

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

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

KATHERINE SCOTT, et al.,
Plaintiffs,
v.
AT&T INC., et al.,
Defendants.

Case No. [19-cv-04063-SK](#)

**ORDER REGARDING
SUPPLEMENTAL EVIDENCE**

In their Complaint, Plaintiffs allege that AT&T Services, Incorporated and AT&T Mobility, LLC (collectively “AT&T”) has improperly provided its customers’ real-time location data to third parties without the customers’ consent. (Dkt. No. 1 (Compl.), ¶¶ 1, 4, 42.) Plaintiffs allege that AT&T sold its customers’ real-time location data to a company called Securus Technologies, Inc. through third party aggregators. (*Id.*, ¶¶ 42-43.) Securus then sold AT&T’s customers’ location data to thousands of other third parties. (*Id.*, ¶ 44.) In May 2018, Securus’ server was breached by a hacker who reported that it was relatively simple to obtain the location information for AT&T’s customers. (Dkt. No. 1, ¶¶ 52-53.) Also, in May 2018, a researcher identified a security flaw in another aggregator’s online demonstration, allowing the public to obtain real-time location information for AT&T customers. (*Id.*, ¶ 54.)

AT&T also provided its customers’ real-time location data to another aggregator, who then sold the data to a company called Microbilt, which then sold the location data to many others. (*Id.*, ¶¶ 65-66.) A newspaper reporter was able to find the real-time location of a phone by buying location data from Microbilt through a bounty hunter. (*Id.*, ¶ 69)

In June 2018, AT&T stated that “[it would] be ending [its] work with aggregators for these services as soon as practical in a way that preserves important, potential lifesaving services like emergency roadside assistance.” (*Id.*, ¶ 58.)

United States District Court
Northern District of California

1 AT&T admitted that it did not obtain direct consent from its customers to release their
2 location data. Instead, AT&T maintained that the companies selling its customers' location data
3 were responsible for obtaining consent. (*Id.*, ¶ 127.) However, the aggregators' customers failed
4 to verify consent before releasing the location data. (*Id.*, ¶¶ 129-133, 141, 142.)

5 As Plaintiffs summarize their allegations:

6 Plaintiffs' allege that (i) by continuing to disclose customer location
7 data without adequate notice and consent—including by using a
8 legally deficient system that puts all AT&T customers at risk of
9 breach—AT&T continues to violate the FCA, and (ii) by misleading
10 Plaintiffs and the public about its sales, use, and safeguarding of
11 location data, AT&T is violating the UCL and CLRA. Compl. ¶¶
12 176-218, 281-83, 233-65. They seek injunctive relief to enjoin
13 compliance with the FCA and its implementing regulations, and to
14 enjoin AT&T from continuing to publicly misrepresent its location
15 data disclosure and security practices. *Id.* ¶¶ 279, 285, 299, 342.

16 (Dkt. No. 131.)

17 AT&T moved to dismiss Plaintiff's request for injunctive relief on the grounds that it
18 stopped providing its customers' location data to aggregators as of March 29, 2019. The Court
19 provided Plaintiffs an opportunity to conduct jurisdictional discovery on this issue.

20 Upon review of the parties' evidence and briefs after the jurisdictional discovery, the Court
21 determined that additional submissions from the parties would be beneficial. The Court noted that
22 AT&T submitted a declaration from Greg Hill in which he unequivocally stated that as of March
23 29, 2019, AT&T stopped providing its customers' geolocation data to data aggregators. (Dkt. No.
24 73-1, ¶ 3.) However, the declaration did not state that AT&T stopped providing that data to any
25 other source. Additionally, the Court noted that AT&T argued, but did not provide supporting
26 evidence to show, that AT&T had only provided its customers' location data to third parties
27 through aggregators. Lastly, the Court noted that AT&T clarified through argument, but not
28 evidence, that after March 29, 2019, it only provided its customers' geolocation data to
governmental agencies and life alert companies with life alert pendants.

In response, AT&T submitted additional declarations attesting that: (1) other than for call
routing and life-critical Internet of Things ("IoT") companies, AT&T stopped providing its
customers' geolocation data to non-governmental third parties on March 29, 2019; (2) AT&T

1 continues to provide geolocation information to four life-critical IoT companies when a customer
2 of the life alert company activates his or her pendant to be located during an emergency; and (3)
3 AT&T continues to use the cell tower location of its mobile customers for call routing functions.
4 (Dkt. No. 127 (Declaration of Greg Hill), ¶¶ 3, 4; Dkt. No. 128 (Declaration of Tad Reynes), ¶¶ 4,
5 5; Dkt. No. 126 (Declaration of Kris Weterrings), ¶ 4.) Weterrings explains that there are limited
6 commercial functions of the call routing. When an AT&T customer uses an abbreviated dialing
7 code, AT&T will disclose the cell tower originating the call to a service provider, which then
8 converts the cell tower location to a county to route the call to an applicable land line. (Dkt. No.
9 126, ¶¶ 5, 6.)

10 Plaintiffs now argue that AT&T's supplemental evidence creates additional questions of
11 fact regarding their request for injunctive relief. With respect to the life alert IoT, Plaintiffs do not
12 allege that any of them are customers of a life alert company. Thus, Plaintiffs do not have
13 standing to challenge a practice of providing geolocation data to such companies. Additionally, if
14 the only purpose is to provide geolocation data in the event of an emergency when a life alert
15 company's customer activates his or her pendant, presumably the customer explicitly chooses to
16 disclose her or his location for that emergency.

17 However, with respect to the call routing functions, it is not clear if or how disclosure of
18 this location data falls under Plaintiffs' allegations and/or how this call routing violates the Federal
19 Communications Act as alleged by Plaintiffs. In the interests of fairness, before the Court grants
20 AT&T's motion to dismiss Plaintiffs' request for injunctive relief, the Court will permit Plaintiffs
21 with a limited opportunity to conduct discovery on this issue.

22 By no later than January 18, 2021, Plaintiffs may take a deposition under Federal Rule of
23 Civil Procedure 30(b)(6) for no more than four hours on AT&T's call routing practices only and
24 on no other subject. By no later than February 1, 2021, Plaintiffs may then file a further brief,
25 with supporting evidence, to explain if and/or how AT&T's call routing practices discloses
26 AT&T's customers' geolocation data in violation of the FCA as alleged in their Complaint.
27 Plaintiffs may provide "rough" copies of the deposition transcript if a formal copy is not available.

28 ///

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

AT&T may file a responsive brief by no later than February 8, 2021.

IT IS SO ORDERED.

Dated: December 7, 2020



SALLIE KIM
United States Magistrate Judge

United States District Court
Northern District of California