Shana E. 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

Attorneys for Plaintiffs and the Proposed Class

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

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' OPPOSITION TO DEFENDANTS AT&T SERVICES, INC. AND AT&T MOBILITY, LLC'S MOTION TO DISMISS

Hearing Date: November 9, 2020
Hearing Time: 9:30 a.m.
Judge: Hon. Sallie Kim
Ctrm: C-15th Floor

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

STATE CASES

FEDERAL STATUTES

FEDERAL RULESS

I. INTRODUCTION

As a telecommunications service provider, AT&T is entrusted with access to the highly sensitive, real-time location data of each of its customers. Complaint, ¶¶ 1, 35-40 (ECF No. 1). This location data is extremely granular; it can pinpoint a person's location within their home, or on an exact floor within an office building. *Id.*, ¶¶ 113-16. Recognizing the sensitivity of this data, and the risks to mobile customers when it is disclosed, federal law prohibits AT&T from selling it to anyone without its customer's notice and opt-in consent and requires that the company protect it from unauthorized access. *Id.*, ¶¶ 176-211. When mobile customers, including Plaintiffs, signed up for or renewed their AT&T services, AT&T promised them—and publicly represented—that it would not sell this sensitive data "to anyone for any purpose. Period." *Id.*, ¶¶ 1, 84, 157. AT&T also promised that it would use "security safeguards" to protect it. *Id.*, ¶ 236.

But in 2018, public reporting revealed that AT&T had, in fact, been selling its customers' real-time location data to hundreds of third parties since at least 2011, and that its lax location data safety and security systems had allowed repeated, widespread breaches. Compl., ¶¶ 1, 59-81, 236-40. When AT&T's practices were publicly disclosed, it promised to stop selling location data and to take immediate steps to secure it. *Id.*, ¶¶ 58, 82, 252-57. But AT&T's conduct did not stop; it continues to access its customer location data, sell it to third parties, and utilize the same woefully inadequate data safeguards and consent verification mechanisms that have since been found legally deficient by the Federal Communications Commission ("FCC").[1]

AT&T's conduct exposes Plaintiffs, members of the proposed class, and the public to ongoing safety and security risks. *Id.*, ¶¶ 1, 7, 147-53. Plaintiffs seek an injunction to address AT&T's misconduct, including to enjoin the unlawful disclosure of location data, secure previously-disclosed data, mandate compliance with the federal law requiring customer notice and valid consent

[1] *See* Declaration of Abbye R. K. Ognibene in Support of Plaintiffs' Opposition to Defendants AT&T Services, Inc. and AT&T Mobility, LLC's Motion to Dismiss ("Ognibene Decl."), Ex. F (Notice of Apparent Liability for Forfeiture and Admonishment, *In the Matter of AT&T Inc.*, FCC 20-26 (Feb. 28, 2020) (hereafter, "NAL")), concurrently filed herewith.

before location data is disclosed *to any third party*, and correct AT&T's public disclosures regarding its location data sales and safeguards. *Id.*, ¶¶ 279, 285, 299, 311, 342.

AT&T charts a narrow course in its Rule 12(b)(1) effort to avoid jurisdiction. It submits that in March 2019, it voluntarily stopped selling location data to one category of customers, third-party middlemen called "location data aggregators," who formerly brokered the sale of location data between AT&T and other third parties. ECF No. 73 ("Motion") at 4. Based on this thinnest of reeds, AT&T seeks dismissal of a subset of Plaintiffs' claims, arguing that Plaintiffs lack standing to pursue injunctive relief related to (i) providing location data aggregators with access to its customers' location data, and (ii) misrepresenting its sales to those aggregators. *Id.*

But AT&T's position runs counter to the law in the Ninth Circuit and the well-pleaded allegations in the Complaint. Multiple grounds establish jurisdiction here, where AT&T's illegal practices continue. *First*, AT&T's ongoing collection and disclosure of location data, coupled with its insufficient data security policies, creates an ongoing risk of injury. *Campbell v. Facebook, Inc.*, 951 F.3d 1106 (9th Cir. 2020); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1109 (N.D. Cal. 2010).

