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

John K. Sherk, SBN 295838
Annie Y.S. Chuang, SBN 196307
One Montgomery, Suite 2700
San Francisco, California 94104
Tel: 415.544.1900 | Fax: 415.391.0281
jsherk@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 CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES

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

Hearing date: August 17, 2017
Time: 9:00 a.m.
Judge: Hon. Jacqueline Scott Corley
Courtroom: F-15th Floor

NOTICE OF MOTION

TO ALL PARTIES AND ATTORNEYS OF RECORD HEREIN:

Please take notice that on August 17, 2017, at 9:00 a.m. before the Honorable Jacqueline Scott Corley, in Courtroom F of the United States District Court for the Northern District of California, San Francisco Division, located at 450 Golden Gate Avenue, San Francisco, California, defendants Uber Technologies, Inc.; Uber USA, LLC; and Rasier-CA will and hereby do move the Court for an Order dismissing Plaintiff's Complaint.

This motion is made pursuant to Rule 12(b)(1) and Rule 12(b)(6) of the Federal Rules of Civil Procedure and is based on the following grounds:

1) Plaintiff's claim under the Wiretap Act 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 "tracking devices";
2) Plaintiff's California Invasion of Privacy Act claim fails for similar reasons, including the failure to allege Uber "eavesdropped on confidential communications";
3) The constitutional privacy claim fails for similar reasons and because the state constitution protects only against much more serious intrusions than alleged here; and
4) Plaintiff's Unfair Competition Law claim fails because he has not alleged injury in fact or any loss of money or property, and has not alleged any basis for equitable relief.

The motion is based on the Notice of Motion, the supporting memorandum, the pleadings, and such argument as the Court may allow.

Dated: June 19, 2017

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

By: /s/ *John K. Sherk*
PATRICK L. OOT
JOHN K. SHERK
ANNIE Y.S. CHUANG

Attorneys for Defendants

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF CONTENTS

INTRODUCTION 1

FACTUAL BACKGROUND 2

LEGAL STANDARD 4

ARGUMENT 4

I. Plaintiff fails to allege facts showing a violation of the Wiretap Act. 4

A. Plaintiff does not allege an interception. 4

B. The communications at issue here were "electronic communications … readily accessible to the general public." 6

C. Plaintiff does not allege Uber intercepted the "contents" of a communication. 8

D. The Wiretap Act does not extend to electronic communications made by tracking devices, including smartphones. 10

II. Plaintiff's CIPA claim fails for similar reasons. 11

A. CIPA section 632 is inapplicable because Plaintiff does not allege that Uber eavesdropped on any confidential communications. 11

B. Plaintiff's section 637.7 claim fails because he consented to providing his location data to Lyft. 13

III. Plaintiff's constitutional privacy claim fails. 13

IV. Plaintiff's Unfair Competition Law claim also fails. 16

A. Plaintiff lacks standing to pursue his UCL claim. 16

1. Plaintiff has not alleged injury-in-fact. 16

2. Plaintiff does not allege any loss of money or property. 17

B. The UCL claim also fails because Plaintiff does not allege facts showing the available legal remedies would be inadequate. 18

CONCLUSION 19

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

TABLE OF AUTHORITIES

Cases **Page(s)**

Ashcroft v. Iqbal,
556 U.S. 662 (2009)....................4, 5, 15

Bell Atl. Corp. v. Twombly,
550 U.S. 544 (2007)....................4

Bentley v. United of Omaha Life Ins. Co.,
No. CV-15-7870, 2016 WL 7443189 (C.D. Cal. June 22, 2016)....................19

Berry v. Webloyalty.com, Inc.,
No. 10-cv-13582011, 2011 WL 1375665 (S.D. Cal. Apr. 11, 2011)....................14

Birdsong v. Apple, Inc.,
590 F.3d 955 (9th Cir. 2009)....................17

Campbell v. Facebook Inc.,
77 F. Supp. 3d 836, 849 (N.D. Cal. 2014)....................17

Claridge v. RockYou, Inc.,
785 F. Supp. 2d 855 (N.D. Cal. 2011)....................17

Cobra Pipeline Co. v. Gas Natural, Inc.,
132 F. Supp. 3d 945, 948 (N.D. Ohio 2015)....................5

Cousineau v. Microsoft Corp.,
992 F. Supp. 2d 1116 (W.D. Wash. 2012)....................9, 10

Crandall v. Starbucks Corp.,
No.15-cv-01828–JSC, 2017 WL 1246749 (N.D. Cal. Apr. 5, 2017)....................2

Crowley v. CyberSource Corp.,
166 F. Supp. 2d 1263 (N.D. Cal. 2001)....................5

Datel Holdings, Ltd. v. Microsoft Corp.,
712 F. Supp. 2d 974 (N.D. Cal. 2010)....................2

Dept. of Fish & Game v. Anderson-Cottonwood Irrigation Dist.,
8 Cal. App. 4th 1554 (1992)....................18

