Patrick L. Oot, Jr. (admitted *pro hac vice*)
SHOOK, HARDY & BACON L.L.P.
1155 F Street NW, Suite 200
Washington, D.C. 20004
Tel: 202.783.8400 | Fax: 202.783.4211
oot@shb.com

M. Kevin Underhill, SBN 208211
Annie Y.S. Chuang, SBN 196307
SHOOK, HARDY & BACON L.L.P.
One Montgomery, Suite 2700
San Francisco, California 94104
Tel: 415.544.1900 | Fax: 415.391.0281
kunderhill@shb.com | achuang@shb.com

Attorneys for Defendants

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

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

Defendants.

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

DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS PLAINTIFF'S FIRST AMENDED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES

[Fed. R. Civ. P. 12(b)(1) and 12(b)(6)]

Date: January 11, 2017
Time: 9:00 a.m.
Judge: Hon. Jacqueline Scott Corley
Courtroom: F-15th Floor

NOTICE OF MOTION

PLEASE TAKE NOTICE that on January 11, 2018, at 9:00 a.m., before the Honorable Jacqueline Scott Corley, in Courtroom F of the U.S. District Court for the Northern District of California, San Francisco Division, at 450 Golden Gate Avenue, San Francisco, California, defendants Uber Technologies, Inc.; Uber USA, LLC; and Rasier-CA (collectively referred to here as "Uber") will and hereby do move the Court for an order dismissing the First Amended Complaint. This motion is pursuant to Rule 12(b)(6) and based on the following grounds:

- Plaintiff's Wiretap Act claim fails because he does not allege Uber "intercepted" his communications, and because the information was "readily accessible to the general public," was not "content," and was collected by smartphones used as "tracking devices";
- Plaintiff's California Invasion of Privacy Act claim fails for similar reasons, including the failure to allege that Uber "eavesdropped on confidential communications";
- The new Stored Communications Act claim fails because Plaintiff does not allege Uber "trespassed" in order to obtain communications from temporary storage "incidental to transmission";
- The new California Computer Data Access and Fraud Act claim fails because Plaintiff does not allege Uber "accessed" a computer "without permission" or that he suffered any damage or loss as a result;
- The constitutional privacy claim fails for similar reasons and because the state constitution protects only against much more serious intrusions than alleged here; and
- Plaintiff's Unfair Competition Law claim fails because he has not alleged any loss of money or property or any basis for equitable relief in general.

The motion is based on this notice, the supporting memorandum, the pleadings, and such argument as the Court may allow.

Dated: October 27, 2017

Respectfully submitted,
SHOOK HARDY & BACON L.L.P.

By: */s/ M. Kevin Underhill*
PATRICK L. OOT
M. KEVIN UNDERHILL
ANNIE Y.S. CHUANG

Attorneys for Defendants

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Other Authorities

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Plaintiff still cannot explain what private "communications" Uber allegedly "intercepted" or just how it did so. In granting leave to amend, the Court made clear it expected to see a complaint containing facts, not just a "quote from somebody's article" followed by legal conclusions. But of the 15 pages of "substantive allegations" in the First Amended Complaint, five are the same quote from somebody's article, now followed by three pages taken largely from Wikipedia articles and a fourth from Lyft's terms of service. Well over half the FAC's "substance," in other words, is still just material Plaintiff found on the Internet. And of the remaining 55 paragraphs in that section, 30 are alleged "on information and belief." It seems doubtful this is what the Court had in mind.

Rather than including new and potentially material facts, Plaintiff has used the FAC as a sort of supplemental brief in which he tries again to explain his theory of the case. But this is the same theory, just adorned with buzzwords like HTTP, TCP, "scraping," and "sniffing." There are no new facts here that matter. Plaintiff still alleges only that Uber acted as a Lyft rider in order to receive driver ID and GPS information from Lyft, data that Uber supposedly then used for its own commercial purposes. That does not allege an "interception" of the "contents" of anyone's "communications," or that Uber was "eavesdropping" on anyone. In one way or another, this failing defeats all of Plaintiff's privacy-related claims, including the two new ones, although some of the claims also fail for other reasons.

Finally, Plaintiff's Unfair Competition Law claim fails not just because all the underlying statutory claims do, but because Plaintiff again fails to allege that he lost any money or property as a result of Uber's alleged actions. Even if he had alleged facts showing Uber violated his privacy, he does not allege he lost money, and offers nothing but speculation as to the effects the scheme might have had "over time." For that reason, too, the Court should dismiss the FAC.

FACTS ALLEGED

Plaintiff again relies primarily on the text of the article published by *The Information*. FAC ¶ 50, at pp. 8–13. He then alleges that "upon information and belief," what *The Information* reported is "true and accurate." FAC ¶ 51. Plaintiff now bolsters this with about three pages' worth of

quotations from two Wikipedia articles discussing the Hypertext Transfer Protocol (HTTP) and the Transmission Control Protocol (TCP). FAC ¶¶ 56, 57, 59–62, 71. He has also added numerous paragraphs alleged only "upon information and belief," a phrase that now appears in the complaint more than three dozen times.[1] FAC ¶¶ 8, 9, 28, 29, 51, 53, 54 (twice), 56, 65, 66, 67, 73–76, 79, 80, 82, 83 (three times), 85–94, 97–101. He does not use the phrase consistently, however—and in at least three paragraphs, Plaintiff alleges "on information and belief" that *he* did something. FAC ¶¶ 85 ("Upon information and belief, Plaintiff used the Lyft app … to send an HTTP request…."), 92 (similar allegation regarding transmission of personal information), 93 (similar allegation regarding lack of consent). He can hardly need discovery to allege his own actions.

The Wikipedia quotes and related allegations discuss basic information about how the Internet works. Plaintiff's goal is evidently to draw an analogy between the information he sent while using the Lyft app and information contained within a physical letter mailed from one place to another. FAC ¶ 55, 69, 70, 72, 77. In the analogy, an "HTTP request" or "TCP packet" is "the digital equivalent of the physical envelope," the IP addresses are like the mailing and return addresses written on the envelope, and the driver's "personal information" is like the words on the letter inside the envelope. *Id.* ¶¶ 69, 72. The implication is that Uber was reading someone else's mail.

In Plaintiff's analogy, drivers send "letters" to Lyft "containing" their driver ID numbers, GPS locations, and the implied message that each is willing to give someone a ride. *Id.* Meanwhile, potential riders are sending similar "letters" to Lyft, containing their Lyft customer ID numbers, GPS locations, and (presumably) the implied message that each wants a ride. *Id.* ¶¶ 63–66. Lyft opens and reads all these, connects riders and drivers, and then sends each rider a "response letter" containing a list of nearby drivers to choose from and the corresponding information for each. *Id.* ¶ 67. Plaintiff's description stops there, but it is reasonable to infer that the rider makes a choice, sends another "letter" to Lyft saying so, and Lyft then sends a "letter" to the chosen driver.

