UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MICHAEL GONZALES,
Plaintiff,
v.
UBER TECHNOLOGIES, INC., et al.,
Defendants.

Case No.17-cv-02264-JSC

ORDER RE: DEFENDANTS' MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT

Re: Dkt. No. 59

Plaintiff Michael Gonzales brings this action on his own behalf and as a putative class action for Lyft drivers whose electronic communications and whereabouts were allegedly intercepted, accessed, monitored, and transmitted by Defendants Uber Technologies, Inc., Uber USA LLC, and Raiser-CA (collectively, "Uber"). Now pending before the Court is Defendants' motion to dismiss Plaintiff's Second Amended Complaint ("SAC").[1] (Dkt. No. 59.)[2] After careful consideration of the parties' briefing, and having had the benefit of oral argument on September 20, 2018, the Court GRANTS Defendants' motion to dismiss with prejudice as to Plaintiff's federal under the Stored Communications Act. The Court declines to exercise supplemental jurisdiction over the remaining state law claims, and dismisses those claims without prejudice.

BACKGROUND

I. Complaint Allegations

The factual background in this case is set out in detail in the Court's order granting Uber's motion to dismiss the First Amended Complaint. (*See* Dkt. No. 51.) The gravamen of the

[1] Both parties have consented to the jurisdiction of a magistrate judge pursuant to 28 U.S.C. § 636(c). (Dkt. Nos. 10 & 15.)

[2] Record citations are to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of the documents.

complaint is that Uber created fake Lyft rider accounts and used spyware to send fake ride requests from those accounts, collect the geolocation data of Lyft drivers that Lyft sent in response to the ride requests, and thereafter monitor the locations of Lyft drivers. Uber then used the data it collected to gain a competitive advantage in several major metropolitan areas.

II. Procedural History

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

Plaintiff then filed a First Amended Complaint ("FAC") seeking the same relief under the same causes of action with two additional claims: (1) the Federal Stored Communications Act (the "Stored Communications Act") and (2) the California Computer Data Access and Fraud Act ("CDAFA"). (Dkt. No. 34.) Uber then moved to dismiss all claims. (Dkt. No. 38.) The Court granted Uber's motion with leave to amend as to Plaintiff's Wiretap Act, Stored Communications Act, CDAFA, and invasion of privacy claims; granted dismissal of Plaintiff's Invasion of Privacy Act claim without leave to amend; and denied Uber's motion as to the UCL claim. (Dkt. No. 51.) Uber filed a motion for reconsideration as to the UCL claim, (Dkt. No. 52), which the Court granted, (Dkt. No. 57).

Plaintiff next filed the SAC, bringing Stored Communications Act, CDAFA, UCL, and invasion of privacy claims. (Dkt. No. 58.) Uber moves to dismiss all claims. (Dkt. No. 59.)

DISCUSSION

I. Federal Claim

A. Stored Communications Act

Plaintiff's complaint alleges that Uber accessed Lyft's computer servers by "falsely pos[ing] as a Lyft rider" and sending fake ride requests to obtain the personal information of Lyft drivers that Lyft stored in its servers "for the purpose of backup protection." (Dkt. No. 58 at ¶¶

130-36.)

"The Stored Communications Act provides a cause of action against anyone who 'intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.'" *Theofel v. Farley-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) (quoting 18 U.S.C. §§ 2701(a)(1), 2707(a)). The Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purpose of backup protection of such communication." 18 U.S.C. § 2510(17)(A),(B). As relevant here, "subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission." *Theofel*, 359 F.3d at 1076.

The Court previously dismissed this claim because the allegations failed to show that the data at issue was stored temporarily, and thus, fell within subsection (A), or that the data was stored for "backup protection" under subsection (B). The dismissal was with leave to amend to allege facts that plausibly suggest that Uber accessed communications in "electronic storage" as defined under the Stored Communications Act. In the SAC, Plaintiffs attempt to plead that the data falls within subsection (B): stored for "backup protection."

Uber seeks to dismiss Plaintiff's claim on the grounds that Plaintiff again fails to plausibly allege that the accessed data was stored for "backup protection." (Dkt. No. 59 at 13.) The Court agrees.