Duttweiler v. Triumph Motorcycles (Am.) Ltd.,
No. 14-cv-04809, 2015 WL 4941780 (N.D. Cal. Aug. 19, 2015)....................18

Egan v. Schmock,
93 F. Supp. 2d 1090 (N.D. Cal. 2000)....................15

1 *Faulkner v. ADT Sec. Servs., Inc.*,
706 F.3d 1017 (9th Cir. 2013) 12
2
3 *Fredenburg v. City of Fremont*,
119 Cal. App. 4th 408 (2004) 14
4 *Gelbard v. United States*,
5 408 U.S. 41 (1972)....................9
6 *Hill v. Nat'l Collegiate Athletic Ass'n*,
7 Cal. 4th 1 (1994) 13, 14, 15
7
8 *In re Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel.*,
849 F. Supp. 2d 526 (D. Md. 2011)....................10
9
10 *In re Carrier IQ, Inc.*,
78 F. Supp. 3d 1051 (N.D. Cal. 2015)....................10, 11
11
12 *In re Facebook Internet Tracking Litig.*,
140 F. Supp. 3d 922, 935 (N.D. Cal. 2015)....................8
13 *In re Facebook Privacy Litig.*,
No. 12-15619, 2014 WL 1815489 (9th Cir. May 8, 2014)....................17
14
15 *In re iPhone Application*,
844 F. Supp. 2d 1040 (N.D. Cal. 2012)....................9, 15
16 *In re iPhone Application Litig.*,
17 No. 11–MD–02250, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011)....................17
18 *In re Pharmatrak, Inc. Privacy Litig.*,
329 F.3d 9 (1st Cir. 2003)....................6
19
20 *In re Zynga Privacy Litig.*,
750 F.3d 1098 (9th Cir. 2014) 9
21 *Jou v. Kimberly-Clark Corp.*,
22 No. C-13-03075-JSC, 2013 WL 6491158 (N.D. Cal. Dec. 10, 2013)....................16
23 *Kearney v. Salomon Smith Barney, Inc.*,
39 Cal. 4th 95 (2006) 12
24
25 *Knievel v. ESPN, Inc.*,
393 F.3d 1068 (9th Cir. 2005) 2
26 *Konop v. Hawaiian Airlines, Inc.*,
27 302 F.3d 868 (9th Cir. 2002) 4, 6, 8
28

Korea Supply Co. v. Lockheed Martin Corp.,
29 Cal. 4th 1134 (2003) 18

Kwikset v. Super. Ct.,
51 Cal. 4th 310 (2011) 16

Leonel v. Am. Airlines, Inc.,
400 F.3d 702 (9th Cir. 2005) 14

London v. New Albertson's, Inc.,
No. 08-cv-1173, 2008 WL 4492642 (S.D. Cal. Sept. 30, 2008)....................14

Luman v. Theisman,
647 F. App'x 804 (9th Cir. Apr. 8, 2016)....................18

Marsh v. Zaazoom Solutions, LLC,
No. C-11-05226, 2012 WL 952226 (N.D. Cal. Mar. 20, 2012) 4

Morales v. Trans World Airlines, Inc.,
504 U.S. 374 (1992)....................18

Moss v. Infinity Ins. Co.,
197 F. Supp. 3d 1191, 1203 (N.D. Cal. 2016) 18

Munning v. Gap, Inc.,
No. 16-CV-03804, 2017 WL 733104 (N.D. Cal. Feb. 24, 2017) 18

Nguon v. Wolf,
517 F. Supp. 2d 1177 (C.D. Cal. 2007) 14

Nguyen v. Nissan N. Am., Inc.,
No. 16-cv-05591, 2017 WL 1330602 (N.D. Cal. Apr. 11, 2017)....................18

NovelPoster v. Javitch Canfield Group,
140 F. Supp. 3d 938, 954 (N.D. Cal. 2014) 11

Opperman v. Path, Inc.,
87 F. Supp. 3d 1018, 1056 17

People v. Nakai,
183 Cal. App. 4th 499 (2010) 12

Perez v. Nidek Co.,
711 F.3d 1109 (9th Cir. 2013) 18

Philips v. Ford Motor Co.,
No. 14-cv-02989, 2015 WL 4111448 (N.D. Cal. July 7, 2015) 18

Pioneer Elecs. (USA), Inc. v. Superior Court,
40 Cal. 4th 360 (2007) 13, 14

Ruiz v. Gap, Inc.,
540 F. Supp. 2d 1121 (N.D. Cal. 2008), *aff'd*, 380 Fed. App'x 689 (9th Cir. 2010) 15

Snow v. DirecTV, Inc.,
450 F.3d 1314 (11th Cir. 2006) 7, 8

Thomasson v. GC Services Ltd. P'ship,
321 Fed. App'x 557 (9th Cir. 2008) 12

United States v. Jones,
565 U.S. 400 (2012)..10, 11

United States v. Reed,
575 F.3d 900 (9th Cir. 2009) 9

Zapata Fonseca v. Goya Foods Inc.,
No. 16-cv-02559, 2016 WL 4698942 (N.D. Cal. Sept. 8, 2016)..18

