obscene, profane, offensive, sexually oriented, threatening, harassing, or illegal;
> g. use the Lyft Platform in any way that infringes any third party's rights, including but not limited to: intellectual property rights, copyright, patent, trademark, trade secret or other proprietary rights or rights of publicity or privacy;
> h. post, email or otherwise transmit any malicious code, files or programs designed to interrupt, damage, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or surreptitiously intercept or expropriate any system, data or personal information;
> i. forge headers or otherwise manipulate identifiers in order to disguise the origin of any information transmitted through the Lyft Platform;

k. modify, adapt, translate, reverse engineer, decipher, decompile or otherwise disassemble any portion of the Lyft Platform or any software used on or for the Lyft Platform;

m. use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, scrape, "data mine", or in any way reproduce or circumvent the navigational structure or presentation of the Lyft Platform or its contents;

p. cause any third party to engage in the restricted activities above.

Lyft Terms of Service, at ¶9 (Ex. 1.) The allegations in the Complaint allege that Uber violated many of Lyft's terms, including, but not limited to, a, b, c, d, f, g, h, i, k, m, and p.[11] As such, Uber's intrusion into Lyft's computer systems was unauthorized.

LEGAL STANDARD

Dismissal under Federal Rule of Civil Procedure 12(b)(6) "is appropriate only where the complaint lacks a cognizable legal theory or sufficient facts to support a cognizable legal theory." *Mendiondo v. Centinela Hosp. Med. Ctr.*, 521 F.3d 1097, 1104 (9th Cir. 2008). When deciding whether to grant a motion to dismiss, the court may consider material submitted as part of the complaint or relied upon in the complaint, and may also consider material subject to judicial notice. *See Lee v. City of Los Angeles*, 250 F.3d 668, 688–89 (9th Cir. 2001). Because of the drastic nature of a motion to dismiss and the importance of safeguarding a plaintiff's right to a trial, "to affirm this type of dismissal, it must appear to a certainty that the plaintiff would not be entitled to relief under any set of facts that could be proved." *W. Reserve Oil & Gas Co. v. New*, 765 F.2d 1428, 1430 (9th Cir. 1985); *see also, Halet v. Wend Inv. Co.*, 672 F.2d 1305, 1309 (9th Cir. 1982).

The court must accept as true all allegations of material fact offered by the non-moving party and draw all justifiable inferences in the light most favorable to the non-moving party. *See N. Star Int'l v. Arizona Corp. Comm'n*, 720 F.2d 578, 580 (9th Cir. 1983). In the event a complaint is deemed deficient, "[i]t is black-letter law that a district court must give plaintiffs at least one chance to amend… absent a clear showing that amendment would be futile." *Nat'l Council of La Raza v. Cegavske*, 800 F.3d 1032, 1041 (9th Cir. 2015); *see also Martin v. Tradewinds Beverage Co.*, No. CV16-9249 PSG (MRWX), 2017 WL 1712533, at *12 (C.D. Cal. Apr. 27, 2017) ("The Court… may deny leave to

[11] Ironically, Uber places similar restrictions on the use of its application, precluding, *inter alia*, the "attempt to gain unauthorized access to or impair any aspect of the Services or its related systems or networks," demonstrating the confidential nature of the communications and information transmitted therein. Uber Terms of Service ("Restrictions" § vi) (Ex. 10).

amend if plaintiff has repeatedly failed to cure deficiencies or if amendment would be futile."). In the event that the Court finds Plaintiff's allegations insufficient, Plaintiff requests leave to amend the Complaint.

ARGUMENT

I. Plaintiff Asserts Valid Claims for Violations of the Wiretap Act.

The Wiretap Act prohibits the intentional interception of any wire, oral, or electronic communication. 18 U.S.C. § 2511(1)(a). Defendants argue that Plaintiff has failed to allege (1) an interception, (2) of protected communications, (3) of the 'contents' of those communications, and (4) from an applicable device. Defendants are wrong on all counts.

A. Plaintiff alleges Defendants' intentional interception of wire, oral, or electronic communications.

Defendants' first argument in support of dismissing Plaintiff's Wiretap Act claims is predicated on the erroneous proposition that they failed to physically intercept any communications. Mot. at 4. The act defines the term "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." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 877 (9th Cir. 2002) (quoting 18 U.S.C. § 2510(4)). As the ordinary meaning of "intercept" is to "stop, seize, or interrupt in progress or course before arrival," "acquisition contemporaneous with transmission" is a critical element of the Wiretap Act. *Id.* at 878.