Plaintiff alleges that Uber acted as a Lyft rider so that it too could receive these letters. That is, he alleges Uber "created a network of fake Lyft riders" to send "forged HTTP requests to Lyft,"

[1] In accordance with this Court's standing order, Uber has provided a redline showing the differences between the original complaint and the FAC. *See* Ex. 1 to Decl. of M. Kevin Underhill.

and Lyft would send back what were "essentially ... response letter[s]" containing the same information described above. FAC ¶¶ 74, 76, 77, 80. Uber would then collect the information, according to Plaintiff, hoping to identify drivers who used both companies' apps. *Id.* ¶ 101. It would then, using its own system, direct "more frequent and more profitable" trips to drivers on that list. *Id.*

There are at least two problems with Plaintiff's description of the process, one factual and one legal. The *factual* problem is the description of HTTP and/or TCP as "digital envelopes." (The FAC is not always clear as to which Plaintiff believes is the "envelope" and which is the "letter.") These are not containers or enclosures, they are *protocols*: standardized sets of rules that govern communications. HTTP is the "transfer protocol" that provides the general framework—for example, messages are sent in plain-text ASCII, lines end with particular characters, and so on. *See In re Zynga Privacy Litig.*, 750 F.3d 1098, 1101 (9th Cir. 2014) (HTTP is "the language of data transfer on the internet"). TCP is the "communication protocol," basically the set of rules for sending information in chunks or "packets" so the pieces can be routed through various network nodes and reassembled at a destination. *IDN Technologies, LLC v. Verisign, Inc.*, No. C 03–3029, 2004 WL 2196545, at *1 & n.2 (N.D. Cal. Sept. 24, 2004). An equivalent "postal protocol" might be the set of rules governing the size or weight of an envelope or how the Post Office will move it from point A to point B—not the physical envelope itself. It is therefore not entirely clear what HTTP or TCP have to do with Plaintiff's theory of the case.

As discussed below, the *legal* problem with Plaintiff's approach, from his perspective and given the claims he asserts here, is that it does not describe a scheme in which Uber was reading anyone else's "mail" (and certainly not Plaintiff's)—only its own, after receiving its "letters" back from Lyft. Presumably for that reason, Plaintiff now alleges that another, initial step was involved. He alleges, "upon information and belief," that Uber used "sophisticated software" called "network analyzers" or "sniffers" to "detect, copy, and decode the TCP packets sent from Lyft's Central Communication Servers to the Lyft App." *Id.* ¶¶ 53, 54, 73. Having thus "reverse-engineered the communication process," it could then "masquerade as Lyft riders seeking rides," as the allegations above contend. FAC ¶ 74. Plaintiff does not allege any facts explaining how this might have worked, however, and most significantly, he does not allege who was using the Lyft app when Uber

supposedly did this. He alleges only that Uber copied and decoded packets sent to "the Lyft App." *Id.* ¶ 73. Nor does he explain why Uber would have needed to use a packet sniffer given his allegation that it could create fake rider accounts and receive information that way.

Finally, Plaintiff has tweaked the allegations about possible harm caused by Uber's actions in two ways. First, Plaintiff previously alleged only that Uber provided incentives to "dual-app" users once it identified them, supposedly part of a long-term scheme to harm Lyft. Now he also alleges that Uber planned to "inundate drivers who used both platforms with work," and that by "inundating these drivers from [*sic*] Uber rides, Uber was able to discourage drivers from accepting work on the Lyft platform, reducing the effective supply of Lyft drivers available." FAC ¶¶ 9, 101. But as before, Plaintiff never alleges *he* was "inundated with work," was discouraged from accepting Lyft work, or actually lost any money as a result of the alleged scheme. Second, Plaintiff now alleges twice—both times "upon information and belief"—that "Uber was able to use the data collected to determine the identities of the drivers' rider customers." *Id.* ¶ 83; *see id.* ¶ 89. He pleads no facts to support this, and does not even allege Uber *actually* did this, only that it might have been able to. Nor would it appear to have anything to do with Plaintiff's theory of the case—that Uber was interested in dual-app drivers, not riders, who like Lyft are not parties to this case.

ARGUMENT

Rule 12(b)(6) requires "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *see Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (Rule 8 "does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions."). The allegations "must be enough to raise a right to relief above the speculative level." *Twombly*, 550 U.S. at 555. Allegations that are "merely conclusory" or require "unreasonable inferences" need not be presumed true. *Iqbal*, 556 U.S. at 678.

I. Plaintiff again has failed to allege facts showing a violation of the Wiretap Act.

A. Plaintiff does not allege an interception.

The Wiretap Act prohibits only the intentional "interception" of wire, oral, or electronic communications. 18 U.S.C. § 2511. Though it creates a private right of action for any person whose communication is "intercepted, disclosed, or intentionally used in violation of this chapter" (18

U.S.C. § 2520(a)), only the disclosure or use of intercepted communications is a violation. 18 U.S.C. § 2511; *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 n.7 (9th Cir. 2002). In *Konop*, the Ninth Circuit held that "interception" requires more than mere "acquisition" of an electronic communication. 302 F.3d at 876–79. Noting that the ordinary meaning of "intercept" is "to stop, seize, or interrupt in progress or course before arrival," the court held that the Wiretap Act applies only if a communication is "acquired during transmission[.]" *Id.* at 878 (emphasis added; quoting Webster's Ninth New Collegiate Dictionary 630 (1985)); *see also Marsh v. Zaazoom Solutions, LLC*, No. C-11-05226, 2012 WL 952226, at *17 (N.D. Cal. Mar. 20, 2012) (dismissing claim because plaintiff did not allege defendant acquired information "by capturing the transmission of information that was otherwise in the process of being communicated to another party").

As discussed above, the FAC again relies almost entirely on *The Information*'s article, which alleges Uber collected data by creating Lyft rider accounts and viewing the information Lyft sent to those accounts. FAC ¶ 50, at pp. 10:25–11:14. Plaintiff's new allegations consist primarily of technical jargon rather than factual allegations, and still fail to allege an interception.

1. Plaintiff's own "post office" analogy shows his theory is unfounded.

As before, Plaintiff alleges that Uber somehow intercepted messages that drivers like himself sent to prospective riders—sealed messages that drivers sent "through" Lyft servers or the Lyft app. FAC ¶¶ 4, 10, 86, 91. This is the theory Plaintiff's counsel sought to explain at the hearing:

> The driver is communicating their location and their Driver I.D. out through the Lyft application.... Uber is accepting—is intercepting that communication of their I.D. and their location as—in real time as they're going around driving around. They have all these intercepted locations going on. So driver data is going out ... to potential passengers through the Lyft system. Okay? Just because it goes through Lyft's communication system doesn't change the fact that it's still a communication that they're making to other people.

Tr. (Dkt. 37) at 8:7-19. Plaintiff's new allegations present a "post office" analogy intended to support this, asserting that drivers send riders "a sealed letter traveling between different post offices en route to its final destination." FAC ¶ 70, *see id.* ¶ 77. But this (flawed) analogy actually helps show Plaintiff's theory is wrong. What he alleges is not a transmission from driver to rider, but a series of discrete transmissions between drivers and Lyft on the one hand, and potential riders and Lyft on the other.