A. Backup Protection

Plaintiff alleges that Lyft's and Uber's computer systems "store the location of every driver, whether on duty or off duty, every few seconds," (Dkt. No. 58 at ¶¶ 110-11), and neither Uber nor Lyft "ever delete the geolocation data they collect from drivers, (*id.* at ¶ 113). Lyft collects and stores the information "for backup purposes" and retrieves it "as need to respond to government inquiries, insurance evaluations, or analyses of individual drivers." (*Id.* at ¶ 133.)

Plaintiff's allegations do not give rise to a plausible inference that the data is stored for "backup protection" for two reasons: (1) the allegations show that Lyft sent real-time and not historical geolocation data to the fake Lyft rider accounts created by Uber; and (2) there is no allegation that Uber accessed a separate copy of historical geolocation data that exists elsewhere or ever existed.

1. Uber Obtained Real-time Geolocation Data From Lyft

In explaining the data that Uber obtained from Lyft, the SAC alleges that Uber used its spyware:

> to send numerous forged [ride] requests to Lyft's Computer Communication Servers which caused [Lyft] to automatically respond initially with Driver Information it had previously stored in databases, and as [the spyware] requests continued, redirect/forward Driver Information transmitted directly by Lyft Driver Apps that was intended for actual fare-paying riders nearby. Thus, the Hell spyware allowed Defendants to access Driver Information being transmitted through Lyft's Computer Communications Servers in real time (save for the inherent lag in any computer network) as well as access the Driver Information stored in databases on Lyft's Computer Communications Servers.

(*Id.* at ¶ 114.) Plaintiff's allegation that Lyft would "initially" respond to a fake ride request with "previously stored" geolocation data is not plausible given that Lyft allegedly updates "the location of every Lyft driver, whether on duty or off duty, every few seconds," (*see id.* at ¶ 110). It is, however, plausible to infer from Plaintiff's allegations that Lyft would respond to a ride request with geolocation data that was at most a "few seconds" old and then "redirect/forward" in "real time" driver geolocation data to the fake rider. Indeed, Plaintiff further alleges that:

> [a]s designed, the Hell spyware enabled Defendants to surreptitiously access, monitor, use, and/or transmit personal information as well as electronic communications and whereabouts *in real time*, other than the nominal delay attributable to network speed limitations when moving communications across Lyft's servers.

(*Id.* at ¶ 119) (emphasis added.) And although Plaintiff alleges that Uber also accessed "Driver Information [that Lyft] had previously stored in databases" through its use of fake ride requests, (*see id.* at ¶ 114), that allegation is rendered implausible by a later allegation stating, in pertinent part, that"[a]ctual Lyft riders would have no way of keeping such records [of historical geolocation data], especially because the unique identifiers belonging to Lyft drivers [are] not displayed on the visual display available to riders searching for a driver," (*see id.* at ¶ 118). In other words, a fake ride request would not prompt a response from Lyft showing where a driver *had been* located (i.e., historical or "stored" geolocation data), but instead, where a driver was *currently* located. Obtaining the most recent version of data that is continuously updated every few seconds and thereafter receiving updates in real time can hardly be described as obtaining data that is stored "for the purpose of backup protection." Since the SAC does not plausibly allege that Uber accessed data stored "for the purpose of backup protection," the Stored Communications Act fails.

2. Uber Did Not Access a Copy Stored For Backup Protection

Even assuming that the SAC plausibly alleged that Uber accessed historical geolocation data in addition to the real-time data transmitted to Lyft riders, the SAC does not plausibly allege that the historical geolocation data was stored "for the purpose of backup protection." *See* 18 U.S.C. § 2510(17)(B). To constitute storage "for the purpose of backup protection," there must be another copy of the data to "backup." Plaintiff does not allege that Uber accessed a separate copy of historical geolocation data that exists outside of Lyft's servers; instead, Plaintiff alleges only that Lyft collects and stores the geolocation data of drivers "every few seconds" and stores the information for business purposes unrelated to backup protection of an original copy. That is insufficient. *See Theofel*, 359 F.3d at 1076 ("[T]he mere fact that a copy could serve as a backup does not mean that it is stored for that purpose.").

