Shana Scarlett (State Bar No. 217895)
Benjamin Siegel (State Bar No. 256260)
HAGENS BERMAN SOBOL SHAPIRO LLP
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Tel: (510) 725-3000
shanas@hbsslaw.com
bens@hbsslaw.com

Aaron Mackey (State Bar No. 286647)
Andrew Crocker (State Bar No. 291596)
Adam D. Schwartz (State Bar No. 309491)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
amackey@eff.org
andrew@eff.org
adam@eff.org

Attorneys for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

KATHERINE SCOTT, CAROLYN JEWEL, and GEORGE PONTIS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

AT&T INC.; AT&T SERVICES, INC.; AT&T MOBILITY, LLC; TECHNOCOM CORP.; and ZUMIGO, INC.,

Defendants.

No. 3:19-cv-04063-SK

PLAINTIFFS' RESPONSE TO ORDER REQUIRING FURTHER BRIEFING

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. FACTUAL BACKGROUND 1

III. PROCEDURAL BACKGROUND 3

IV. LEGAL STANDARD 4

V. ARGUMENT 4

A. Dismissing Plaintiffs' injunctive relief claims under Rule 12(b)(1) is improper where the merits of the motion to dismiss and the merits of Plaintiffs' claims are entwined and sufficient discovery has not been conducted. 5

B. The Supplemental Declarations do not establish facts warranting dismissal. 7

1. AT&T's declarations reveal a previously undisclosed, separate system for the sale of customer geolocation data for commercial call routing. 7

2. AT&T's disclosure of location data to IoT companies creates the same risks of breach and unauthorized disclosure as sales to aggregators. 8

3. AT&T's Supplemental Declarations fall short of establishing that AT&T has ceased providing customer location data to all third parties. 10

VI. CONCLUSION 10

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

Augustine v. United States,
704 F.2d 1074 (9th Cir. 1983) 1, 6, 7

Barnum Timber Co. v. EPA,
633 F.3d 894 (9th Cir. 2011) 4

Bell v. Hood,
327 U.S. 678, 66 S. Ct. 773, 90 L. Ed. 939 (1946) 6

Campbell v. Facebook, Inc.,
951 F.3d 1106 (9th Cir. 2020) 1, 7

Hernandez v. Levy Premium Foodservice, LP,
2014 WL 12569361 (C.D. Cal. Mar. 17, 2014) 6

Philips v. Ford Motor Co.,
2016 WL 693283 (N.D. Cal. Feb. 22, 2016) 6

Safe Air for Everyone v. Meyer,
373 F.3d 1035 (9th Cir. 2004) 4, 5

Sun Valley Gas., Inc. v. Ernst Enters.,
711 F.2d 138 (9th Cir. 1983) 6

UMG Recordings, Inc. v. Glob. Eagle Entm't, Inc.,
2015 WL 12752879 (C.D. Cal. July 2, 2015) 5

Villa v. Maricopa County,
865 F.3d 1224 (9th Cir. 2017) 1

Young v. United States,
769 F.3d 1047 (9th Cir. 2014) 6

FEDERAL STATUTES

Federal Communications Act, 47 U.S.C. §151 2

Privacy of Customer Information, 47 U.S.C. § 222 ..... 2, 8

FEDERAL RULES

Rule 12(b)(1) 1, 4, 5

I. INTRODUCTION

AT&T's attempt to dismiss Plaintiffs' injunctive relief claims by making untested factual assertions—all while resisting fulsome discovery on those same facts—is procedurally improper. As AT&T has stressed, its motion to dismiss relies on a single fact: Whether it stopped providing location data to aggregators. With its new declarations, AT&T significantly expands the universe of disputed facts by making new assertions about the nature, extent, and mechanisms of location disclosures to two additional categories of entities, commercial call routing and internet of things ("IoT") companies. AT&T also for the first time reveals that it maintains a *separate* system for disclosing customer location data for call routing purposes, in addition to the system AT&T previously described to Plaintiffs and the Court. In so doing, AT&T has (i) raised additional facts deserving of further discovery, and (ii) intertwined its jurisdictional motion with the merits of Plaintiffs' claims. AT&T thus asks this Court to make fact-finding determinations and legal conclusions on disputed facts over which no discovery has occurred. To do so under Rule 12(b)(1) standards would be improper. *Augustine v. United States*, 704 F.2d 1074, 1077 (9th Cir. 1983).