Defendants' only support for the argument that Plaintiff fails to allege "acquisition contemporaneous with transmission" is that the Northern District of Ohio recently dismissed purportedly similar accusations in *Cobra Pipeline Co. v. Gas Nat., Inc.*, 132 F. Supp. 3d 945, 952-53 (N.D. Ohio 2015). *Cobra* is inapposite. The plaintiffs in *Cobra* predicated their Wiretap Act claims on interception of information where there was no intended recipient. *Id.* at 953. Specifically, the data acquired came from GPS tracking service trucks, which was routed through a cellular communication tower, processed in an operation center, and then made available to users on a web portal. *Id.* at 987–48. The system then stored the data for historical review. *Id.* at 948. Plaintiffs brought suit after learning that Defendant (a former employee) continued to use the web portal after termination. *Id.* at 947. In response to Defendants' Motion for Summary Judgment, plaintiffs did not even address the

allegation that no communications were "intercepted." *Id.* at 952–53. Thus, the court held the data was accessed "at the expected end-point of the transmission." *Id.* at 953.

Here, Plaintiff alleges that Defendant intercepted communications "nearly in real time." Compl. ¶49. Plaintiff alleges that the program interfered with Plaintiff's (and Lyft's) system by "fooling" it into thinking there were riders in particular locations, "organized in a grid-like format so that it could view the entire city." *Id.* Plaintiff has alleged interference with communications contemporaneous with transmission, as without this 'real time' interception and interruption of Plaintiff's and Lyft's systems, Defendants' program would have been all but useless. Plaintiff's allegations satisfy the traditional definition of "intercept" articulated by *Konop*.

As the Court in *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 2027–28 (N.D. Cal. 2014) noted, arguments that contradict Plaintiffs' allegations cannot be considered in a motion to dismiss. "In other words, until the Court can determine when and how [defendant] intercepted users' emails, the Court must accept as true Plaintiffs' allegation that they were accessed while 'in transit.'" *Id.* at 1028 (denying motion to dismiss Wiretap Act claim on the basis that the Wiretap Act does not apply to the emails at issue). *See also*, *In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1082 (N.D. Cal. 2015) (holding that where there were no allegations in plaintiffs' complaint that interception occurred while the communications resided in storage, allegations that communications were intercepted contemporaneously with their transmission is sufficient to state a claim under the Wiretap Act); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 841 (N.D. Cal. 2014) (holding that the issue of whether a communication was intercepted during transmission is premature at the motion to dismiss stage of litigation). At a minimum, the question of "interception" presents myriad fact issues and is otherwise not suitable for resolution at this stage in the litigation.

B. Plaintiff alleges the intercepted communications were protected by the Wiretap Act.

Defendants' next argument against Plaintiff's wiretap claim is that the Wiretap Act does not protect communications that are "readily accessible to the public." Mot. at 6. Although the Wiretap Act does not protect against interceptions "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public" (18 U.S.C. § 25111(2)(g)(i)), the definition of "readily accessible" is not as narrow as Defendants would

like this Court to believe. As Plaintiff alleges interception of electronic communications (as opposed to less private forms of communication, like radio transmissions), the ordinary meaning of "readily accessible" applies. *See, e.g.*, *In re Google Inc. St. View Elec. Comms. Litig.*, 794 F. Supp. 2d 1067, 1073 (N.D. Cal. 2011), *aff'd sub nom. Joffe v. Google, Inc.*, 729 F.3d 1262 (9th Cir. 2013). Where plaintiffs plead "that Defendant intentionally created, approved of, and installed specially-designed software and technology… and used this technology to intercept Plaintiffs' data packets," plaintiffs have sufficiently alleged that the communications intercepted were not readily accessible to the general public. *Id.* at 1082. As this Court noted in *In re Google Inc. Street View*:

> Defendant's contention that Plaintiffs fail to state a claim for violation of the Wiretap Act, as Plaintiffs plead that their networks were "open" and "unencrypted," is misplaced. While Plaintiffs plead that their… electronic communications systems, were configured such that the general public may join the network and readily transmit electronic communications across that network to the Internet, Plaintiffs plead that the networks were themselves configured to render… electronic communications, unreadable and inaccessible without the use of… technology allegedly outside the purview of the general public. Thus, the Court finds that Plaintiffs plead facts sufficient to support a claim that the Wi–Fi networks were not readily accessible to the general public.