Statutes

18 U.S.C. §2510(4) 8

18 U.S.C. § 2510(8) (1986) 8, 9, 10

18 U.S.C. § 2510(12) 10

18 U.S.C. § 2511...4

18 U.S.C. § 2511(2)(g) 7

18 U.S.C. § 2511(2)(g)(i)...6

18 U.S.C. § 2520(a) 4

18 U.S.C. § 3117...10

Cal. Bus. & Prof. Code § 17204 ....16, 17

Cal. Penal Code § 632(a) 12

Cal. Penal Code § 632(c) 12

Cal. Penal Code § 637.7(a) 13

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

Michael Gonzales claims Uber violated his privacy by collecting data related to his work as an independent, third-party transportation provider ("driver") with Lyft. But that data was never private. Lyft is a ridesharing-request service that uses a smartphone app to match potential riders with drivers. Gonzales's business as a driver therefore *depended* on making his location available, and he expressly agreed to let Lyft broadcast his location for just that reason: trying to connect with nearby riders to take them places just doesn't work if you keep your whereabouts a secret.

As almost anyone who has walked the streets of a major American city can attest, cars bearing Lyft and Uber logos are everywhere. So are brightly colored taxicabs. Beyond this public-facing trade dress, ridesharing-request services use smartphone GPS technology, which allows riders to identify on a map the available drivers in close proximity and then enables safety-monitoring features once a trip begins. Having consented to let Lyft broadcast his location to the public, Gonzales cannot reasonably claim he also expected it to be private. The Court should dismiss his complaint for several reasons.

First, Gonzales's Wiretap Act claim fails because, among other things, the allegedly "private" information was in fact "readily accessible to the general public" via the Lyft application, and because Gonzales does not allege that Uber intercepted any communication, much less the *content* of a communication.

Second, his claim under California's Invasion of Privacy Act fails for similar reasons: he does not allege Uber "eavesdropped" on "confidential communications," and he expressly consented to allow Lyft to broadcast the supposedly private location data.

Third, the California constitution protects only against "serious violations" of a "legally protected" and "reasonable" expectation of privacy. Again, while Gonzales's complaint is full of electronic-privacy buzzwords, it contains no facts showing that any of these elements are met here.

Finally, Gonzales's UCL claim fails because he does not allege any unfair or unlawful conduct, because he does not adequately allege injury-in-fact, and because he does not claim he lost money or property as a result of the alleged conduct.

FACTUAL BACKGROUND

Plaintiff Michael Gonzales ("Plaintiff") is a California resident who alleges he was a Lyft driver from sometime in 2012 until November 2014. Compl. ¶¶ 15–16. His complaint, however, says little about what it means to be a "Lyft driver" or how ridesharing-request services work. For that matter, there are few factual allegations anywhere in the complaint other than those copied from the text of an online article originally posted on a tech-news website. *See* Compl. ¶ 49 (quoting article posted on "The Information," www.theinformation.com, on Apr. 12, 2017). The article itself hinges on two anonymous sources. *See id.* ¶ 49 at p. 8:18–19 (citing one "person who was involved in the program" and one who was only "briefed about it"). Plaintiff has simply cut-and-pasted the text of the article into Paragraph 49, which comprises almost all of the complaint's "Substantive Allegations" section. *See id.* ¶¶ 46–59.

Plaintiff does allege that ridesharing-request services match those who need rides with drivers, which is done using software applications that riders and drivers download to their smartphones. *See* Compl. ¶ 49 at pp. 10:21–23; 11:5–8. That is consistent with Lyft's description of its service as providing "a marketplace where persons who seek transportation to certain destinations ('Riders') can be matched with persons driving to or through those destinations ('Drivers')." Lyft Terms of Service ¶ 1.[1]

Lyft driver location information is sent via the internet directly from driver smartphones to Lyft servers. *See* Compl. at ¶¶ 6, 49, pp. 10–11 (referring to Lyft's "platform" or "network"); *see also* Lyft Terms of Service, ¶ 12 ("Any of your Information, including geolocational data, you upload, provide, or post *on the Lyft Platform* may be accessible to Lyft and certain Users of the Lyft Platform") (emphasis added). When a user seeks a ride, the company's system sends driver locations to the app. Compl. ¶ 49 at p. 10:6–10. This data transmission not only provides the number of

---

[1] Plaintiff cites and relies on Lyft's Terms of Service ("TOS") and so has incorporated them by reference. *See* Compl. ¶ 49 at p. 9:25–27, ¶ 50; *Knievel v. ESPN, Inc.*, 393 F.3d 1068, 1076 (9th Cir. 2005). Lyft's TOS is also available online at www.lyft.com/terms. As this Court recently noted, "[i]t is not uncommon for courts to take judicial notice of factual information found on the world wide web." *Crandall v. Starbucks Corp.*, No.15-cv-01828–JSC, 2017 WL 1246749, at *4 (N.D. Cal. Apr. 5, 2017); *see Datel Holdings, Ltd. v. Microsoft Corp.*, 712 F. Supp. 2d 974, 983–84 (N.D. Cal. 2010) (taking judicial notice of online license and terms of use).

drivers in the area, but also the individual drivers' precise locations and anonymized ID numbers.[2] *Id*. The broad dissemination of driver-geolocation data, of course, is necessary to a ridesharing-request service, as Lyft's own terms of service explain: "Rider and Driver location is core to the Lyft Platform and without it we can't provide our services to you." Lyft Terms of Service, ¶ 5. Plaintiff does not allege that Uber eavesdropped on driver communications with Lyft or that it interfered with any transmission, only that Uber collected location data.