Plaintiff alleges as follows:

- "[T]he Lyft Driver App uses the Hypertext Transfer Protocol ('HTTP') to communicate with Lyft's Computer Communication Servers." FAC ¶ 56. According to Plaintiff, this is like a letter that contains the driver ID, GPS data, and the (implied) message that the driver is ready to work. *Id.* ¶ 72(d).
- At the same time, potential riders are sending "letters" to Lyft. FAC ¶ 65 ("after a rider logs into the Lyft App the app sends an HTTP request to Lyft's Computer Communication Servers." FAC ¶ 65. This "letter" contains the rider's Lyft customer ID and GPS data (and the implied message of willingness to ride). *Id.* ¶ 66.
- Having received the drivers' and riders' letters, Lyft then sends the rider's app "a list of nearby drivers" who are willing to do the job. FAC ¶ 67.
- Though Plaintiff's description stops there, the Court can infer that each rider then sends a message back to Lyft, and Lyft then sends the driver a message with the rider's location.

Importantly, Plaintiff minimizes a critical point: unlike the Post Office, Lyft is "opening" and reading the "letters," analyzing data, and sending back "letters" of its own, not just "redirecting and forwarding" sealed letters sent "through" its facility. This is implicit in Plaintiff's admission that what Lyft sends back to riders is a "list of nearby drivers." FAC ¶ 67 (emphasis added). This is what ride-sharing services *do*: connect drivers and riders in a way that would be far more difficult, if not impossible, for those people to achieve on their own. A Lyft driver cannot match herself directly with a Lyft rider, and vice versa. Instead, the eventual connection between driver and rider depends first on Lyft's separate communications with the respective parties, and what it does with the information. In short, Lyft (or its server) is an endpoint for communications, not a relay station.

Plaintiff's theory of the case is that "Uber created fake Lyft rider accounts and used commonly available software to fool Lyft's system into thinking those riders were in particular locations...." FAC ¶ 50 at 10:25–27; *see id.* ¶¶ 77, 80 (alleging that Uber sent messages to Lyft, and "Lyft's servers would fall for the deception and transmit back information for all nearby Lyft drivers"). Plaintiff is alleging that Uber deceived Lyft by posing as a rider (or multiple riders), not that Uber acquired a communication from Plaintiff or, for that matter, that it acquired any communication "during transmission" to anyone other than Uber. If Uber had been "opening mail," it would only have been opening its own. Plaintiff has therefore not alleged an "interception" for purposes of the Wiretap Act. *Konop*, 302 F.3d at 876–79; *Marsh*, 2012 WL 952226, at *17.

2. Plaintiff's new "sniffer" allegations do not change the analysis.

Possibly realizing that the above theory fails, in the FAC Plaintiff now alleges Uber used "network analyzers" or "[packet] sniffers" as well. *See* FAC ¶ 53–54, 73. His brief allegations again fail to allege any sort of "interception." These paragraphs state—again on "information and belief"—that Uber "used network analyzers to detect, copy, and decode the TCP packets sent from Lyft's Central Communication Servers to the Lyft App." *Id.* ¶ 73. In some way Plaintiff does not explain, this allegedly allowed Uber to "reverse-engineer[ ] the communication process," so that it was "then able to use the Hell spyware to masquerade as Lyft riders seeking rides." *Id.* ¶ 74. Many facts are missing from this (as is a clear understanding of how sniffers work), but the most important one is the identity of the person using "the Lyft App" at the time. That is, Plaintiff does not allege that Uber was intercepting TCP packets or any other sort of communications that were sent by him or to some third party. His theory of the case is that Uber acted as a Lyft rider or riders, but Uber could not have "intercepted" the packets it received from Lyft as a result.

Nor do the new allegations (or any others) support the claim that Uber somehow "gained access to Lyft's systems." The core of the FAC is that Uber obtained information by using forged accounts to send messages, not that Uber somehow hacked into Lyft's systems. But even if Uber had gained access to Lyft's system in this way, that still would not have been an "interception" for reasons Uber has explained. *See Cobra Pipeline Co. v. Gas Natural, Inc.*, 132 F. Supp. 3d 945, 948 (N.D. Ohio 2015). In *Cobra Pipeline*, the plaintiff argued the defendants violated the Wiretap Act when they improperly accessed a web portal that tracked, in real-time, the locations of plaintiff's utility vehicles. The website also provided other data like historical location information, vehicle ID numbers, and driver names. *Id.* at 948. The court held this did not show the defendants "intercepted" a communication before it reached an intended recipient. *Id.* at 952–53. Whether the defendants had authorization to access the web portal, or how they got it, was immaterial to the "threshold" question of whether doing so was an "interception" under the Act. "Interception requires a transmission of communications between two points, with some interruption during or contemporaneous with that transmission." *Id.* at 953. The defendants' use of the web portal at the endpoint of the transmission "did not interrupt an otherwise-occurring transmission." *Id.* The same is true here.

B. The communications at issue were "readily accessible to the general public."

Even if Plaintiff had alleged an "interception" in some sense, the claim would still fail. Congress's objective in passing the Wiretap Act was to ensure that federal law adequately guarded against the unwanted interception of electronic communications from "overzealous law enforcement agencies, industrial spies, [or] just plain snoops." *See* S. Rep. No. 99-541, at 1–3 (Conf. Rep.); 145 Cong. Rec. S.7992 (daily ed. June 19, 1986) (statement of Sen. Leahy). A plain and common-sense reading of the Wiretap Act and its legislative history shows that Congress meant to protect private communications. *See* 145 Cong. Rec. S.7992 (daily ed. June 23, 1986); *see also Konop*, 302 F.3d at 875 (holding legislative history shows "Congress wanted to protect electronic communications that are configured to be private, such as email[.]"). Accordingly, the Act expressly does not cover 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. § 2511(2)(g)(i).

Lyft's electronic communication system is most certainly configured to be "readily accessible to the general public." Lyft itself describes its service as a "marketplace" in which riders and drivers can be connected. *See* Lyft TOS (Ex. A to Request for Judicial Notice) at ¶ 1. That marketplace is enormous. Lyft is operating a business, and hopes to reach as many riders as possible—a goal Plaintiff likely shared while he was driving with Lyft. All it takes to create an account and access the Lyft app is an email address and phone number. Anyone can do this. Plaintiff alleges there were 315,000 Lyft drivers in 2016 alone (FAC ¶ 50, at p. 11:18), and a 2016 estimate suggested that the total number of monthly active Lyft riders at the time was about 3.6 million. If an electronic rideshare-request service used by millions of Americans is not "readily accessible to the general public," it is a mystery as to what system would be sufficiently public to qualify for the Wiretap Act exception.

The Eleventh Circuit reached a similar conclusion in a case involving an electronic bulletin board. *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1320 (11th Cir. 2006). The bulletin board required users to register, create a password, and affirm that they had no association with DirecTV. *Id.* at 1316. Despite the "private" nature of the bulletin board, and the claim that DirecTV had violated the board's terms of service by accessing the site, the court held the plaintiff had not stated a claim

because he had not alleged the board restricted access to the general public. *Id.* at 1322. Users had to sign up, it was true, but anyone could sign up. The allegations therefore described only "a self-screening methodology by which those who are not the website's intended users would voluntarily excuse themselves." *Id.* The court dismissed the ECPA claim because "the requirement that the electronic communication not be readily accessible by the general public is material and essential to recovery[.]" *Id.* at 1321. That requirement defeats Plaintiff's claim here as well.