Id. at 1083.

Here, obtained data from a password protected website, accessed contrary to terms and conditions, using sophisticated and unique technology. Uber cites only one, inapposite case in its defense, *Snow v. DirecTV, Inc.*, 450 F.3d 1314 (11th Cir. 2006). In *Snow*, plaintiff alleged that defendants had "accessed his website and viewed its electronic bulletin board, in excess of their authority." *Id.* at 1316. All Snow stated to infer that his website was not readily accessible to the general public was that his website was a "non-commercial private support group." *Id.* at 1321. The court noted that "registrants need only to create a password and acknowledge that they were not associated with… [a] prohibited entity" to gain access to the bulletin board. *Id.* at 1322.

Like the plaintiffs in *In re Google*, Plaintiff here alleges that Uber utilized sophisticated software technology to circumvent and surreptitiously access Lyft's ride-sharing system. Specifically, Plaintiff alleges that Uber created fake accounts with Lyft, in violation of a contract that all users agreed prior to creating accounts with Lyft. Compl. ¶49. Moreover, Plaintiff alleges that this top-secret software/spyware was unique to Uber, and was designed to be invisible and undetectable to Lyft, Class

Members, and other end-users of Lyft's systems, such that the general public was not receiving the same communications that Uber intercepting. *Id.* at ¶¶ 48-49, 55. At this stage in the litigation, that is sufficient to survive a motion to dismiss. *Snow* confirms: "[a] short simple statement that the plaintiff screens the registrants before granting access" may be sufficient "to infer that the website was not configured to be readily accessible to the general public." *Id.* at 1322. The pleading standard does "not require a plaintiff to 'plead in grave detail' all of a website's restrictive technical configurations." *Id.* "[F]urther factual development may show that the… system was configured in a way that allows access by the public, but at this stage the Court must accept Plaintiffs' allegations as true and construe all reasonable inferences in their favor." *Lane v. Brocq*, No. 15 C 6177, 2016 WL 1271051, at *8 (N.D. Ill. Mar. 28, 2016) (denying motion to dismiss Wiretap Act claim where plaintiffs alleged that Defendant had to login to a password protected site, which required individuals to register and obtain a user identification and password to access the system) (citing *Konop*, 302 F.3d at 875).

C. Plaintiff alleges that Defendants intercepted the contents of communications.

Defendants next assert that information intercepted does not qualify as "contents" based on judicial interpretation of the Wiretap Act. Mot. at 8-9. Defendants specifically argue that "[e]ven if Plaintiff had alleged Uber was 'intercepting' communications not 'readily available to the general public' his claim would still fail because he alleges only that Uber intercepted data, not 'contents.'" *Id.* Contents of communications are defined as "information concerning the substance, purport, or meaning of [the] communication." 18 U.S.C. § 2510 (8). As such "contents of communication" for purpose of a Wiretap Act claim are "limited to information the user intended to communicate." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012). Accordingly, automatically generated data, rather than data generated through the intent of the user, "does not constitute 'content' susceptible to interception" under the Wiretap Act. *Id. See also*, *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1126–27 (W.D. Wash. 2012) (dismissing Wiretap Act claim where plaintiff alleged defendant intercepted geolocation data from her cellphone without consent).

Unlike the plaintiffs in *Cousineau* and *In re iPhone Litig.*, Plaintiffs in this case allege more than "interception only of automatically generated geolocation data." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012). Here, Plaintiff has alleged that their location was only

broadcast while they were available for work and not that their smartphone broadcast their location to Uber automatically or all the time. Plaintiff and the Class had to open the Lyft app and affirmatively indicate that they were available to work. This availability for hire is human-generated content that required class members to input information into their smartphone. It is no different than sending a text or iMessage to one's employer asking if there is any piece-rate work available for them to do. That the content can be sent by pressing a button or toggling a switch is no different than replying to a phone call using the pre-written message options on a smartphone such as "I'm on my way." This is not machine-generated data; it is a human-generated content protected under the Wiretap Act.