Nonetheless, AT&T's latest factual submissions confirm that Plaintiffs and all California AT&T customers have standing to seek public injunctive relief under controlling Ninth Circuit law. Plaintiffs have standing where they establish either (a) continuing adverse effects as a result of AT&T's violations of federal privacy law and state consumer protection laws, and/or (b) a sufficient likelihood that they will again be harmed in a similar way. *Villa v. Maricopa County*, 865 F.3d 1224, 1229 (9th Cir. 2017). AT&T's failure to adopt location data disclosure and security protocols that reasonably protect its customers' sensitive data and its ongoing disclosure of location data to third parties—*as confirmed in AT&T's latest declarations*—together with its ongoing failure to correct its misrepresentations about its location data practices confer Plaintiffs with standing to pursue their injunctive relief claims. *Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020).

II. FACTUAL BACKGROUND

Plaintiffs' injunctive relief claims center upon requiring AT&T to comply with federal privacy law—the Federal Communications Act ("FCA") and its implementing regulations—by ensuring it does not sell its customers' location data to third parties without customer notice and

consent and requiring it to protect and safeguard this sensitive data.[1] *See* ECF No. 106-01 (Notice of Apparent Liability for Forfeiture and Admonishment, *In the Matter of AT&T Inc.*, FCC 20-26 (Feb. 28, 2020) ("NAL")) ¶ 52 (AT&T has a duty to "take reasonable steps to safeguard their customers' CPNI and to discover attempts to gain access to their customers' CPNI."[2]); *see also* Compl. ¶¶ 176-225 (detailing notice, knowing consent, and data safeguarding requirements).

Rather than diligently safeguard the data entrusted to it and keep its promise that it won't "sell [customers'] personal information to anyone for any purpose," AT&T has for years profited off the sale of highly sensitive location data. Compl. ¶¶ 241-42. Despite its public promises to safeguard this data, AT&T allowed a robust, uncontrolled market to develop wherein location data was routinely breached. *Id.* ¶¶ 236-40. This market grew out of AT&T's flawed mechanisms for obtaining and verifying the consent required under the FCA. AT&T provided third parties with *direct access* to its customers' location data, giving each the ability to access *any AT&T customer's* location data. *Id.* ¶¶ 82, 87-93. The only structural protections that AT&T put in place to protect the data were (i) contractual obligations wherein the third parties agreed to seek customer consent and to implement "information security requirements," and (ii) an illusory "consent verification" system. NAL ¶¶ 53-59. Following a factual investigation, the FCC found that these protections were woefully inadequate. First, "the contractual safeguard alone was insufficient to prevent the misuse of the customer location information to which AT&T sold access." *Id.* ¶ 54. Likewise, AT&T took no steps to determine whether the "information security requirements" were "actually being followed." *Id.* ¶ 58. And AT&T's consent verification system did not actually *verify consent*, instead relying "almost entirely on the unverified assertions" of third parties. NAL ¶ 56. The FCC found that this system "clearly failed in practice" and allowed ongoing breaches to "continue *for at least four years* without AT&T's knowledge." *Id.* (emphasis in original). AT&T's system provided "almost no other

[1] The FCA also establishes AT&T's ongoing duty to "discover attempts to gain access to [its] customers' CPNI," NAL ¶ 52, and inform customers if their CPNI is accessed without permission, Compl. ¶ 214. Plaintiffs' injunctive relief would also require AT&T to comply with these provisions.

[2] CPNI includes "information that relates to the . . . location . . . of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222.

visibility or apparent awareness into how the location data it sold was used or protected." *Id.* ¶ 59. In sum, AT&T failed to implement reasonable safeguards even after repeated breaches "laid bare the fundamental weaknesses of AT&T's safeguards . . ." *Id.* ¶ 60. The FCC concluded that by utilizing this system, AT&T "failed in its obligation under [the FCA] and our rules to have reasonable measures in place to discover and protect against attempts to gain unauthorized access to its customers' CPNI" and proposed a more than $57 million fine against the company. *Id.* ¶¶ 70, 81.