Plaintiff alleges that, beginning sometime in 2014, Uber began copying the publicly available location information to use as market intelligence. Compl. ¶ 49. He further alleges that the data allowed Uber to analyze the number of available Lyft drivers in a given area and learn the prices being charged for certain trips. *Id.*

In the online article on which Plaintiff relies, the article's author speculated that Uber may have used location data to steer more rides towards drivers who were working for both Lyft and Uber. Compl. ¶ 49. The author concedes, however, that even if Uber did try to sway Lyft drivers, the actual impact of this rumored incentive program, if any, would be "hard to estimate." *Id.* The author also did not conclude that Uber's alleged use of Lyft data had any negative impact on Lyft drivers themselves. *Id.* The author's source told him that Uber stopped copying Lyft driver data sometime "in the early part of 2016." *Id.*

According to Plaintiff, "more than 315,000 individuals have driven for Lyft in the United States." Compl. ¶¶ 36, 49. He purports to represent a nationwide class of Lyft drivers "whose private information and whereabouts was obtained by Uber by accessing computer systems operated or used by Lyft and the Class." *Id.* ¶ 32. Importantly, although drivers may use both the Uber and Lyft apps, the putative class members are Lyft-only drivers, or those who "(1) worked as drivers for Lyft, (2) while not working for Uber[.]" *Id.* ¶¶ 32–33. Plaintiff asserts claims for alleged violations of the Federal Wiretap Act as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C.

---

[2] Though Plaintiff refers to the Lyft identifier numbers as anonymous "driver ID[s]," it would be more accurate to call them "*vehicle* identifiers." This is more accurate because Plaintiff does not even allege Uber was ever interested in or collected any of his personal data, only his location while he was in a vehicle operating as a Lyft driver.

§§ 2510 *et seq.*, referred to here as the "Wiretap Act"); the California Invasion of Privacy Act (Cal. Penal Code §§ 630 *et seq.*); California's Unfair Competition Law (Cal. Bus. & Prof. Code §§ 17200 *et seq.*); and Article I, Section I of the California Constitution.

LEGAL STANDARD

A court must dismiss a complaint under Rule 12(b)(6) where a plaintiff fails to allege "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(a) "does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions."). This requires "factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged," and "asks for more than a sheer possibility that a defendant has acted unlawfully." *Iqbal*, 556 U.S. at 678. 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.

ARGUMENT

I. Plaintiff fails 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 Wiretap Act

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").

Here, Plaintiff alleges that Uber collected information about his location and the location of other Lyft drivers by creating Lyft rider accounts and viewing the information Lyft sent to those accounts. Compl. ¶ 49 at pp. 9:25–10:10. That information included the anonymized Lyft ID numbers for Lyft drivers in the area. *Id*. Importantly, however, Plaintiff specifically alleges only that Uber collected this information from Lyft rider accounts that Uber had created. *Id*. He does **not** allege it collected this data during a transmission between Lyft and its drivers or vice versa. Therefore, Plaintiffs do not allege an "interception" within the meaning of the Wiretap Act.

Plaintiff's allegations are analogous to Wiretap Act claims recently dismissed by the Northern District of Ohio. *Cobra Pipeline Co. v. Gas Natural, Inc.*, 132 F. Supp. 3d 945, 948 (N.D. Ohio 2015). There, 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 additional data, such as historical location information, vehicle identification numbers, and driver names. *Id.* at 948. The court dismissed the Wiretap Act cause of action because the plaintiff had not shown 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 was immaterial to the "threshold" question of whether doing so was an "interception" under the Wiretap Act. As the court stated (consistent with *Konop* and *Marsh*), "[i]nterception 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 transmissions' endpoint "did not interrupt an otherwise-occurring transmission." *Id*. The same would be true of Uber's alleged use of Lyft rider accounts here.

While the complaint occasionally suggests that Uber accessed computer systems operated by Lyft and/or Lyft drivers themselves, those are conclusory allegations unsupported by facts. *See, e.g.*, Compl. ¶¶ 4, 32, 54; *see also Iqbal*, 556 U.S. at 678 (conclusory allegations not entitled to presumption of truth); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1268 (N.D. Cal. 2001) ("The Court need not accept a conclusory allegation that conduct alleged in the complaint

constituted an interception under the Wiretap Act."). Plaintiff's "substantive allegations" are drawn entirely from the online article, and that article alleges only that Uber acquired Lyft driver data from the rider accounts it created, not from transmissions between two other points and certainly not from the servers or computers of Lyft or Lyft drivers. *See* Compl. ¶ 49 at pp. 9:25–10:15. Therefore, Plaintiff has not adequately alleged that Uber "intercepted" anything, and his Wiretap Act claim fails for this reason alone.