Plaintiff alleges the program was used 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 - all in an attempt to sabotage Lyft and its employees by luring divers away from Lyft and depressing the availability of drivers and the overall success of the company. Compl. ¶¶48-49. In accessing this information, Uber also obtained the unique driver ID, and intercepted their "those drivers' habits, such as what time of day or what days of the week they would run the Lyft app." Compl. ¶49. Indeed, Uber's interception gave them "specific identities and contact information for the majority of Lyft's weekly or monthly service drivers in a particular place." *Id.* This information is not unintentionally or automatically generated data but constitutes substantive content that Lyft's systems were designed to collect and convey.[12]

D. The Wiretap Act does not exclude interception of communications from a smartphone.

Defendants' final attempt to dispose of Plaintiff's Wiretap Act claim rests on the erroneous proposition that the Wiretap Act excludes interception of communications made by smartphones, as smartphones are GPS tracking devices. Mot. at 10. Logically, this argument must be wrong because the

[12] Defendants insinuate that there must also be a privacy interest in the communications (although, as detailed below, there is) which is equally unavailing. "The statute itself does not require that a plaintiff establish a privacy interest in the communication at issue, and instead provides a civil cause of action whenever an individual intentionally intercepts… [an] electronic communication meeting the statutory definitions." *Lane v. Brocq*, No. 15 C 6177, 2016 WL 1271051, at *7 (N.D. Ill. Mar. 28, 2016). Such an accusation provides no basis to dismiss Plaintiffs' claims. *Id.*

Wiretap Act was created to prevent, *inter alia*, unauthorized surveillance of phone conversations and courts routinely uphold claims under the Wiretap Act for interception of communications originating from smartphones. *See, e.g.*, *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1042–43 (N.D. Cal. 2014) (finding plaintiff stated a claim under the Wiretap Act for interception of iMessages on iPhones). But the argument is also legally wrong and misinterprets the central premise of Plaintiff's Wiretap Act claim. Plaintiff is not "essentially alleging that Uber used Lyft drivers' smartphones as tracking devices." Mot. at 10. As detailed above, Plaintiff instead alleges that "Uber deployed the Hell spyware and/or software on computer systems… to remotely and surreptitiously access, monitor, intercept, and/or transmit personal information as well as electronic communications and whereabouts." Compl. ¶¶51-52. These allegations provide no basis to reduce the accepted definition of "smartphone" to nothing more than a "tracking device" such that Uber's interception of communications from the device would be excluded from the purview of the Wiretap Act.

II. Plaintiff Asserts Valid Claims for Violations of CIPA.

Defendants' arguments against the California Invasion of Privacy Act ("CIPA") claims similarly hinge on the misunderstanding of Plaintiff's Complaint. Plaintiff does not assert invasion of privacy based on Uber's acquisition of geolocation data "broadcast" by Lyft, but instead alleges, *inter alia*, "Uber deployed the Hell spyware and/or software on computer systems… to remotely and surreptitiously access, monitor, intercept, and/or transmit personal information as well as electronic communications and whereabouts." Compl. ¶¶51-52. For the reasons detailed below, Plaintiff has stated a claim for relief under CIPA and Defendants' motion should be denied.

A. Plaintiff alleges that Defendants eavesdropped on confidential communications.

Section 632 of CIPA "was enacted to address concerns that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties." *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1388 (2011). "The crux of section 632 is the right to prevent a simultaneous dissemination to an unannounced listener." *Id.* at 1389. That is exactly what happened here. Section 632 prohibits any unconsented-to monitoring of confidential communications,

defined to include "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto." *Id.* at 1388–89. The test for "confidential communications" "require[s] nothing more than the existence of a reasonable expectation by one of the parties that no one is 'listening in' or overhearing the conversation." *Flanagan v. Flanagan*, 27 Cal. 4th 766, 772–776 (2002) (adopting 'Frio Test,' *Frio v. Super Ct.*, 203 Cal. App. 3d 1480 (Cal. Ct. App. 1988)). Under this standard, the fact that the plaintiff knew, or should have known, that the information will be shared with other parties does not change the confidential character of the communication for purposes of section 632. *Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1397 (2011) (citing *Flanagan*); *see also Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004) ("The busybody that gets permission to come inside by posing as a meter reader is a trespasser…permission… provides no refuge for a defendant that procures consent by exploiting a known mistake that related to the essential nature of his access.").

"To prevail against a Rule 12(b)(6) motion… [a plaintiff] would have to allege facts that would lead to a plausible inference that his was a confidential communication – that is, a communication that he had an objectively reasonable expectation was not being recorded.." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1020 (9th Cir. 2013) (granting motion to dismiss where plaintiff asserted "too little" concerning the particular circumstances of a recorded phone call). Defendants do not assert a deficiency in the Complaint concerning the particular circumstances of the alleged interception, but rather continue to argue that they never intercepted confidential communications – these are fact issues that directly contradict Plaintiff's Complaint and should not be heard at this stage of the litigation. *See*, *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 2027-28.