Plaintiff's renewed allegation that Uber collected anonymized "Lyft ID" numbers does not change the result. FAC ¶ 50, at p. 11:8–14. Plaintiff claims his Lyft ID number was transmitted whenever a Lyft rider opened the Lyft app to look for nearby drivers. *Id.* Regardless of whether Plaintiff knew he was providing his Lyft ID number along with his location, it was nevertheless offered to the general public as an intrinsic component of Lyft's service. Again, therefore, Uber could not be held liable under the Wiretap Act for collecting information that Lyft was making "readily accessible to the general public." Plaintiff tries to avoid this by alleging that the information was not available generally, but only to "prospective passengers" or "authorized riders in Plaintiff's vicinity seeking transportation." FAC ¶¶ 10, 86. But anyone with the Lyft app can view drivers' locations, regardless of whether they actually want a ride or are in the vicinity. For example, a Lyft app user could physically be in San Francisco, but could select a pick-up location in New York City. In doing so, the user could view drivers in the vicinity of that pick-up point, even though she is thousands of miles away. This information is available to anyone who opens the Lyft app, and anyone who wants the Lyft app can get it. For these reasons, Plaintiff is describing a system "readily accessible by the general public."

C. Plaintiff does not allege Uber intercepted the "contents" of a communication.

The Wiretap Act prohibits only the interception of the "*contents* of any wire, electronic, or oral communication...." 18 U.S.C. § 2510(4) (emphasis added). "Contents" of a communication are defined as "any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8). The Ninth Circuit has held that "'the term 'contents' 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' such as a name,

address, or the identi[t]y" of a person making a communication. *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 935 (N.D. Cal. 2015) (quoting *In re Zynga Privacy Litig.*, 750 F.3d at 1106–07). Here, Plaintiff alleges only that Uber intercepted an anonymized ID number and location data, not "contents" of a confidential communication.

The information Uber allegedly collected using the Lyft app did not reveal the substance, purport, or meaning of any communication. As this Court and others have held, geolocation data and other pieces of background information (like an anonymized Lyft ID number) constitute record information, not "contents" for purposes of the Wiretap Act. *See In re Zynga*, 750 F.3d at 1106 (explaining that "record information" refers to non-content information that is generated in the course of a communication"). "'[C]ontent' is limited to information the user intended to communicate, such as the words spoken in a phone call." *In re iPhone Application*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (citing *United States v. Reed*, 575 F.3d 900 (9th Cir. 2009)).

In the *iPhone* case, the plaintiffs claimed Apple violated the Act by allowing third-party apps to collect personal information such as the plaintiffs' names, precise geographic locations, unique device identifiers, genders and ages. *Id.* at 1061–62. The court held that iPhone geolocation data was not comparable to a phone conversation, and thus not the "content" of a communication, even if it could convey the parties' identities. *Id.* at 1061. Indeed, the court observed that prior to the 1986 ECPA amendments, the definition of "content" covered "all aspects of the communication itself," including the identity of the parties and the fact that the communication occurred. *Id.* (quoting *Gelbard v. United States*, 408 U.S. 41, 51 n.10 (1972)). But the amended definition eliminated the phrase "information concerning the identity of the parties to such communication or the existence … of that communication." *See id.* (citing 18 U.S.C. § 2510(8) (1986)). Thus, "under the current version of the statute, personally identifiable information that is automatically generated by the communication, but that does not comprise the substance, purport, or meaning of that communication, is not covered by the Wiretap Act." *Id.* at 1062.

Here too, despite Plaintiff's claim that Uber was "reading a digital letter" that "contained" a driver's unique identifier, precise geolocation, willingness to provide services, and an estimated price for the ride, none of that information would qualify as "contents" for purposes of the Wiretap

Act. All of it was automatically generated when Plaintiff turned on his Lyft app—except for pricing, which is determined by Lyft, not drivers. FAC ¶ 72; Lyft TOS ¶ 4 (discussing pricing). Plaintiff therefore cannot successfully contend that Uber was accessing the protected "contents" of a communication he sent.[2]

Similarly, courts have held that cell-site location information "does not constitute the contents of a communication under § 2510(8)." *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116, 1127 (W.D. Wash. 2012). In *Cousineau*, the plaintiff alleged that Microsoft invaded her privacy and violated the Wiretap Act by collecting smartphone users' approximate latitude and longitude to facilitate targeted advertisements based on their location. *Id*. at 1120–21. Relying on prior decisions involving government surveillance requests, the court concluded that the definition of "contents" under section 2510(8) "does not include location information." *Id*. at 1127; *see also In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051 (N.D. Cal. 2015) (citing *Cousineau*). Like the plaintiff in *Cousineau*, Plaintiff alleges only that Uber obtained automatically generated geolocation and anonymized Lyft ID record information, not the "substance, purport, or meaning" of any communication. Because none of the alleged information can constitute actual "content," his Wiretap Act claim fails.

D. The Wiretap Act does not extend to electronic communications made by tracking devices, including smartphones.

Finally, the Wiretap Act claim fails because a communication sent from a smartphone does not constitute an "electronic communication" under the Act, which specifically provides that a "communication from a tracking device" is not a covered "electronic communication." 18 U.S.C. § 2510(12). A "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117. Courts have consistently held that cell site and GPS data transmitted from cellphones fall within this exclusion. *See, e.g., In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel.*, 849

[2] Plaintiff's "post office" analogy breaks down at this level, as discussed at the hearing. In particular, there is no "envelope," and so the distinction Plaintiff draws between "inside" and "outside" information is not useful. The better approach, as most courts have recognized, is the distinction between "content" and "non-content." *See* Orin S. Kerr, "Applying the Fourth Amendment to the Internet: A General Approach," 62 Stan. L. Rev. 1005 (2010). Under either approach, however, Plaintiff's location was not part of the "content" of his message(s).

F. Supp. 2d 526, 577 (D. Md. 2011) (collecting cases; holding that "cell phones, to the extent that they provide prospective, real time location information, regardless of the specificity of that location information, are tracking devices."). Here, Plaintiff alleges that Uber used Lyft drivers' smartphones as tracking devices, and so his Wiretap Act claim would fail even if that were true.

II. Plaintiff fails to demonstrate violations of CIPA sections 632 and 637.7.

The California Invasion of Privacy Act is similar to the federal Wiretap Act, and the two claims often fail for the same or similar reasons. *See NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 938, 954 (N.D. Cal. 2014). That is the case here. As in the initial complaint, the FAC alleges only two CIPA sections, 632 and 637.7. Uber has limited its discussion to those two sections. *See In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1098 (N.D. Cal. 2015) (providing that a plaintiff must identify the particular section of a statute that was violated). Plaintiff's CIPA claim fails because: (i) he failed to allege Uber "eavesdropped" on any "confidential communication" (as required by section 632), and (ii) he expressly consented to allow his smartphone to be used to track his location (triggering the exception to a section 637.7 violation).

A. CIPA section 632 is inapplicable because Plaintiff does not allege Uber eavesdropped on any confidential communications.

Section 632 punishes only an "eavesdropper," someone who:

> intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio . . . .

Cal. Penal Code § 632(a). The Ninth Circuit defines "eavesdrop" as "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). Plaintiff does not contend Uber intercepted, "secretly listened to," or recorded any of his communications. He contends Uber collected data from messages sent to Uber by Lyft, data that Plaintiff voluntarily sent to Lyft and agreed to let Lyft disseminate. *See* FAC ¶ 50 (at pp. 10:25–11:24); ¶ 72. He does not allege Uber "eavesdropped" on anyone.

Moreover, Plaintiff's willingness or availability to work, geolocation information, and Lyft ID number are not "confidential communications," which CIPA defines as:

> 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, but excludes a communication made in a public gathering ..., or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded.

Cal. Penal Code § 632(c); *see People v. Nakai*, 183 Cal. App. 4th 499, 518–19 (2010) (holding internet chat dialogues were not confidential communications under section 632 because users understood those conversations could be shared). The reasonable-expectation standard is objective — a communication is confidential only if "a party to the conversation had an objectively reasonable expectation that the conversation was not being overheard or recorded." *Faulkner v. ADT Sec. Servs., Inc.*, 706 F.3d 1017, 1019 (9th Cir. 2013) (quoting *Kearney v. Salomon Smith Barney, Inc.*, 39 Cal. 4th 95, 117 n.7 (2006)). Logic dictates that a Lyft driver cannot hold a reasonable expectation of privacy in his or her availability to work or geolocation data while using the Lyft app.

Plaintiff knew 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. He specifically consented to this. *See* Lyft TOS at p. 28 ("When you open Lyft on your mobile device, we receive your location."). Likewise, Plaintiff cannot claim a confidential interest in his "affirmation that he is currently willing to provide services to a rider" because he manifested this willingness as soon as he turned on the app, and he relied on Lyft to broadcast this information to the general public so that he could secure rides. FAC ¶ 72. Plaintiff cannot claim a reasonable expectation of privacy in information that was essential to his use of the Lyft app. He necessarily had to announce to Lyft that he was available for rides, and he knew Lyft would pass that information (along with his GPS location) to anyone who asked for it. There is nothing "confidential" about any of the driver information Lyft broadcasts, and for this reason, too, Plaintiff's section 632 claim fails.

B. Plaintiff's section 637.7 claim fails because he consented to the use of his cellphone as a tracking device with respect to his vehicle.

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). Here, Plaintiff, like all other Lyft drivers, expressly consented to the use of his cellphone as a

"tracking device" when he signed up to be a Lyft driver. In doing so, he agreed not only to let Lyft track his movements while he was working, but also to broadcast that information as widely as possible, so that he could make earnings. Thus, Plaintiff's section 637.7 claim fails because he consented to the use of his smartphone as a tracking device.

III. Plaintiff fails to state a claim under the Stored Communications Act.

Plaintiff's SCA claim—alleged in a single sentence—also fails. FAC ¶¶ 119–21.

A. Plaintiff does not allege Uber obtained Lyft driver information by "trespass."

The SCA prohibits unauthorized access to communications in electronic storage within "a facility through which an electronic communications service is provided…." 18 U.S.C. § 2701(a). This is analogous to common-law trespass. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) ("Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents … the Act protects users whose electronic communications are in electronic storage…."). Just as with trespass, an SCA violation requires unlawful entry. *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1041 (N.D. Cal. 2014) (SCA creates liability for "certain unauthorized access to wire and electronic communications and records"); *cf. State Wide Photocopy Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (stating section 2701 "was primarily designed to provide a cause of action against computer hackers (i.e., electronic trespassers).").

Plaintiff alleges only that Uber accessed "a facility through which an electronic communication services is provided," without clarifying which "facility" he means. FAC ¶ 121. He asserts twice that Uber "accessed" drivers' computers or smartphones directly (FAC ¶¶ 52, 97), but alleges no facts to support this. In any event, courts in this district have held personal devices are not "facilities" for SCA purposes. *See In re iPhone Application Litig.*, 844 F. Supp. 2d at 1057-58 (citing cases). As for the claim that Uber "accessed" a *Lyft* "facility" to obtain his stored electronic communications, as discussed above Plaintiff's allegations fail to show that Uber did any such thing. He alleges that Uber sent "requests" to Lyft servers and that those requests prompted Lyft servers to respond with "a list of nearby drivers who were logged in" to the Lyft app. FAC ¶¶ 67, 91. Plaintiff does not assert that Uber somehow hacked or otherwise trespassed into Lyft systems to obtain this information. Rather, the allegation is that Lyft itself provided the driver information to Uber upon

request. To apply Plaintiff's "post office" analogy, Plaintiff would be arguing that Uber knocked on Lyft's door and Lyft then slid under the door an envelope containing a list of nearby drivers. *See id.* ¶ 77 (claiming that "Lyft's servers transmitted" the driver information to Uber). Even if Uber said it was someone else at the door, it did not break in to get the envelope itself. Although Plaintiff insists that he did not intend for the envelope to be delivered to Uber, that is irrelevant. What matters is whether Uber accessed electronic information from within Lyft "facilities." Plaintiff alleges no facts to support such a claim.

B. Lyft driver IDs and GPS data are not temporary "stored communications."

As relevant here, the SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof...." 18 U.S.C. § 2510(17)(A). Plaintiff does not allege his driver data was in "temporary, intermediate storage" incidental to transmission.

To the contrary, Plaintiff alleges that Lyft keeps all geolocation data *permanently*. *Id.* ¶ 90 (alleging that neither Uber nor Lyft "ever delete the geolocation data" they collect.). If Plaintiff were right about that, then the SCA would not apply. *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001). In *Doubleclick*, the court considered whether cookies on the plaintiffs' hard drives were in "electronic storage" for purposes of § 2701. The court held they were not, because the plaintiff alleged they remained there indefinitely. *Id.* (holding SCA "only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it."). Plaintiff's similar allegation about Lyft's geolocation data defeats his SCA claim.

To the extent Plaintiff contends that Lyft kept the geolocation data only temporarily, he would still not have alleged a trespass to "electronic storage" under the SCA because he does not allege the communications were in "intermediate" storage "incident to transmission." The language and legislative history of the definition "make evident that 'electronic storage' ... is specifically targeted at communications temporarily stored by electronic communications services incident to their transmission—for example, when an email service stores a message until the addressee downloads it." *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal. 2015)

(citation and punctuation omitted). As discussed above, what Plaintiff alleges here is not access to a message being stored temporarily on Lyft servers until it can be sent on to a potential rider. He alleges a process that involved two or more steps: Lyft received communications from Lyft drivers and potential riders, and then, after analyzing the data, it sent its own communications back to potential riders. Unlike an email provider temporarily storing a message until the addressee downloads it—the scenario the SCA was intended to address—Lyft driver information is not being stored in Lyft's servers while awaiting final transmission to another location. Indeed, the drivers have no idea which third parties are receiving their most recent location and driver ID, so the email analogy is not accurate.

Because even a generous reading of Plaintiff's FAC fails to demonstrate that Uber accessed electronic communications in "electronic storage," Plaintiff's SCA claim should be dismissed.