Second, the significant likelihood of future harm establishes an independent basis for jurisdiction. Under controlling Ninth Circuit law, Plaintiffs adequately allege a real and immediate threat of repeated injury here, where their injuries stem from AT&T's polices and patterns of practice. *Armstrong v. Davis*, 275 F.3d 849, 867 (9th Cir. 2001), *abrogated on other grounds by Johnson v. California*, 543 U.S. 499 (2005). AT&T has not changed those policies or implemented any technical safeguards to prevent unauthorized disclosure of customers' location data, nor has AT&T put forward evidence that it will not disclose location data in the future.

Finally, this Court has jurisdiction over Plaintiffs' claims for injunctive relief concerning AT&T's public statements regarding its location sales practices because AT&T's repeated misrepresentations leave Plaintiffs unable to rely on the company assertions. *Id.*, ¶ 258. *Davidson v. Kimberly-Clark Corp.*, 889 F.3d 956, 970 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 640 (2018).

Plaintiffs provide multiple, independent bases for this Court's jurisdiction, each supported by well-pleaded allegations and buttressed by facts uncovered by the FCC or disclosed in discovery. Plaintiffs respectfully request that AT&T's motion be denied in full.

II. FACTUAL BACKGROUND

A. AT&T profited from its disclosure of its customers' private location data.

Beginning by at least January 2011, AT&T sold access to its mobile customers' real-time location data to hundreds of third parties without customers' knowledge or consent. Compl., ¶¶ 1, 83-84. AT&T sold this data directly to third parties and indirectly through location data aggregators, who in turn resold the data. *See* NAL, ¶¶ 12-13. All the while, AT&T failed to make reasonable efforts to ensure that customers' location data was only disclosed following the notice and consent required by law and was not later resold downstream to additional third parties. Compl., ¶¶ 126-44, 238-40. As a result, a lucrative and unregulated location data market developed—wherein some third parties charged as much $1,100 per location request or "ping"—which jeopardized customers' safety and invaded their privacy. *Id.*, ¶¶ 79, 83-125.

B. When AT&T's misconduct was exposed, it made vague promises to stop.

AT&T only got caught, and its customers only learned the truth about its location data practices, when an FBI investigation found that the company's location sales system allowed a Missouri sheriff to "access location information for anyone he pleased" for years. NAL, ¶ 21. The sheriff unlawfully obtained the real-time location of 147 AT&T customers, including a state court judge. Compl., ¶¶ 5, 41-47; NAL, ¶¶ 20-21. He was able to access the data by uploading fraudulent consent records—including pages from his car insurance policy—which AT&T never reviewed or verified. Compl., ¶¶ 131-33; NAL, ¶ 21. In May 2018, the *New York Times* ran a story about Sheriff Hutcheson and publicly revealed AT&T's location data sales for the first time. Compl., ¶¶ 42-47.

Mere days after the Sheriff Hutcheson story broke, the weakness of AT&T's security protocols for customer location data was highlighted by two data breaches. *First*, hackers breached the same company that the sheriff used to access AT&T customers' data, compromising the highly sensitive location data of millions of AT&T customers. Compl., ¶ 53. *Second*, the same day, a researcher revealed that the location-querying demonstration that a separate AT&T client had publicly hosted for more than 16 months allowed "[a]nyone with a modicum of knowledge about how Web sites work" to obtain *any* AT&T customer's real-time location without consent. *Id.*, ¶ 56.

AT&T faced immediate public outcry, including condemnation by U.S. Senator Ron Wyden, who requested that the FCC investigate AT&T's "abusive and potentially unlawful" data sales practices, including its faulty consent-verifying system, which "needlessly exposes millions of Americans to potential abuse and surveillance[.]" *Id.*, ¶ 50. In June 2018, AT&T responded by representing that the reporting reflected isolated incidents, but that it would nonetheless "be ending [its] work with aggregators[.]" *Id.*, ¶ 58.

C. Despite its promise to stop, AT&T continued its sell customers' location data—including to aggregators—for nine more months.

AT&T's representations about the scope of its location data practices, and its promises to end its sale of the data, were false. Reporting throughout 2018 and into 2019 revealed that Sheriff Hutcheson's unlawful access was not an isolated incident; AT&T had been covertly selling its customers' location data to third parties across varied sectors—from bail bondsmen to landlords—for years. *See* Compl., ¶¶ 59-62 (June 2018 reporting reveals data was sold for wide-ranging purposes); ¶¶ 63-73 (January 2019 reporting reveals that AT&T is selling location data "to a dizzying number of sectors" and its location data clients are reselling the data, for as little as $300 per request, without customer consent); ¶¶ 74-81 (February 2019 reporting reveals AT&T's sales of a particularly sensitive type of location data to more than 250 bounty hunters and related businesses).