Broken down, Defendants first argue that "Plaintiff does not contend Uber secretly listened to or recorded any of his communications," but that is not the appropriate standard for Section 632 claims, and is contrary to the allegations contained in Plaintiff's Complaint. As detailed *supra*, Plaintiff has alleged that Uber collected real-time information on Plaintiff and the class members' employment history, dates and times they were available for work, precise location information, personally identifying information (unique Lyft ID numbers, names and identities), locations of homes, offices, and other frequented locales, *inter alia*. As just noted by the Supreme Court of California last week,

"absent employees have a bona fide interest in the confidentiality of their contact information. While less sensitive than one's medical history or financial data, 'home contact information is generally considered private.'" *MICHAEL WILLIAMS, Petitioner, v. THE SUPERIOR COURT OF LOS ANGELES COUNTY Respondent; MARSHALLS OF CA, LLC, Real Party in Interest.*, No. S227228, 2017 WL 2980258, at *12 (Cal. July 13, 2017) (collecting cases).

Defendants also argue that the SGD intercepted is not a confidential communication under CIPA because "Plaintiff knew that Lyft was continually broadcasting his location to a countless number of potential Lyft riders precisely so that his location could be tracked while he was working." Mot. at 12. However, as detailed below, Defendants' reliance on Plaintiff's acceptance to Lyft Terms of Service is unavailing. Defendants' selective quotation to Lyft Terms of Service is (1) inappropriate for a motion to dismiss, which is limited solely to the content of the pleadings absent special circumstances not present here, (2) does not evidence consent to *Uber* intercepting SGD intended for Lyft and/or Lyft rides and (3) reveals to the Court that Uber actions was a direct violation of the Lyft terms of use. Simply because Plaintiff and members of the class were aware that the information was in transmission to various people, or that it would eventually be shared with other parties, does not vitiate the confidential character of the communications. *See Kight v. CashCall, Inc.*, 200 Cal. App. 4th 1377, 1397 (2011).

Moreover, the medium of transmission furthers a finding of confidentiality. Contrary to *People v. Nakai*, 183 Cal. App. 4th 499 (2010) and other cases involving emails and chats, the communications at issue here could not be easily shared, printed, or forwarded; they are not "by their very nature recorded on the computer of at least the recipient, who may then easily transmit the communication to anyone else who has access to the internet or print the communications." *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *23 (N.D. Cal. Sept. 26, 2013). Even if someone took a screenshot of the Lyft app before taking a ride, it would merely show vehicle icons on a map without any of the Lyft IDs or other information such as the make and model of the vehicles.

B. Plaintiff did not consent to Defendants' invasion of privacy.

Defendants' argument that Plaintiff consented to having his privacy invaded by Uber fails on three separate and independent grounds. First, the Terms of Service do not show that Plaintiff

consented to the Uber's surreptitious conduct. "[C]onsent is only effective if the person alleging harm consented 'to the particular conduct, or to substantially the same conduct.'" *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016), *see also Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). As Uber quotes, Plaintiff allegedly only agreed that "[w]hen you open Lyft on your mobile device, we (Lyft) receive your location." Mot. at 12. Second, Plaintiff did not consent to Uber's surreptitious tracking and he certainly did not agree to Uber receiving his communications to Lyft for the purposes of industrial espionage. *See*, Compl. ¶¶55, 67.

Finally, whether terms of service can constitute consent is often considered a fact issue not appropriate for resolution at the motion to dismiss stage. *See, e.g., Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1073–74 (N.D. Cal. 2016) (finding a fact issue sufficient to preclude summary judgment on the scope and efficacy of consent to website's terms and conditions); *In re Google Inc.*, 2013 WL 5423918, at *12–15 (denying motion to dismiss Wiretap Act claim where plaintiffs adequately alleged they did not explicitly or implicitly consent to Google's interception of email in transit) (dismissing CIPA claim on other grounds).

III. Plaintiff Asserts a Valid Claim for Constitutional Invasion of Privacy.

Article I, section 1 of the California Constitution is an enumeration of the inalienable rights of all Californians, including the right to privacy. *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 16 (1994). To state a claim for invasion of privacy under California's Constitution, Plaintiffs must demonstrate (1) a legally protected privacy interest, (2) a reasonable expectation to privacy under the circumstances, and (3) a serious invasion of the privacy interest. *Id.* at 39–40.