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

Even if Plaintiff had alleged an "interception" in some sense, he has not alleged the communications involved were protected under the Wiretap Act. Congress's objective in passing the Wiretap Act was to ensure that federal law adequately guarded against the unwanted interception of electronic communications. *See* S. Rep. No. 99-541, at 1–3 (Conf. Rep.). Be it from "overzealous law enforcement agencies, industrial spies, [or] just plain snoops," Congress believed that intrusion on personal or proprietary communications threatened the sanctity and privacy of America's communications systems. *See* 145 Cong. Rec. S.7992 (daily ed. June 19, 1986) (statement of Sen. Leahy). A plain and common-sense reading of ECPA's Wiretap Act provisions and its legislative history shows that Congress meant to provide additional protections for *private* communications. *See* 145 Cong. Rec. S.7992 (daily ed. June 23, 1986) (statement of Rep. Moorhead: "In short, [ECPA] provides clear rules governing the interception of private communications and thereby maintains the integrity of our communications systems."); *see also Konop*, 302 F.3d at 875 (holding ECPA legislative history suggests "Congress wanted to protect electronic communications that are configured to be private, such as email[.]"); *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003) ("The paramount objective of the Wiretap Act is to protect effectively the privacy of communications."). Accordingly, the Wiretap 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." Again, Lyft itself describes its service as a "marketplace" in which

riders and drivers can be matched. Lyft Terms of Service ¶ 1. That marketplace is enormous. Lyft is, of course, 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.[3] Plaintiff's source alleges that there were 315,000 Lyft drivers in 2016 alone (Compl. at 10:13), and a 2016 estimate suggested that the total number of monthly active Lyft riders at the time was about 3.6 million.[4] 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 meet 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).[5] The bulletin board required users to register, create a password, and affirm that they had no association with DirectTV. *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. Therefore, the plaintiff's allegations 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

---

[3] *See* Lyft Help, How to Create a Lyft Account, https://help.lyft.com/hc/en-us/articles/214216237-How-to-Create-a-Lyft-Account.

[4] Mike Sonders, *These latest Uber statistics show how it's dominating Lyft*, Medium, Dec. 7, 2016, https://medium.com/@sm_app_intel/these-latest-uber-statistics-show-how-its-dominating-lyft-53f6b255de5e.

[5] *Snow* involved a Stored Communications Act claim, but the SCA and the Wiretap Act share the same "readily accessible" exception language. *See* 18 U.S.C. § 2511(2)(g) (also referring to electronic communications "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.").

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

that the electronic communication not be readily accessible by the general public is material and essential to recovery[.]"[6] *Id.* at 1321. That requirement defeats Plaintiff's claim here as well.

Plaintiff's allegation that Uber collected anonymized "Lyft ID" numbers does not change the result. Compl. at p. 10:6–10. Plaintiff claims that 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. (Plaintiff's complaint admits that the Uber app also uses publicly disclosed driver ID numbers.) 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."[7]

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). Interpreting this definition, 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 1098, 1106–07 (9th Cir. 2014)). Even if Plaintiff had alleged Uber was

---

[6] The *Snow* court distinguished *Konop*, where the plaintiff had created an electronic bulletin board that was only available to particular Hawaiian Airlines employees. 302 F.3d 868, 872–73 (9th Cir. 2002). Unlike the bulletin board in *Snow*, one wishing to access the *Konop* airline employee site needed to have knowledge that was not publicly available (an eligible employee's name). No such special information is needed to use the Lyft app.

[7] Notably, much of the same information is apparently being collected by other entities or individuals not associated with Lyft. *See, e.g.*, NYC Taxi and Limousine Commission, TLC Trip Data, http://www.nyc.gov/html/tlc/html/about/trip_record_data.shtml (providing monthly summary reports aggregating taxi, Uber, and Lyft usage statistics, including pick-up and drop-off locations); *see also* Todd Schneider, "Taxi, Uber, and Lyft Usage in NYC," http://toddwschneider.com/posts/taxi-uber-lyft-usage-new-york-city/ (also analyzing this data).