Despite this reporting and its promises in June 2018, AT&T did not stop selling location data. As Senator Wyden pointedly explained in January 2019 after media reports revealed ongoing sales:

> We catch them in 2018, they claim that they're going to stop—not a whole lot of qualifiers, they just say, 'We're going to stop'—and then we . . . saw that at least three of the four major carriers [including AT&T] had basically fed the American consumer a bunch of baloney . . . [T]hey made these promises to me in writing in 2018. Now, they're making these promises again, and so... permit me to be a little bit skeptical. I'll believe it when I actually see it. And there is a real pattern now in the technology space where essentially these companies get caught in irresponsible conduct... they apologize... and they pledge it won't happen again. But of course, it does it happen again. You can almost set your clock by it.

Compl., ¶ 257. That same month, fifteen U.S. senators wrote to the FCC and the Federal Trade Commission urging an investigation. *Id.*, ¶ 73. Congressman Frank Pallone, Jr., called for an

emergency hearing in February 2019, stressing the "grave consequences that unauthorized sharing of customer location data could have for public safety and national security[.]" *Id.*, ¶ 150.

D. The FCC investigated and proposed a $57 million fine against AT&T for its failure to adequately protect its customers' location data.

The FCC began investigating AT&T's disclosure of customer data shortly after publication of the *New York Times* story in 2018, culminating in the agency's Enforcement Bureau announcing that it was seeking more than $57 million in fines from AT&T in February 2020. NAL, at ¶¶ 30. The enforcement action centers on AT&T's violations of the Federal Communications Act ("FCA"), the federal law establishing AT&T's duty to protect the privacy and security of information about its customers. *See* 47 U.S.C. § 222. After reviewing more than 28,000 pages of AT&T documents, the FCC concluded that AT&T "willfully and repeatedly" violated the FCA and its accompanying CPNI regulations[2] by improperly disclosing its customers' location data without consent. *Id.*, ¶ 31. The Commission found that AT&T separately violated the FCA by "failing to protect the confidentiality of its customers' CPNI and by failing to employ 'reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI.'" *Id.*, ¶ 32 (quoting 47 § CFR 64.2010(a)). AT&T denied any wrongdoing throughout the FCC's investigation. Ognibene Decl., Ex. A.

In March 2019, more than nine months after initially promising to do so, AT&T finally cut off location data aggregators' access to its customers' location data. Mot. at 7-8;[3] Hill Decl., ¶ 3 & Ex. A.[4]

[2] CPNI is defined by the FCA as, *inter alia*, "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(h)(1); Compl., ¶ 181. The FCC has concluded that the real-time location data at issue here "falls squarely" within the definition of CPNI. NAL, ¶ 34.

[3] "Mot." or "Motion" refers to Defendants AT&T Services, Inc. and AT&T Mobility, LLC's Motion to Dismiss, Nov. 27, 2019, ECF No. 73.

[4] "Hill Decl." refers to the Declaration of Greg Hill, Nov. 27, 2019, ECF No. 73-1.

E. AT&T continues to collect and sell its customers' location data and has failed to rectify its data security practices.

Jurisdictional discovery has established that AT&T continues to sell acess to its customers' location data directly to third parties. Ognibene Decl., Exs. B-C. These direct sales occur over the same technical infrastructure, called an "application programming interface," or API, that AT&T used to provide location data access to aggregators and the aggregators' clients. *Id.*, Ex. D. The FCC found in February 2020 that AT&T never reformed the notice and consent procedures—nor the infrastructure issues—that gave rise to ongoing and widespread breaches of its customers' data over the preceding decade, despite its assurances that it would implement "enhanced" notice and consent in 2019. *See* NAL, ¶¶ 25, 68. Further, AT&T did not introduce new safeguards or other mechanisms to protect customer data sold to third parties, meaning it continues to have "almost no other visibility or apparent awareness into how the location data it sold was used or protected." *Id.*, ¶ 59. AT&T has made no public commitments regarding changes to its practices or policies nor any promises regarding future behavior. In essence, the totality of AT&T's location data system, polices, and practices—and its public representations regarding the same—remain unchanged, but for its voluntarily decision to end sales to aggregators.