First, Plaintiff has alleged invasion of a legally protected privacy interest. Again, Defendants' contention that Plaintiff failed in this regard is based on a misinterpretation of Plaintiff's claims. Plaintiff does not allege disclosure of "mere contact information" or "general location." Mot. at 14. Plaintiff alleges the interception and acquisition of, *inter alia*, (1) precise geolocation data of class members' cell phones in 2014, 2015, and 2016; (2) class members' unique Lyft ID number; (3) that class members' are employed by Lyft; (4) the dates and times that class members' indicated that they were available to work; (5) the locations of class members' homes, offices, and other locations; (6) the full names and identity of class members using geolocation data such as start and stop locations; and

(7) the full names and identity of class members using Uber's own location data associated with driver and passenger records. *See* pp. 4-5, *supra*. *Williams* demonstrates that there is a "bona fide" expectation to privacy in this type of information, "[t]o be sure." *MICHAEL WILLIAMS, Petitioner,*, 2017 WL 2980258, at *12. *Pioneer Elecs., Inc. v. Super. Ct.* is inapposite as it concerned disclosure of contact information of potential class members, whereby the Court determined, after carefully balancing the protective measures the lower court put in place to minimize the privacy intrusion, would not be withheld in discovery. *Pioneer Elecs., Inc. v. Super. Ct.*, 40 Cal. 4th 360, 371-72 (Cal. 2007). The circumstances alleged by Plaintiff are distinguishable as Plaintiff was not a potential class member or witness to pending litigation with a protective order in place limiting the use of his information to litigation. Plaintiff agrees that information such as Uber and Lyft's driver lists are discoverable but may be designated as confidential and protected from public disclosure. Second, Defendants' contention that Plaintiff had no expectation to privacy under the circumstances as a matter of law is simply wrong. *See* Mot. at 14. "[P]rivacy… is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law." *Sanders v. Am. Broad. Companies, Inc.*, 20 Cal. 4th 907, 915–16 (1999). In no case has California "stated that an expectation of privacy, in order to be reasonable for purposes of the intrusion tort,[13] must be of absolute or complete privacy." *Id.* at 914–15. Here, Plaintiff has a reasonable expectation of privacy because their consent was limited to the legitimate use of the Lyft application by Lyft and its legitimate customers, not for espionage to their economic disadvantage. The Ninth Circuit explained this principle in *Theofel*, reasoning that "[a] defendant is not liable for trespass if the plaintiff authorized his entry. But an overt manifestation of assent or willingness would not be effective . . . if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended." *Theofel*, 359 F.3d at 1073 (internal citation and quotation omitted).

[13] "The right to privacy in the California Constitution sets standards similar to the common law tort of intrusion." *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 287 (2009). "Borrowing certain shorthand language from *Hill*… which distilled the largely parallel elements of these two causes of action, [courts] consider (1) the nature of any intrusion upon reasonable expectations of privacy, and (2) the offensiveness or seriousness of the intrusion, including any justification and other relevant interests." *Id.* (quoting *Hill*, 7 Cal. 4th 1).

Contrary to Defendants' assertions, Plaintiff does not allege disclosure of "mere contact information," "[a] person's general location," or "de-identified" information such that the contents cannot be linked to individuals. Mot. at 14-15. Plaintiff instead alleges the interception of information from which Uber derived intimate details of each driver's personal life including, but not limited to, "home" and "work" locations, identity, employment hours, work schedule, and employment history, *inter alia*. It is not axiomatic that courts find no reasonable expectation of privacy in location information; indeed, courts will routinely find the opposite. *See*, *In re Application for Tel. Info.*, 2015 WL 4594558, at * 7-12 (finding an "eminently" reasonable expectation of privacy in historic cell site location information); *United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *6–8 (N.D. Cal. Mar. 2, 2015) ("Society's expectation of privacy in historical cell site data is also evidenced by many state statutes and cases which suggest that this information exists within the ambit of an individual's personal and private realm… the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy.") (collecting cases) (internal quotation and citations omitted). That this information constitutes a trade secret of Lyft, the unauthorized use and disclosure of which expressly violates its terms and service, further demonstrates the reasonable expectation to privacy that each driver personally has in it. *See* pp. 2-7, *supra*.