1 "intercepting" communications not "readily accessible to the general public," his claim would still
2 fail because he alleges only that Uber intercepted data, not "contents."
3 The information Uber allegedly collected using the Lyft app did not reveal the substance,
4 purport, or meaning of any communication. As this Court and others have held, geolocation data and
5 other pieces of background information (like an anonymized Lyft ID number) constitute record
6 information, the collection of which does not implicate the Wiretap Act. *See In re Zynga*, 750 F.3d at
7 1106 (explaining that "record information" refers to non-content information that is generated in the
8 course of a communication"). "'[C]ontent' is limited to information the user intended to
9 communicate, such as the words spoken in a phone call." *In re iPhone Application*, 844 F. Supp. 2d
10 1040, 1062 (N.D. Cal. 2012) (citing *United States v. Reed*, 575 F.3d 900 (9th Cir. 2009)).
11 In *In re iPhone Application*, iPhone users claimed Apple violated the Wiretap Act by
12 allowing third-party applications to collect personal information, such as the plaintiffs' names,
13 precise geographic locations, unique device identifiers, genders and ages. *Id.* at 1061–62. The court
14 held that iPhone geolocation data was not comparable to a phone conversation, and thus not the
15 "content" of a communication, even if it conveyed the identity of the parties. *Id.* at 1061. Indeed, the
16 court observed that the Wiretap Act definition of "content" in effect prior to the 1986 ECPA
17 amendments covered "all aspects of the communication itself," including the identity of the parties
18 and the fact that the communication occurred. *Id.* (quoting *Gelbard v. United States*, 408 U.S. 41, 51
19 n.10 (1972)). But the amended definition of "content" eliminated the phrase "information concerning
20 the identity of the parties to such communication or the existence ... of that communication." *See id.*
21 (citing 18 U.S.C. § 2510(8) (1986)). Thus, "under the current version of the statute, personally
22 identifiable information that is automatically generated by the communication, but that does not
23 comprise the substance, purport, or meaning of that communication, is not covered by the Wiretap
24 Act." *In re iPhone Application*, 844 F. Supp. 2d at 1062.
25 Similarly, courts have held that cell-site location information "does not constitute the
26 contents of a communication under § 2510(8)." *Cousineau v. Microsoft Corp.*, 992 F. Supp. 2d 1116,
27 1127 (W.D. Wash. 2012). In *Cousineau*, the plaintiff alleged that Microsoft invaded her privacy and
28 violated the Wiretap Act by collecting smartphone users' approximate latitude and longitude in order

to facilitate targeted advertisements based on their location. *Id.* at 1120–21. Relying on prior decisions involving government surveillance requests, the *Cousineau* 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 copied automatically generated geolocation and anonymized Lyft ID record information, not the "substance, purport, or meaning" of any communication. For that reason as well, the Wiretap Act claim fails.

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

The location data transmitted by smartphone does not constitute an "electronic communication" for purposes of the Wiretap Act. The Act 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 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.").[8] Here, Plaintiff is essentially alleging that Uber used Lyft drivers' smartphones as tracking devices, and so his Wiretap Act claim fails.

The specific exclusion of "tracking devices" from Wiretap Act coverage undermines Plaintiffs' suggestion, citing *United States v. Jones*, that *any* sort of "tracking" or use of an

---

[8] Reinforcing the conclusion that the Wiretap Act does not cover smartphone geolocation data is the fact that Congress considered but did not pass legislation that would have changed this, closing what some members view as a technological "loophole." S.1223, 112th Cong. (2011); Location Privacy Protection Act of 2012, *available at* https://www.congress.gov/bill/112th-congress/senate-bill/1223. Because that bill — and others like it — failed, the broad definition of tracking devices passed in 1986 remains in place.

individual's GPS location data is necessarily insidious or threatening. Compl. ¶ 7 (citing *Jones*, 565 U.S. 400 (2012) (Sotomayor, J., concurring)). *Jones* has nothing to do with this case. First, as Plaintiff's own allegation shows, *Jones* involved the collection and use of location data by the *government*, implicating Fourth Amendment concerns not present here. 565 U.S. at 413 (cautioning that government's "unfettered" use of GPS tracking "may alter the relationship between citizen and government in a way that is inimical to democratic society") (citation omitted); *id.* at 416 ("Awareness that the *Government* may be watching chills associational and expressive freedoms") (emphasis added). Second, the *Jones* majority did not reach the question whether the government's use of a GPS tracking device attached to the defendant's vehicle was an invasion of privacy; its holding rested on the conclusion that the government's installation of the device amounted to a warrantless physical search. *Id.* at 404–05. In any event, Plaintiff's suggestion is vastly overblown in a case alleging only that Uber collected and used data that he and others knew Lyft would broadcast for the very purpose of making it easier to locate drivers. Regardless, for the reasons shown above, Plaintiff's Wiretap Act claim fails.

II. Plaintiff's CIPA claim fails for similar reasons.

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). Here, Plaintiff's CIPA claim[9] fails for at least two reasons similar to those discussed above: (i) he does not allege Uber "eavesdropped" on any "confidential communication," and (ii) Plaintiff expressly consented to allow his smartphone to be used to track his location. Again, Plaintiff has not alleged an invasion of privacy.

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

Section 632 punishes only one who:

[9] Plaintiff alleges only that Uber violated CIPA section 632 and 637.7, and so 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).

> 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). As noted above, Plaintiff does not contend Uber "secretly listened to" or recorded *any* of his conversations or communications. He contends only that Uber collected location data from broadcasts made by Lyft based on data that Plaintiff voluntarily sent to Lyft and agreed to let Lyft disseminate. *See* Compl. ¶ 49 at p. 9:25–10:17. In other words, Plaintiff alleges Uber copied Lyft ID numbers and location information from Lyft broadcasts, not from Lyft drivers like himself.