IV. Plaintiff fails to state a claim under the Computer Data Access and Fraud Act.

Again for similar reasons, Plaintiff fails to state a claim under California's Computer Data Access and Fraud Act ("CDAFA"). Cal. Penal Code § 502. Plaintiff alleges Uber violated subdivisions(c)(1)–(3), (5), and (7). FAC ¶¶ 122–29. Among other things, this requires him to allege that (1) Uber acted "without permission" and (2) he "suffer[ed] damage or loss by reason of [the] violation." *Id.* § 502(c)(1)–(3), (5), (7), (10); id. § 502(e)(1). Under sections 502(c)(1), (2), and (7), Plaintiff must also allege unauthorized "access." He does not allege any of these requirements.

A. Plaintiff does not allege unauthorized "access."

Plaintiff's CDAFA claim is also conclusory and, among other things, does not even make clear what Plaintiff contends Uber "accessed" for purposes of CDAFA. Rather, he merely recites the statutory language. *See, e.g.*, FAC ¶ 125 (alleging Uber accessed "data, or a computer, or a computer system, or a computer network"). That does not satisfy Rule 8. *See Satmodo, LLC v. Whenever Commc'ns, LLC*, No. 17-CV-0192-AJB NLS, 2017 WL 1365839, at *6 (S.D. Cal. Apr. 14, 2017) (holding plaintiff had failed to allege sufficient facts to plead "access"). In any event, as discussed above, Plaintiff does not allege any facts showing that Uber "accessed" anyone's computer system other than Uber's own. *See e.g.*, FAC ¶¶ 52, 73, 77, 79, 85, 86. Just as he failed to allege a "trespass" for SCA purposes, he fails to allege the access required to show a violation of 502(c)(1), (2), and (7).

B. Plaintiff fails to allege that Uber acted "without permission."

Most courts have interpreted "without permission" for CDAFA purposes to mean "in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access." *Satmodo*, 2017 WL 1365839, at *6; *see also In re Google Android Consumer Privacy Litig.*, No. 11–mc–02264–JSW, 2013 WL 1283236, at *12 (N.D. Cal. Mar. 26, 2013); *In re iPhone Application Litig.*, No. 11–md–02250–LHK, 2011 WL 4403963, at *12–13 (N.D. Cal. Sept. 20, 2011). In the *Google* case, the court held allegations that Google used tracking codes (which, as in this case, the plaintiffs labeled "spyware") to collect personal data from Android phones were not sufficient to allege this element. 2013 WL 1283236, at *11-12; *see iPhone App. Litig.*, 2011 WL 4403963, at *12 (similar holding). Nor is it sufficient to allege, as Plaintiff also does here, that a defendant violated a term of service in order to get information. *iPhone App. Litig.*, 2011 4403963, at *12. Although Plaintiff's FAC is full of buzzwords like "scraping," "sniffers," and "industrial espionage," he actually alleges (at most) only that Uber used open-source or commercially available HTTP traffic logging software to collect data sent to Uber by Lyft's servers in response to requests made by Uber. FAC ¶¶ 53, 73. The FAC does not allege that Uber circumvented any technical or code-based barriers to do this. The CDAFA claim would fail for that reason as well.

A few courts have held that the "technical or code-based" requirement applies only to the CDAFA subdivisions that require proof of "access" (*i.e.*, hacking). *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 954, 965-67 (N.D. Cal. 2014). That would include all but two of the CDAFA subdivisions Plaintiff cites here, (c)(3) and (c)(5), and those claims would fail for other reasons. In particular, both sections require some sort of damage to or disruption of a computer. *See Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc.*, 556 F. Supp. 2d 1122, 1133 (E.D. Cal. 2008) (holding that like similar federal statute, 502(c)(3) requires damage to computer)); Cal. Pen. Code § 502(c)(5) (expressly requiring disruption or denial of service). There are no facts in the FAC suggesting any such effect on Lyft's servers or Plaintiff's phone.

C. Plaintiff fails to allege any "damage or loss."

Nor has Plaintiff himself suffered any damage. Section 502(e)(1) allows a party to recover compensatory damages only for "expenditure reasonably and necessarily incurred by the owner or

lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Plaintiff does not allege anything of the kind, nor (as discussed in more detail below) does he adequately allege any economic injury at all. He only speculates that, "over time," Uber's actions might have "reduce[d] the effectiveness of the Lyft app, thus harming drivers such as Plaintiff...." FAC ¶ 102. No facts support these assertions. Plaintiff does not allege, for example, that Lyft ridership or his earnings decreased while Uber allegedly used the program, or that ridership or his earnings increased after Uber stopped. Nor are his claims regarding the alleged collection of his private information sufficient to allege damage or loss. *See In re Google Android Consumer Privacy Litig.*, at *11 (dismissing Plaintiffs' CDAFA claim because the allegations regarding the diminished value of Plaintiffs' personally identifiable information were not sufficient to allege damage or loss). This claim, too, should be dismissed.

V. Plaintiff's constitutional privacy claim fails.

The last of Plaintiff's privacy claims, brought under the California Constitution, is also the weakest. To adequately allege this claim, a plaintiff must allege (1) a "reasonable expectation of privacy in the circumstances," (2) a "legally protected privacy interest," and (3) conduct that constitutes a "serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 39–40 (1994); *see Pioneer Elecs. (USA), Inc. v. Superior Court*, 40 Cal. 4th 360, 370 (2007) (California's "right of privacy protects [an] individual's reasonable expectation of privacy against a serious invasion") (emphasis in original). Even where those elements can be established, a court must still balance the privacy interest allegedly invaded against other competing or countervailing interests that may exist. *Pioneer*, 40 Cal. 4th at 371. Again, Plaintiff fails to state a claim.

First, for the same reasons explained above, Plaintiff has not alleged facts showing he had a "reasonable expectation of privacy" in the data Uber was allegedly collecting. A "reasonable" expectation of privacy is "an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal. 4th at 36. The extent of this entitlement depends on, for example, "[c]ustoms, practices, and [the] physical settings surrounding particular activities," as well as whether the plaintiff had "advance notice" of a potential intrusion and "the presence or absence of opportunities to consent voluntarily[.]" *Id.* Plaintiff concedes he voluntarily used Lyft's ridesharing-

request service. He downloaded the required Lyft app and agreed to terms and conditions that expressly allowed Lyft to track and broadcast his location. Plaintiff thus had no reasonable expectation of privacy as a matter of law. *Hill*, 7 Cal. 4th at 36–37; s*ee also Berry v. Webloyalty.com, Inc.*, No. 10-cv-13582011, 2011 WL 1375665, at *10 (S.D. Cal. Apr. 11, 2011) (holding plaintiff had no reasonable expectation of privacy in information he gave to MovieTickets.com where enrollment page stated that information would be shared); *vacated on other grounds*, 517 F. App'x 581 (9th Cir. 2013).

Second, Plaintiff has not pled a "legally protected privacy interest." The type of interest protected by the constitution is "an interest in precluding 'the dissemination or misuse of sensitive and confidential information[.]'" *Pioneer Elects.*, 40 Cal. 4th at 370 (quoting *Hill*, 7 Cal. 4th at 35) (emphasis added). A person's confidential medical profile or sexual orientation, for example, certainly might qualify. *See, e.g., Leonel v. Am. Airlines, Inc*., 400 F.3d 702, 712 (9th Cir. 2005) (medical profile); *Nguon v. Wolf*, 517 F. Supp. 2d 1177, 1196 (C.D. Cal. 2007) (sexual orientation). But the disclosure of "mere contact information," such as names and addresses, does not. *Pioneer Elects*., 40 Cal. 4th at 372 (holding this would not "unduly interfere" with the right to privacy). Similarly, "[a] person's general location is not the type of core value, informational privacy explicated in *Hill*." *Fredenburg v. City of Fremont*, 119 Cal. App. 4th 408, 423 (2004).