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

III. PROCEDURAL BACKGROUND

On November 27, 2019, AT&T moved to dismiss, asserting that Plaintiffs lack standing to seek public injunctive relief. ECF No. 73. On January 15, 2020, the parties stipulated to, and the Court ordered, jurisdictional discovery. ECF No. 81. After the parties filed a joint brief concerning the proper scope of jurisdictional discovery, the Court held that Plaintiffs could only seek documents targeted to whether "Defendants stop[ped] selling location data or geolocation information to third parties[.]" ECF No. 96 at 2-3 ("Discovery Order"). On July 8, 2020, Plaintiffs served targeted RFPs seeking the identification of all such entities. Siegel Decl., Ex. A. AT&T refused to identify any third parties outside "aggregators and all parties receiving geolocation through aggregators." *Id.*, Ex. B. at 5. AT&T represented that when it ended aggregators' access to its location API system, it effectively ended all location data disclosures, other than those to IoT companies. *Id.*, Ex. C. Plaintiffs asked AT&T to confirm this representation and stressed that the Complaint clearly concerns "AT&T's violations of federal and state law by selling or providing access to customers' geolocation information—to *any third party*—without the required notice and consent or valid legal authority." *Id.* at 3. In response, AT&T provided a new basis for its refusal to identify all relevant third parties, arguing

that—based on the term "selling" in the Discovery Order—it would *only* identify entities "to which AT&T could have been deemed to have 'sold' geolocation information" but reiterated that it had identified the only disclosure system. *Id.*, Ex. D. It wasn't until September—9 months into jurisdictional discovery—that AT&T disclosed that it also gave unidentified "third party call routers" and AT&T affiliates access to customer location data, but maintained that such disclosures were not "the subject of [this] lawsuit" and refused to provide discovery. *Id.*

During the hearing on AT&T's motion, AT&T counsel made factual representations "not contained in any declaration or admissible documents," concerning its ongoing location disclosures. ECF No. 122 at 1. The Court ordered AT&T to provide further information concerning "the status of [AT&T] customers' geolocation data." *Id.* at 2. In response, AT&T filed three declarations on November 29, 2020. ECF Nos. 127 ("Second Hill Decl."), 128 ("Renyes Decl."), 129 ("Weterrings Decl."), together "Supplemental Declarations." These declarations provide new, untested facts, about AT&T's location disclosure practices and the potential risks associated with them.

IV. LEGAL STANDARD

A defendant moving to dismiss under Federal Rule of Civil Procedure 12(b)(1) may make a facial or factual jurisdictional attack. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). A factual attack "disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction." *Id*. While a response to a factual attack must meet evidence with evidence (*id*.), a response to a facial attack may rest on specific plausible allegations (*Barnum Timber Co. v. EPA*, 633 F.3d 894, 899 (9th Cir. 2011)). "In resolving a factual attack on jurisdiction," the Court "may review evidence beyond the complaint without converting the motion to dismiss into a motion for summary judgment." *Safe Air*, 373 F.3d at 1039. However, "a jurisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Id.* (internal quotation and alteration omitted).

V. ARGUMENT

In challenging Plaintiffs' standing to seek injunctive relief, AT&T has repeatedly made limited factual statements concerning its ongoing data disclosure and security practices, all while

refusing to provide discovery on these same topics. In its latest attempt, AT&T submits three declarations, each of which presents new, untested factual assertions concerning matters over which Plaintiffs were denied discovery, placing Plaintiffs in the inequitable position of not being able to gather evidence to meet their burden. *UMG Recordings, Inc. v. Glob. Eagle Entm't, Inc*., 2015 WL 12752879, at *11 (C.D. Cal. July 2, 2015) ("In the Ninth Circuit, jurisdictional discovery 'should ordinarily be granted where pertinent facts bearing on the question of jurisdiction are controverted or where a more satisfactory showing of the facts is necessary.'" (quoting *Butcher's Union Local No. 498 v. SDC Investment, Inc*., 788 F.2d 535, 540 (9th Cir. 1986))).

Because the declarations introduce facts intertwined with the merits of Plaintiffs' case, dismissal under Fed. R. Civ. P. 12 is improper. *Safe Air*, 373 F.3d at 1039. Nonetheless, the Supplemental Declarations fail to establish that Plaintiffs lack standing to seek injunctive relief; instead, they highlight that AT&T continues to collect and disclose location data, utilize insecure systems for its disclosure, and misrepresent its practices to the public.

A. Dismissing Plaintiffs' injunctive relief claims under Rule 12(b)(1) is improper where the merits of the motion to dismiss and the merits of Plaintiffs' claims are intertwined and sufficient discovery has not been conducted.