Moreover, Plaintiff's 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 their geolocation data while driving for Lyft.

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. Plaintiff specifically consented to this. *See* Lyft Terms of Service ("When you open Lyft on your mobile device, we receive your location."). In common terms, Lyft uses a digital megaphone to commercially advertise location and driver information in hopes of telling as many potential Lyft

riders as possible about the driver's availability. There is nothing "confidential" about 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 providing his location data to Lyft.

Similarly, Plaintiff's section 637.7 claim fails because he not only understood, but expressly agreed, that his smartphone would be used to track him and that this information would be publicly broadcast. It is true that, as Plaintiff alleges, section 637.7 prohibits the "use [of] an electronic tracking device to determine the location or movement of a person." Cal. Penal Code § 637.7(a). An "electronic tracking device" is defined as any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals." *Id.* § 637.7(d). But there can be no violation of section 637.7 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(b). Again, Plaintiff expressly consented to the use of his cellphone as a "tracking device" when he signed up to be a Lyft driver. He agreed not only to let Lyft track his movements while he was working, but also to broadcast that information as widely as possible. In fact, he was *counting* on Lyft to do so in order to make money. Plaintiff's consent dooms his CIPA section 637.7 claim.

III. Plaintiff's constitutional privacy claim fails.

Plaintiff's claim under the California Constitution is even more tenuous. That claim requires him to adequately 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. Here, Plaintiff has not adequately alleged facts supporting any of these requirements.

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; *see 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 the information would be shared); *vacated on other grounds*, 517 F. App'x 581 (9th Cir. 2013).

Second, Plaintiff has not pleaded the existence of a "legally protected privacy interest." The type of interest protected by the state 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).

And even in the context of something as sensitive as private medical information, courts have held 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 that the number was accompanied

by any 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 driver. Compl. at p. 10:6–10. *Lyft* could presumably do that, of course, but Plaintiff alleges only that Uber was interested in the drivers' locations, and then only while they were driving for Lyft.[10] For this reason, too, Plaintiff does not allege facts showing an intrusion on any legally protected privacy interest.

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 his fourth 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* Compl. ¶ 89 (quoting *Hill*); *Iqbal*, 556 U.S. at 678 (reiterating that allegations merely reciting the elements of a cause of action "will not do"). Courts have held that 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)).

---

[10] This "surveillance" is no more diabolical than writing down the tail number of an aircraft and using the internet to track its location, something anyone can do. *See, e.g.,* FlightAware, https://flightaware.com/. FlightAware users can also see each plane's unique tail number identifier on the site and use that number to track future flights. But this would hardly infringe on a legally protected privacy interest of the pilot, or anyone else on board, for that matter.

Plaintiff's allegation that Uber might have been able to determine his location, or rather the location of an anonymous Lyft driver bearing a particular Lyft ID number, pales by comparison.

IV. 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. Compl. ¶¶ 76–85. These claims fail, first, because as discussed above, there is nothing "unlawful" or "unfair" as to Uber's alleged collection and analysis of information publicly broadcast by Lyft. But even if that were not true, the UCL claim would still fail because Plaintiff has not adequately alleged that Uber caused him any injury, much less the loss of money or property required by the UCL. Beyond that, Plaintiff has not alleged facts justifying any sort of equitable remedy, including under the UCL.

A. Plaintiff lacks standing to pursue his UCL claim.

A private party has standing to bring a UCL action only if the party has (1) suffered "injury in fact" **and** (2) 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); *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 the burden to establish standing). Plaintiff cannot establish either of these.

1. Plaintiff has not alleged injury-in-fact.

First, Plaintiff has not alleged that he — or *any* Lyft driver — was injured by Uber's alleged conduct. Plaintiff exclusively used the Lyft app to connect with Lyft riders. Compl. ¶¶ 16–18. He claims Uber used the information it allegedly collected to steer some rides away from *Uber-only* drivers to drivers who used both platforms. *Id.* ¶ 58. But he makes no effort to explain how this would have harmed anyone who, like him (and all putative class members), drove only for Lyft.

Plaintiff suggests only that, in the long run, Lyft-only drivers might ultimately have been harmed if *Lyft* itself had suffered from Uber's alleged program. *Id.* ¶ 59. But again, Plaintiff does not explain this. If the supply of Lyft drivers actually had been reduced (something Plaintiff does not allege), those who remained might have benefitted. Even if Lyft shuttered its business completely, it is not clear that individual, Lyft-only drivers would have suffered any injury, since they all would have been free to drive for other ridesharing-request services like Uber. Indeed, these drivers might

1 have been better off in that situation as well. To the extent Plaintiff suggests *consumers* might not
2 have been better off (*see* Compl. ¶ 58 (speculating Lyft riders might have had longer wait times)), he
3 alleges no facts to support that suggestion, and in any event Plaintiff brings his claim as a driver, not
4 a rider. Compl. ¶¶ 16–17.