Here, Plaintiff alleges that Uber used this program to "monitor the whereabouts of all Lyft drivers in major markets," but as *Fredenburg* explained, such location information does not rise to the level of the "core value, informational privacy" intended to be protected. FAC ¶ 82. In an attempt to create an important privacy interest, Plaintiff hypothesizes about the ways Uber might have used Lyft drivers' location information to "retroactively scrutinize [their] activities." *Id.* ¶ 83. Specifically, Plaintiff alleges Uber created a historical database of Lyft drivers' personal data and then used that data in conjunction with unspecified databases to learn personal details about the drivers, including their full names, addresses, and work schedules (*i.e.*, when, where, and for how many hours they worked). *Id.* But as before, he alleges no facts to support any of this, which is not even consistent with his allegations that Uber's plan was to identify drivers using both apps and

encourage them to use only Uber's. He does not claim Uber had any interest in "tracking" or "scrutinizing" Lyft-only drivers like himself.

Importantly, courts have held that, even in the context of something as sensitive as private medical information, there is no legally protected privacy interest in "de-identified information" that "cannot be linked to individuals." *London v. New Albertson's, Inc.,* No. 08-cv-1173, 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (dismissing Cal. Const. art. I., § 1 claim). Though Plaintiff alleges the Lyft ID number is "tied to each individual driver," he does not allege the number was accompanied by personal information like his name, or that Uber had any way of determining (or was even trying to determine) the real identity of any Lyft-only driver. FAC ¶ 50 at p. 11:8–14. *Lyft* could presumably do that, of course, but Plaintiff alleges only that Uber was interested in the drivers' locations, and only the dual-app drivers' locations, and then only while they were driving for Lyft.

Third, Plaintiff fails to plead facts even approaching a "serious" invasion of privacy." *Hill*, 7 Cal. 4th at 40. Whatever the statutory claims might require, the constitutional claim requires an invasion "sufficiently serious" as to constitute "an egregious breach of the social norms underlying the privacy right." *See id.* at 37 (emphasis added). The conduct Plaintiff alleges here does not measure up. *See, e.g., In re iPhone Application Litig.,* 844 F. Supp. 2d at 1063 (dismissing invasion-of-privacy claim because disclosure of the plaintiffs' unique device identifier number, personal data, and geolocation information did not constitute an egregious breach of social norms); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127–28 (N.D. Cal. 2008), *aff'd*, 380 Fed. App'x 689 (9th Cir. 2010) (holding that negligent conduct leading to theft of highly personal information including Social Security numbers did not "approach [the] standard" required by the California Constitution).

The assertions Plaintiff includes in this cause of action (*e.g.* that the conduct affected his "interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference") are conclusory allegations, not facts, and serve only to highlight the difference between truly "serious" intrusions and what Plaintiff alleges here. *See* FAC ¶ 142 (quoting *Hill*); *Iqbal*, 556 U.S. at 678 (reiterating that allegations merely reciting the elements of a cause of action "will not do"). Californians have a constitutional right to keep intimate bodily functions private (*Hill*, 7 Cal. 4th at 40–41) and to be free from stalking and being filmed in their

homes (*Egan v. Schmock*, 93 F. Supp. 2d 1090 (N.D. Cal. 2000)). Plaintiff's allegation that Uber might have been able to determine the location and typical driving schedule associated with an anonymous Lyft driver bearing a particular Lyft ID number cannot satisfy this standard. Even if Uber had collected such information, the mere collection of that information still would not rise to the level of a serious intrusion on Lyft drivers' privacy. Moreover, there are no allegations that Uber used this information to stalk Lyft drivers (as alleged in *Egan*) or engage in any other intrusive conduct. Plaintiff's citation of an entirely unrelated news article about efforts to track the activities of taxi passengers in New York (FAC ¶ 81) hardly shows that Uber engaged in similar conduct here.

In addition, Plaintiff's new allegation that Uber used these same methods to determine the identities of Lyft drivers' *customers* should not be given any weight. FAC ¶ 83. Lyft riders are not parties or putative class members here, and Plaintiff's allegations about them are even more speculative than the allegations he offers about his own claims. Neither set of allegations is enough to state a claim for violating a constitutional privacy right.

VI. Plaintiff's Unfair Competition Law claim also fails.

Finally, Plaintiff also alleges that Uber's conduct constituted "unlawful" or "unfair" business practices in violation of the UCL. FAC ¶¶ 130–38. These claims fail because, for all the reasons explained above, Plaintiff has not alleged Uber engaged in any "unlawful" or "unfair" conduct. But the UCL claim would also fail because Plaintiff has not alleged any facts showing Uber caused him any injury, much less the loss of money or property required by the UCL. Nor has he alleged facts that would entitle him to equitable relief, the only kind the UCL permits.

A. Plaintiff lacks standing to bring a UCL claim.

A private party has standing to bring a UCL action only if he or she has suffered "injury in fact" and lost money or property as a result of the defendant's alleged unfair or unlawful practices. Cal. Bus. & Prof. Code § 17204; *Kwikset v. Super. Ct.*, 51 Cal. 4th 310, 322 (2011); *Koussa v. Ming Yeung*, No. 16-cv-05137-JSC, 2017 WL 1208073, at *2 (N.D. Cal. Apr. 3, 2017). A plaintiff must allege facts that plausibly "(1) establish a loss or deprivation of money sufficient to qualify as an injury in fact, i.e., *economic injury*, and (2) show that the economic injury was the result of, i.e., *caused by*, the unfair business practice ...." *Koussa*, 2017 WL 1208073, at *2 (quoting *Kwikset*); *see*

Jou v. Kimberly-Clark Corp., No. C-13-03075-JSC, 2013 WL 6491158, at *2–3 (N.D. Cal. Dec. 10, 2013) (noting that plaintiff has burden to establish standing). Plaintiff's FAC still contains no facts showing that he (or anyone) actually lost any money or property as a result of the alleged scheme.

Like the original complaint, the FAC says virtually nothing about the topic, which it covers in just three paragraphs:

- "Upon information and belief, Uber profited from the Hell spyware in a number of ways."
- "Upon information and belief, Uber used the information gleaned from Hell to direct more frequent and more profitable trips to Uber drivers who used the Lyft App. 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 Lyft drivers available."
- "With the effective supply of Lyft drivers reduced, Lyft customers faced longer wait times. As a result, Lyft riders would cancel the ride requested with Lyft and request a new ride from Uber. Over time, this would reduce the effectiveness of the Lyft App, thus harming drivers such as Plaintiff and absent Class Members."

See FAC ¶¶ 100–02.[3] None of this is remotely adequate to allege UCL standing.