Despite maintaining throughout discovery that the "single fact" upon which its Rule 12 motion relied was the cessation of sales to and through aggregators—and using that position to deny discovery concerning the extent, context, and mechanisms of all third party disclosures—AT&T now submits untested facts concerning a much broader range of activity, including select details about how it call routing and IoT location disclosures work. *See* Reynes Decl. ¶¶ 4-6; Weterrings Decl. ¶¶ 4-7; *see also* ECF No. 94 at 5 (AT&T arguing that its "Motion to Dismiss is based on a single fact: AT&T stopped providing geolocation information to data aggregators as of March 29, 2019."). By significantly expanding the realm of disputed facts, AT&T has intertwined the merits of its motion to dismiss with the merits of Plaintiffs' FCA claims. The critical questions in Plaintiffs' FCA claim are (i) whether AT&T disclosed or permitted a third party to access to customers' location data without notice and consent, and (ii) whether AT&T failed to reasonably safeguard the location data. AT&T's Supplemental Declarations bear directly on those questions, but they provide only select facts concerning to whom it disclosed data and the circumstances and mechanisms of those disclosures.

AT&T's jurisdictional attack is now "intermeshed" with and "implicate[s] the merits" of Plaintiffs' claims. *Philips v. Ford Motor Co*., 2016 WL 693283, at *15 (N.D. Cal. Feb. 22, 2016). When a jurisdictional challenge "involve[es] factual issues which also go to the merits, the trial court should employ the standard applicable to a motion for summary judgment, as a resolution of the jurisdictional facts is akin to a decision on the merits." *Augustine*, 704 F.2d at 1077 (citing *Thornhill Publishing Co. v. General Telephone Corp*., 594 F.2d 730, 733-34 (9th Cir. 1979); *see also Young v. United States*, 769 F.3d 1047, 1052 (9th Cir. 2014).[3] Accordingly, AT&T "should prevail only if the material jurisdictional facts are not in dispute and [it] is entitled to prevail as a matter of law. Unless that standard is met, the jurisdictional facts must be determined at trial by the trier of fact." *Augustine*, 704 F.2d at 1077 (citing *Thornhill*, 594 F.2d at 733-35). Where there is a "clear conflict as to the central factual issues on the case[,]" dismissal on the "basis of the pleadings and supporting affidavits" is improper. *Id.* at 1079. This is particularly true when Plaintiffs have been denied discovery on those central facts. *See Hernandez v. Levy Premium Foodservice, LP*, 2014 WL 12569361, at *3 (C.D. Cal. Mar. 17, 2014) (collecting cases standing for the proposition that it is improper to rule on summary judgment before discovery "pertinent to the motion" has taken place).

To hold that Plaintiffs do not establish ongoing injury or a sufficient likelihood of future injury, the Court would have to make factual findings that AT&T no longer permits any access to customers' location data without consent, reasonably protects location data, and has corrected all of its misleading public representations about its location data practices. *See* ECF No. 105-2 (Pltfs.' Opp.'n to AT&T's Mot. to Dismiss). By definition, this requires reaching the merits of Plaintiffs' claims, as it will determine whether AT&T is in compliance with the FCA, UCL, and CLRA. But the facts concerning these merits questions are disputed, as detailed herein. Therefore, "the jurisdictional

[3] Additionally, Plaintiffs assert federal question jurisdiction under the FCA. Compl. ¶ 31. The Ninth Circuit has held that the jurisdiction inquiry and the merits are intertwined where "a statute provides the basis for both the subject matter jurisdiction of the federal court and the plaintiff's substantive claim for relief." *Sun Valley Gas., Inc. v. Ernst Enters.*, 711 F.2d 138, 139 (9th Cir. 1983); *see also Bell v. Hood*, 327 U.S. 678 (1946); *Thornhill*, 594 F.2d at 734 (in such circumstances, "a motion to dismiss for lack of subject matter jurisdiction . . . is proper only when the allegations of the complaint are frivolous." (quotation omitted)). AT&T has not alleged, let alone established, that any of Plaintiffs' FCA claims are frivolous.

determination should await a determination of the relevant facts on either a motion going to the merits or at trial." *Augustine*, 704 F.2d at 1077. Dismissal would be improper.