Plaintiff's opposition to Uber's motion to dismiss insists that "Plaintiff plausibly alleges that the data that Plaintiff provides to Lyft are immediately sent to Lyft riders, therefore there are at least two copies of the data." (Dkt. No. 60 at 16.) That argument is refuted by the SAC. The SAC alleges that "[w]hen logged in to the Lyft Driver App, Plaintiff and the Class consented to share their location, unique identifier, and work availability status, only with Lyft and actual Lyft riders." (Dkt. No. 58 at ¶ 117.) The SAC further alleges, however:

> **Lyft was the *only* entity that Plaintiff and the Class allowed to maintain a historical record of their geolocation data. Actual Lyft riders would have no way of keeping such records,** especially because the unique identifiers belonging to Lyft drivers is not displayed on the visual display available to riders searching for a

> driver. Rather, riders only see an icon of a car imposed on a map.

(*Id.* at ¶ 118) (emphasis added.) Thus, the historical geolocation data maintained by Lyft is not a "copy" of data sent to Lyft riders but is instead the *only* record of that data that ever exists. In other words, Lyft does not maintain a "back up" copy of the data that it sends to Lyft riders because there is no copy.

Plaintiff insists that the Ninth Circuit's "broad view on what constitutes 'electronic storage' for backup purposes" set forth in *Theofel* supports his claim. (Dkt. No. 60 at 16.) Not so. As explained by the *Theofel* court:

> An obvious purpose for storing a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer. The ISP copy of the message functions as a "backup" for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.

Theofel, 359 F.3d at 1075. Here, there is no allegation that Lyft drivers or riders ever received the same data allegedly maintained by Lyft for "back up protection." Further, where the "underlying message" being backed up is merely temporary, *Theofel* expressly holds that subsection (B) does not apply:

> [T]he lifespan of a backup is necessarily tied to that of the underlying message. Where the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as "backing up" those messages.

Id. at 1076. Thus, even if Lyft riders received a copy of the same historical geolocation data maintained by Lyft, or if Lyft drivers retained a copy of the data they send to Lyft through the Lyft App, Plaintiff would need to allege facts demonstrating that those copies were not temporary. Plaintiff fails to do so; instead, the SAC alleges that only one record of Plaintiff's geolocation data ever existed and that record was maintained by Lyft alone.

At oral argument on September 20, 2018, Plaintiff argued that subsection (B) of the Stored Communications Act covers data stored by a corporation that is simultaneously held by different departments within the corporation (i.e., if data is located on a computer in the engineering department and also located on a computer in the legal department, then such storage constitutes storage "for the purpose of backup protection" under the Act). Plaintiff cited *Theofel* in support of this proposition, however, nothing in the *Theofel* court's holding suggests such an all-encompassing reading of the scope of "back up protection" under subsection (B). By Plaintiff's reading, *all* data stored by a corporation in more than one location would fall under the Stored Communications Act, regardless of the *purpose* of its storage. Plaintiff's view is clearly refuted by the plain text of subsection (B), which covers only storage "for the purpose of backup protection." 18 U.S.C. § 2510(17)(B) (emphasis added).

Accordingly, the Court grants Uber's motion to dismiss Plaintiff's Stored Communications Act claim with prejudice. Leave to amend would be futile given the allegations to date regarding Lyft's storage of historical geolocation data and the real-time data allegedly obtained by Uber.

II. State Claims

The SAC asserts that the Court has supplemental jurisdiction over Plaintiff's state law claims based on Plaintiff's Stored Communications Act claim, pursuant to 28 U.S.C. § 1367. (Dkt. No. 58 at ¶ 19.) Upon dismissal of the Stored Communications Act claim—the lone federal claim—the Court declines to exercise supplemental jurisdiction over the remaining state law claims, which were all brought on behalf of the California subclass. *See United Mine Workers v. Gibbs*, 383 U.S. 715, 726 (1966) ("Certainly, if the federal claims are dismissed before trial, even though not insubstantial in a jurisdictional sense, the state claims should be dismissed as well.").

CONCLUSION

For the reasons set forth above, the Court GRANTS Uber's motion to dismiss the Stored Communications Act claim with prejudice; amendment as to that claim would be futile. The Court declines to exercise supplemental jurisdiction over the state law claims, and dismisses those claims without prejudice.

IT IS SO ORDERED.

Dated: September 26, 2018

Jacqueline Scott Corley

JACQUELINE SCOTT CORLEY
United States Magistrate Judge