Plaintiff still cannot or will not plainly allege that *he* lost money. The above paragraphs say only—and only on information and belief—that (1) Uber profited; (2) some "dual-app" drivers benefited; and (3) "over time," the effectiveness of the Lyft app used by drivers "such as" Plaintiff "would" have been reduced. Even assuming a "less effective" Lyft app would necessarily result in reduced earnings, Plaintiff's allegations fall well short of alleging that he actually lost any money. Indeed, Plaintiff concedes he stopped using the Lyft app altogether in November 2014 (FAC ¶ 19), which according to him was in the early part of a scheme that lasted "from 2014 through 2016" (FAC ¶ 8), the effects of which could only have been felt "over time" (FAC ¶¶ 100–02). He offers no facts even suggesting they could have been felt, by anyone, before November 2014. But the bottom line is that he does not allege *he* felt the financial effects, if there were any.

Further, any alleged effects on Uber, on drivers using both the Uber and Lyft apps, or on drivers who used only the Uber app, are all irrelevant to whether *Plaintiff* has standing. Of course,

[3] Paragraphs 9 and 137 technically also relate to injury, but add nothing to those above. Paragraph 9 is the same theory asserted in paragraphs 101 and 102, and paragraph 137 is the conclusory allegation of injury in the UCL count.

Uber and dual-app drivers would all have *benefited*, according to Plaintiff. (If dual-app drivers were "inundated" with ride requests, as Plaintiff alleges, that would presumably have been a good thing for them.) To the extent Plaintiff is still alleging that drivers who used only the Uber app were harmed, that is irrelevant because Plaintiff is not in that group: he used only the *Lyft* app. FAC ¶¶ 19–21. Finally, it is telling that although the whole point of the scheme, according to Plaintiff, was to gain a comparative advantage over Lyft, in the FAC Plaintiff actually appears to downplay the allegations that Lyft itself was ever harmed. Originally, he alleged that "[o]ver time, this would have been *very damaging to the Lyft market*," but now he alleges that "[o]ver time, this would *reduce the effectiveness of the Lyft App*...." Compl. ¶ 59, FAC ¶ 102 (emphasis added). As suggested above, it is not clear just what this new allegation is intended to mean, but nowhere in the FAC are there any facts that would show Lyft itself was actually harmed by the alleged practice. Plaintiff, of course, was at least one step further removed from injury than Lyft. For that matter, if the supply of Lyft drivers had been reduced as Plaintiff previously alleged, Plaintiff or other Lyft drivers might actually have *benefited* because their chances of connecting with a rider could have increased. In short, Plaintiff's sparse allegations of economic injury are only speculation.

Nor could Plaintiff argue he suffered economic injury on some theory that his privacy or the personal information he "lost" had monetary value. The privacy counts fail in any event, but regardless, courts have consistently rejected UCL claims based on theories that information had monetary value. *See, e.g.*, *In re Facebook Privacy Litig.*, No. 12-15619, 2014 WL 1815489, at *1 (9th Cir. May 8, 2014) (affirming dismissal of UCL claim alleging that disseminated personal information had economic value); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014) (finding alleged "property interest" in lost personal information and message content insufficient; noting that "courts have consistently rejected such a broad interpretation of 'money' or 'property'" in UCL cases); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1056 n.22 (N.D. Cal. 2014); *In re iPhone Application Litig.*, No. 11–MD–02250, 2011 WL 4403963, at *14; *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 862 (N.D. Cal. 2011).

In sum, these allegations too amount to nothing more than speculation. Plaintiff alleges no facts whatsoever showing that he (or anyone else) actually suffered any injury in fact as a result of

Uber's alleged conduct. He only recites the phrase "money or property" and theorizes that an injury *might* have been suffered under some set of facts. This does not state a claim. *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 959–62 (9th Cir. 2009) (holding plaintiffs who alleged consumers *might* suffer hearing loss from listening to iPods did not establish Article III or UCL standing). Without any facts to support his assertion, Plaintiff's UCL claim necessarily fails.

B. The UCL claim would also fail because Plaintiff does not allege facts showing the available legal remedies would be inadequate.

Even if Plaintiff had alleged an economic injury of some kind, he could not use the UCL to redress it because he has not alleged that his legal remedies would be inadequate for that purpose. It is fundamental "that courts of equity should not act ... when the moving party has an adequate remedy at law and will not suffer irreparable injury if denied equitable relief." *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 381 (1992) (internal quotation omitted). Here, the UCL claim—which permits only equitable relief—also fails because Plaintiff alleges no facts showing his legal remedies would be inadequate. *See Moss v. Infinity Ins. Co.*, 197 F. Supp. 3d 1191, 1203 (N.D. Cal. 2016); *see also Nguyen v. Nissan N. Am., Inc.*, No. 16-cv-05591, 2017 WL 1330602, at *3–4 (N.D. Cal. Apr. 11, 2017); *Munning v. Gap, Inc.*, No. 16-CV-03804, 2017 WL 733104, at *5 (N.D. Cal. Feb. 24, 2017). If Plaintiff suffered any economic harm, an award of damages would compensate for that, and he alleges no facts suggesting otherwise.

For similar reasons, Plaintiff cannot seek injunctive relief, despite a recent Ninth Circuit decision addressing injunctive relief in UCL deceptive-practice cases. *Davidson v. Kimberly-Clark Corp.*, No. 15-16173, 2017 WL 4700093 (9th Cir. Oct. 20, 2017). In *Davidson*, the court resolved a split of authority by holding that a plaintiff can seek an injunction against false statements in advertising or labeling even though the plaintiff has conceded that he or she is now aware that the statements are false. *Id*. at *6–10. That is irrelevant here, however, both because Plaintiff has not alleged a violation of the UCL's deceptive-practice prong (*see* FAC ¶¶ 130–38) and because Plaintiff has *conceded* he has no basis for injunctive relief. Again, Plaintiff alleges he stopped driving for Lyft in November 2014, and that Uber stopped collecting the allegedly private information in 2016. FAC ¶¶ 8, 50, 52. *See Bentley v. United of Omaha Life Ins. Co.*, No. CV-15-

7870, 2016 WL 7443189, at *7 (C.D. Cal. June 22, 2016) (holding that because policy in question had lapsed, UCL claim for injunctive relief failed). While Plaintiff now alleges that Uber still has the information it collected, he does not actually allege that Uber is using it in any way. FAC ¶ 91. Beyond that, Plaintiff offers no reason to think there would *be* any use now for information about locations he might have occupied more than three years ago. For that reason, too, he cannot seek prospective injunctive relief.

CONCLUSION

Plaintiff's amended complaint is again based mostly on allegations made in a single online article, now bolstered with Wikipedia articles about basic Internet technology and a host of allegations made only on "information and belief." The complaint describes, at best, a claim that Uber collected and used information in communications that it tricked Lyft into sending to Uber, information that Plaintiff had expressly agreed could be disseminated, effectively, to anyone who asked. Even with the benefit of leave to amend, Plaintiff has been unable to allege a plausible theory. The Court should dismiss the FAC with prejudice.

Dated: October 27, 2017

Respectfully submitted,
SHOOK HARDY & BACON L.L.P.

By: */s/ M. Kevin Underhill*
PATRICK L. OOT
M. KEVIN UNDERHILL
ANNIE Y.S. CHUANG

Attorneys for Defendants