B. The Supplemental Declarations do not establish facts warranting dismissal.

Nevertheless, AT&T's Supplemental Declarations fail to rebut the several, independent bases for jurisdictional discovery detailed in Plaintiffs' Opposition, and instead support standing by disclosing wider-ranging use of customer location data. ECF No. 105-2 at 9-19. The newly-submitted evidence confirms that AT&T continues to collect location data, provides that data to myriad third parties, utilizes the same inadequate system to provide such access, and misleads the public about the nature of its location data disclosures and the extent of its security procedures. Under controlling Ninth Circuit law, Plaintiffs have established that their private location data remains at risk—and they continue to overpay for AT&T's service—as a result of AT&T's ongoing practices, and are at a significant risk that AT&T will resume unauthorized location data sales on a larger scale. *See Campbell*, 951 F.3d 1106 (plaintiffs establish continuing and future harms sufficient to confer standing where defendant continues to collect, retain, and use the data at issue). This is sufficient to confer standing. AT&T's attempt to distinguish *Campbell* is unavailing. The Ninth Circuit did not find, as AT&T represents, that the "mere collection" of consumers' data was unlawful; there, as here, it was *use without consent* that constituted the unlawful behavior. *Id.* at 1119 ("Plaintiffs' position that this was being done *without consent* meant that they claimed a violation of the concrete privacy interests that ECPA and CIPA protect . . .") (emphasis added).

1. AT&T's declarations reveal a previously undisclosed, separate system for the sale of customer location data for commercial call routing.

In a declaration submitted by a marketing employee, AT&T for the first time provides details about its sale of location data for call routing—utilizing a previously undisclosed, separate system—a topic on which AT&T refused to provide discovery. AT&T states that it discloses its customers' location data to a "third-party service provider" who, in turn, provides that location to an undisclosed number of third parties for "commercial functions." Weterrings Decl. ¶¶ 4-5. AT&T's assertions that its call routing disclosures are not a "one time look-up" and do not provide "precise latitude and longitude of any AT&T mobile phone customer" are irrelevant. *Id.* ¶¶ 4, 6. This is a clear use of data

protected by the FCA, which prohibits the disclosure, use, or access "information *that relates to the . . . location* . . . of a telecommunications service subscribed to by any customer[.]." 47 U.S.C. § 222 (emphasis added). The Weterrings Declaration establishes that AT&T continues to disclose customers' cell tower location data to a third-party service provider who, in turn, reveals county-level location data to myriad undisclosed additional third parties. Weterrings Decl. ¶¶ 5-6. These disclosures occur without any evidence that AT&T complies with the FCA's notice and consent requirements, the very behavior Plaintiffs seek to enjoin because it violates federal law.

AT&T's declaration discloses for the first time that—despite AT&T's assertions that no separate system exists wherein customer location data is sold to a third party, *see* Siegel Decl., Exs. C & D—the "system….used for call routing is not the same system that was used to provide geolocation to aggregators[.]" Weterrings Decl. ¶ 7. Critically, AT&T provides *no evidence* that AT&T provides notice or obtains consent for these disclosures, as required by the FCA. *See* Compl. 176-225. Additionally, neither the third-party service provider disclosed in the declaration, nor its customers, were ever identified in AT&T's responses to Plaintiffs' RFPs—or the Court's order—seeking the identity of all third parties to whom AT&T provides location data. Indeed, AT&T failed to disclose that its sale of location data for call routing including commercial uses when it first disclosed the service in September 2019. *See* ECF No. 112-1. AT&T's description of the "commercial functions" for which it sells location data is limited, providing only that an AT&T customer's call to a particular company or for a particular service can be "routed to a business in the person's general location." *Id.* ¶ 5. Meanwhile, Plaintiffs have been provided no details about this system and have been denied discovery to understand these commercial disclosures, test the veracity of AT&T's assertions, or confirm that its declarant has the proper foundation for her testimony.[4]

2. AT&T's disclosure of location data to IoT companies creates the same risks of breach and unauthorized disclosure as sales to aggregators.

In the Reynes Declaration, an AT&T sales employee discloses that AT&T sells location data

[4] AT&T provides no facts establishing that a "Lead Marketing Manager" has the requisite foundational knowledge concerning its call routing practices.

to IoT companies and makes new factual claims regarding how those disclosures work.[5] ECF No. 128. In short, AT&T provides SIM cards—akin those in AT&T mobile customers' phones, which provide AT&T with the ability to use network and GPS data to locate the phone (*see* Compl. ¶¶ 77, 110-17)—to these companies for use in pendant devices. Reynes Decl. ¶¶ 405. The IoT companies then "ping" the pendants to determine their location. *Id.* The IoT disclosures use the same system as the aggregators, i.e., AT&T provides direct access to its location API to IoT customers, who can then query location data. *See* Compl. ¶¶ 82, 87-92; ECF Nos. 112-1, 105-6, 105-8; Siegel Decl., Exs. C & D; *c.f.* Weterrings Decl. ¶ 7 (asserting that *call routing* companies do not use the same system as aggregators). The FCC found that this system failed to satisfy the FCA because it provided third parties with access to *all* AT&T customers' location data—i.e., the ability to query the location of *any* SIM card connected to the AT&T network—without adequate safeguards to assure that third parties only obtain the location of customers for whom they have consent. NAL ¶¶ 12, 53-60, 70.