5 But all this is pure speculation. Plaintiff alleges no facts whatsoever showing that he (or
6 anyone else) has actually suffered any injury in fact as a result of Uber's alleged conduct. He only
7 theorizes that an injury *might* have been suffered under some set of facts. This does not state a claim.
8 *See Birdsong v. Apple, Inc.*, 590 F.3d 955, 959–62 (9th Cir. 2009) (holding plaintiffs who alleged
9 consumers *might* suffer hearing loss from listening to iPods did not establish Article III or UCL
10 standing).

11 **2. Plaintiff does not allege any loss of money or property.**

12 Even assuming Plaintiff could establish some nominal "injury" for Article III purposes, his
13 UCL claim would still fail because he does not allege Uber's conduct actually caused him to lose
14 money or property, as the statute requires. Cal. Bus. & Prof. Code § 17204.

15 Plaintiff alleges only that Uber may have collected location information. But the Ninth
16 Circuit and California district courts have consistently rejected UCL claims based on purported
17 losses of personal information, even where plaintiffs have claimed that information had monetary
18 value to them. *See, e.g.*, *In re Facebook Privacy Litig.*, No. 12-15619, 2014 WL 1815489, at *1 (9th
19 Cir. May 8, 2014) (holding that alleging "lost sales value" of disseminated personal information was
20 not enough for UCL standing); *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal.
21 2014) (finding plaintiff's alleged "property interest" in lost personal information and message
22 content insufficient and noting that "courts have consistently rejected such a broad interpretation of
23 'money' or 'property'" in UCL cases); *see also Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1056
24 n.22 (N.D. Cal. May 14, 2014); *In re iPhone Application Litig.*, No. 11–MD–02250, 2011 WL
25 4403963, at *14 (N.D. Cal. Sept. 20, 2011); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 862
26 (N.D. Cal. 2011). Here, Plaintiff merely recites the phrase "money or property" in his UCL cause of
27 action. Compl. ¶ 84. He alleges no facts supporting that assertion, and so his UCL claim fails for that
28 reason alone.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

The UCL authorizes only equitable relief, not legal damages. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1150 (2003). It is hornbook law "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); *see also Dept. of Fish & Game v. Anderson-Cottonwood Irrigation Dist.*, 8 Cal. App. 4th 1554, 1564 (1992) (calling these requirements "fundamental").

Plaintiff's other three claims seek legal damages, including both actual and statutory damages, along with treble and punitive damages (Compl. ¶¶ 68, 73, 92, 93), all of which would more than compensate Plaintiff for any alleged harm. Plaintiff pleads no facts to suggest that these remedies would be inadequate here. Where this is the case, courts in this district, including this one, dismiss UCL and other equitable claims at the pleading stage. *See Moss v. Infinity Ins. Co.*, 197 F. Supp. 3d 1191, 1203 (N.D. Cal. 2016) (Corley, J.); *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); *Zapata Fonseca v. Goya Foods Inc.*, No. 16-cv-02559, 2016 WL 4698942, at *7 (N.D. Cal. Sept. 8, 2016); *Duttweiler v. Triumph Motorcycles (Am.) Ltd.*, No. 14-cv-04809, 2015 WL 4941780, at *8 (N.D. Cal. Aug. 19, 2015); *Philips v. Ford Motor Co.*, No. 14-cv-02989, 2015 WL 4111448, at *16 (N.D. Cal. July 7, 2015).

Plaintiff concedes he has no basis for injunctive relief. To state such a claim, Plaintiff would have to plead facts showing a sufficient likelihood that he might be injured again in a similar way, and that he faces a real threat of irreparable injury. *Luman v. Theisman*, 647 F. App'x 804, 807 (9th Cir. Apr. 8, 2016); *Perez v. Nidek Co.*, 711 F.3d 1109, 1114 (9th Cir. 2013). But Plaintiff admits he stopped driving for Lyft in late 2014, and alleges that Uber ceased collecting the location data in early 2016. Compl. ¶¶ 5, 49, 53. According to his own allegations, therefore, neither he nor anyone else is at any risk of being harmed (immediately or otherwise) by the conduct he alleges. Plaintiff has therefore alleged neither a basis nor a need for injunctive relief as to any of his causes of action.

Bentley v. United of Omaha Life Ins. Co., No. CV-15-7870, 2016 WL 7443189, at *7 (C.D. Cal. June 22, 2016).

CONCLUSION

Plaintiff's entire complaint is based on allegations made in a single online article that in turn was based on two anonymous sources. Even if those allegations were true, they would not describe anything other than the collection and use of location information that Plaintiff knew was being broadcast by Lyft, something to which he had expressly consented. For all of the foregoing reasons, this Court should dismiss Plaintiff's complaint.

Dated: June 19, 2017

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

By: /s/ *John K. Sherk*
PATRICK L. OOT
JOHN K. SHERK
ANNIE Y.S. CHUANG

Attorneys for Defendants