Third, Plaintiff has alleged a serious invasion of his privacy interest. The egregiousness of Defendants' invasion is not only in the content of the intrusion, but in the social norms and business interests which Uber violated by their intrusion. Unlike the conduct at issue in *In re iPhone Application Litigation* where the court found the violation was not "an egregious breach of social norms, but routine commercial behavior," the violation here was well outside the scope of routine commercial behavior.*In re iPhone Application Litigation*, 844 F. Supp. 2d at 1063 (quoting *Folgelstron v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (Cal. Ct. App. 2011)). The factual allegations in Plaintiff's Complaint confirm that this was covert industrial espionage: "Not even Uber's then-powerful 'general managers' who ran the business in individual cities were supposed to know about it." Compl. ¶49. That its conduct exceeded the bounds of routine commercial behavior is corroborated by Lyft: "We are in a competitive industry. However, if true, these allegations are very concerning." *Id.* In short, Plaintiff has stated a claim for Constitutional Invasion of Privacy.

IV. Defendants' Challenges to Plaintiff's Unfair Competition Law Claim Fail.

California's Unfair Competition Law (the "UCL") generally prohibits "any unlawful, unfair or fraudulent business practices." Cal. Bus. & Prof. Code § 17200. It was originally enacted to protect commercial enterprises from business loss resulting from unfair means of drawing away customers from a competitor. *See, e.g., Law Offices of Mathew Higbee v. Expungement Assistance Servs.*, 214 Cal. App. 4th 544, 551 (2013). As a result, "virtually any law–federal, state or local–can serve as a predicate for a section 17000 action." *Id.* at 55 (citations omitted). Like the defendants in *Commc'ns v. L.A. Cellular Tel. Co.*, Uber's practices violate the UCL's unfair prong because they represent "conduct that threatens an incipient violation of an antitrust law or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significant threatens or harms competition." *Cel-Tech Commc'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 186 (1999). The "unfair" standard is intentionally broad, allowing courts maximum discretion to prohibit new schemes such as Uber's Hell spyware which is unfair and caused economic injury and loss to Lyft and its drivers including Plaintiff. *Motors, Inc. v. Times Mirror Co.*, 102 Cal. App. 3d 735, 741 (Cal. Ct. App. 1980). Accordingly, Defendants' conduct in conducting unauthorized and illegal surveillance and intercepting communications, all with the sole purpose of obtaining a competitive advantage over Lyft, constitutes business practices that are easily captured by the UCL's unfair and unlawful prongs.

A. Plaintiff has standing to pursue his UCL claim as he alleges both an injury-in-fact and monetary loss.

Standing to pursue a claim under § 1700 exists where a party alleges that he or she has suffered injury in fact and has lost money or property as a result of the unfair competition. Cal. Bus. & Prof. Code § 17204. Although the following list is not exhaustive, there are innumerable ways in which economic injury from unfair competition may be shown: "A plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary." *Law Offices of Mathew Higbee v. Expungement Assistance Servs.*, 214 Cal. App. 4th 544, 561 (2013) (quoting *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323 (2011)).

"[A]n identifiable trifle is enough for standing" under the UCL. *Id.* Allegations of reduced market share are routinely sufficient to confer UCL standing. *Id.* at 558–559 (collecting cases).

Defendants erroneously contend that Plaintiff has neither (1) suffered an injury in fact, as Lyft drivers could not possibly be harmed by rides being directed towards "dual appers" over Uber only "appers" or diversion of Lyft customers in general; nor (2) suffered monetary or proprietary losses, as Plaintiff only alleges the loss of personal information insufficient to confer standing under the UCL. Mot. at 16-17. First, Plaintiff has alleged an injury in fact. The California Constitution, CIPA, and the Wiretap Act have all created substantive, enforceable, legal rights: "the judgment of… the California Legislature indicate[s] that the alleged violations of Plaintiff's statutory rights under… CIPA constitute concrete injury in fact. This conclusion is supported by the historical practice of courts recognizing that the unauthorized interception of communication constitutes cognizable injury... [r]ather than being a 'bare procedural violation.'" *Romero v. Securus Techs., Inc.*, 216 F. Supp. 3d 1078, 1088–89 (S.D. Cal. 2016) (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *as revised* (May 24, 2016)); *see also Osgood v. Main Streat Mktg., LLC*, No. 16CV2415-GPC(BGS), 2017 WL 131829, at *8 (S.D. Cal. Jan. 13, 2017) (an invasion of privacy injury is sufficient to confer Article III standing). Moreover, Plaintiff alleges that Uber's unlawful and unfair business practices have directly harmed him as they were designed to decrease the availability of Lyft drivers in the area to steer customers away from Lyft altogether. Compl. ¶¶58-59. The invasion of privacy implicated by Uber's violations of the ECPA, CIPA, and the California Constitution, coupled with the intentional interference with Plaintiff's and Lyft's customers creates a judicially cognizable injury in fact.