AT&T has provided no details about how—if at all—its arrangement with IoT companies differs from its arrangement with aggregators. The Reynes Declaration raises material questions about AT&T's practices, which bear on the pending motion to dismiss. It provides only select details about how the IoT customer location querying system works and what (if any) protections AT&T has put in place to protect customers' location data—including how and whether it segregates data from IoT SIM cards from mobile phone SIM cards or prevents IoT customers from accessing mobile phone data. Critically, Plaintiffs were denied discovery on these topics. But for the purpose of Plaintiffs' claims, the relevant inquiry is not whether Plaintiffs own IoT pendants but, rather, whether AT&T's ongoing practice of allowing third parties to query network location information continues to put Plaintiffs and other AT&T customers at risk.[6] Plaintiffs' Complaint centers on the manner in which AT&T discloses and fails protects its customers' location data, not on the entities to whom the

[5] AT&T provides no facts establishing that a "Senior Application Sales Director IoT" has the requisite foundational knowledge on these issues.

[6] This includes a risk of a data breach. By providing third parties with direct access to its API, AT&T allowed a third party to create a web interface that *for years* allowed unauthorized entities to breach *AT&T's system*. Compl. ¶¶ 54-56. By providing any third party with direct access to customer location data, this risk remains for all AT&T customers.

data is sold. Throughout the Complaint, Plaintiffs detail how AT&T's system of passing-down responsibility for obtaining consent, combined with its policy of allowing direct access to location data customers, allows for the rampant abuse of customer location data. AT&T has failed to present facts rebutting Plaintiffs' allegations that it continues to use an insecure system that provides direct access to all AT&T customers' data without adequate measures in place. Accordingly, AT&T does not make a factual attack as to these issues, and Plaintiffs' allegations must be taken as true for purposes of this motion. *Dahlia*, 735 F.3d at 1066.

3. AT&T's Supplemental Declarations fall short of establishing that AT&T has ceased providing customer location data to all third parties.

AT&T's newly-filed declarations make plain that it continues to disclose customer location data without the notice and consent required by law. In the Second Hill Declaration, AT&T's Assistance President of Cybersecurity asserts that, other than the sale of location data for call routing, he is "aware of no other non-governmental third party (excluding AT&T's vendors for AT&T's internal uses) that is provided the ability to access cellular network geolocation data of any AT&T mobile phone customer." Second Hill Decl. ¶ 4. Similarly, he asserts that while "[t]here are other enterprise (business) uses of location … [he is] *not aware* of any such uses involving an AT&T consumer's mobile phone cellular location data." *Id*. ¶ 7 (emphasis added). One employee's statements of what he is "aware of" falls short of a reliable and unqualified representation that AT&T has stopped providing customer cellular location data to all non-governmental, non-call-routing third parties. This declaration is particularly wanting here, where Plaintiffs have been denied the opportunity to probe the bases for these representations, including by inquiring whether (i) Greg Hill is in a position to be aware of all uses of customer location data, and (ii) what investigation informs his awareness of the extent of AT&T's location data uses.

VI. CONCLUSION

For the reasons stated herein, Plaintiffs respectfully submit that AT&T's motion to dismiss should be denied in its entirety.

DATED: December 4, 2020

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By */s/ Shana E. Scarlett*
Shana E. Scarlett (State Bar No. 217895)
Benjamin Siegel (State Bar No. 256260)
715 Hearst Avenue, Suite 202
Berkeley, CA 94710
Tel: (510) 725-3000
Fax: (510) 725-3001
shanas@hbsslaw.com
bens@hbsslaw.com

Thomas M. Sobol (*pro hac vice*)
Abbye R. Klamann Ognibene (State Bar No. 311112)
HAGENS BERMAN SOBOL SHAPIRO LLP
55 Cambridge Parkway, Suite 301
Cambridge, MA 02142
Tel: (617) 482-3700
Fax: (617) 482-3003
tom@hbsslaw.com
abbyeo@hbsslaw.com

Aaron Mackey (State Bar No. 286647)
Andrew Crocker (State Bar No. 291596)
Adam D. Schwartz (State Bar No. 309491)
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel: (415) 436-9333
Fax: (415) 436-9993
amackey@eff.org
andrew@eff.org
adam@eff.org

Counsel for Plaintiffs and the Proposed Class