For similar reasons, Plaintiff has also alleged an economic injury sufficient to state a claim under the UCL. Again, Defendants misconstrue Plaintiff's claim on this point in asserting that "Plaintiff alleges only that Uber may have collected location information," and nothing more. Mot. at 17. Instead, Plaintiff has alleged Uber's unlawful interception of SGD was used to steer Lyft customers to Uber, harming the market for Lyft and its drivers and diminishing Plaintiff's earnings. *See* pp. 5-6, *supra*. Allegations of lost revenue unquestionably satisfy the economic injury required for standing under the UCL. *See, e.g.*, *Luxul Tech. Inc. v. Nectarlux, LLC*, 78 F. Supp. 3d 1156, 1174 (N.D. Cal. 2015) ("Here,

Plaintiff has alleged an economic injury in the form of lost customers and sales revenue. That is sufficient to satisfy standing under the UCL.") (citing *Kwikset Corp.*, 51 Cal. 4th at 336–337).

B. Plaintiff has alleged facts sufficient to show the remedies available at law are inadequate to remedy his injury.

To survive a motion to dismiss, a plaintiff must go beyond demonstrating that equitable remedies merely exist, and "explain how damages are inadequate to compensate for Plaintiff's alleged harm." *Huu Nguyen v. Nissan N. Am., Inc.*, No. 16-CV-05591-LHK, 2017 WL 1330602, at *5 (N.D. Cal. Apr. 11, 2017). The mere existence of potential remedies at common law or provided by statute does not indicate that remedies available at law are inadequate. Specifically, Plaintiff seeks both an injunction and restitution. The injunction claim is two-fold: Plaintiff asks the Court to grant injunctive relief that would require Uber to discontinue its unlawful and unfair business practices, and also would require Uber to purge all ill-gotten personal and private information from their records. Compl. ¶85. These remedies are essential to fully compensate Plaintiff for his claims as available damages do not prevent Defendants' use and retention of Plaintiff's personal information, nor will they curb the anti-competitive business practices described herein.

Ultimately Uber obtained sensitive and private information about Lyft drivers, cultivated and protected through Lyft's proprietary technology, through high-tech devices to which no driver contemplated or consented exposure to. The entire goal of the Hell program was to obtain a competitive advantage over Lyft and steer customers to Uber. Plaintiff and other similarly situated Lyft drivers have been directly injured as a result of this conduct. This industrial espionage epitomizes the deceptive and unfair business practices the UCL was intended to prevent. For the foregoing reasons, Uber's motion with respect to the Plaintiff's UCL claims must be denied.

CONCLUSION

Uber's Hell program is a clear reflection of Uber's overly aggressive business practices; continuously bending and breaking laws and commercial norms to maximize profits and hamstring competitors. Its Motion to Dismiss rests entirely upon a mischaracterization of Plaintiff's claims, turning the real-time interception, acquisition, and collection of sensitive information into simply obtaining "general location information" to which Plaintiff and similarly situated individuals have already consented. This is a fatal flaw in Defendants' Motion; because the information Defendants

intercepted and acquired involved much more intimate details concerning Plaintiff and directly decreased the revenue of Lyft and its drivers, Plaintiff has stated claims for all causes of action alleged in the Complaint. Defendants' Motion must be denied.

Respectfully submitted,

ZIMMERMAN REED LLP

Dated: July 17, 2017

/s/ Caleb Marker
Caleb Marker
E-Mail: Caleb.Marker@zimmreed.com
2381 Rosecrans Ave., #328
Manhattan Beach, CA 90245
(562) 216-7380 Telephone

Mark Burton
E-Mail: mburton@audetlaw.com
Michael McShane
E-Mail: mmcshane@audetlaw.com
AUDET & PARTNERS, LLP
221 Main Street, Suite 1460
San Francisco, CA 94105
(415) 341-0400 Telephone

Counsel for Plaintiff and the Class