III. PROCEDURAL BACKGROUND

Plaintiffs filed the Complaint on July 16, 2019. ECF No. 1. On September 11, 2019, AT&T moved to compel arbitration.[5] ECF No. 35. On November 27, 2019, AT&T moved to dismiss for lack of subject matter jurisdiction, 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, seven months of jurisdictional discovery. ECF No. 81. On July 1, 2020, the parties sought instruction from

[5] Plaintiffs believe that AT&T's present motion is an attempt to moot Plaintiffs' arguments in their opposition to the motion to compel (ECF No. 63). In their opposition briefing, Plaintiffs argue that AT&T's arbitration provision is unenforceable under the California Supreme Court's holding in *McGill v. Citibank, N.A.*, 2 Cal. 5th 945 (2017), because it purports to waive Plaintiffs' right to seek public injunctive relief under California's Unfair Competition Law and Consumers Legal Remedies Act in any forum. But because the present motion to dismiss does not challenge every form of injunctive relief the Plaintiffs seek, the outcome of this motion will have no determinative effect on the motion to compel arbitration.

the Court regarding the permissible scope of jurisdictional discovery. ECF No. 94. On July 8, 2020, the Court ordered that Plaintiffs were entitled to discovery into whether AT&T had stopped selling location data to third parties. ECF No. 96.

IV. LEGAL STANDARD

Plaintiffs bear the burden of establishing jurisdiction when a defendant moves to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1). *See Sciacca v. Apple, Inc.*, 362 F. Supp. 3d 787, 795 (N.D. Cal. 2019). A Rule 12(b)(1) jurisdictional attack may be facial or factual. *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). A facial attack disputes an allegation's sufficiency and a factual attack disputes an allegation's truth. *Id.* The motion might dispute the truth of some allegations and the sufficiency of others. *See, e.g.*, *Weiss v. See's Candy Shops, Inc.*, 2017 WL 3326760, *2 (N.D. Cal. Aug. 3, 2017). While a response to a factual attack must meet evidence with evidence (*Safe Air*, 373 F.3d at 1039), 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)).

AT&T has proffered evidence on a single point: whether, and with whom, it stopped sharing location data. Plaintiffs present facts responding to that evidence. *See* Ognibene Decl., Exs. B-D, F. On all other points, AT&T raises only facial challenges. Throughout this brief, Plaintiffs cite factual evidence—including facts disclosed by the FCC after the Complaint was filed—establishing the plausibility of their allegations on these points, allegations that must be taken as true for purposes of this motion. *Dahlia v. Rodriguez*, 735 F.3d 1060, 1066 (9th Cir. 2013) (at the motion to dismiss phase, the court '"must accept all factual allegations of the complaint as true and draw all reasonable inferences in favor of the nonmoving party"' (quoting *TwoRivers v. Lewis*, 174 F.3d 987, 991 (9th Cir. 1999))).

V. ARGUMENT

AT&T's motion to dismiss ignores the well-settled law of the Ninth Circuit—reiterated just six months ago in the privacy class action context—under which Plaintiffs have adequately established two independent bases for this Court's jurisdiction: the ongoing risk of harm and the real and immediate risk of future harm. *Campbell*, 951 F.3d at 1106. AT&T attacks only a subset of Plaintiffs' injunctive relief claims, arguing that they lack standing to (i) enjoin "the provision of

geolocation data to aggregators" (Mot. at 2), and (ii) "prohibit[] AT&T from making false statements in connection with providing geolocation information to data aggregators." *Id.* at 6. Its challenges rest on the same, singular ground: because AT&T voluntarily stopped providing aggregators with location data before Plaintiffs filed the Complaint, these injunctive relief claims should be dismissed for want of subject matter jurisdiction. AT&T does not challenge Plaintiffs' claims for any other form of injunctive relief.[6]

AT&T's motion fails because it ignores that the Complaint, and the injunctive relief it seeks, aims to remedy the company's failures to prevent disclosure of its customers' location data *to any party* without customer notice and consent.[7] As the Complaint makes clear, the issue is not AT&T's sale to the aggregators, *per se*, but rather its practice of "selling its customers' real-time location data to . . . third parties *without the required customer consent and without any legal authority*." Compl., ¶ 1 (emphasis added). The narrow fact that AT&T has voluntarily ceased selling location data to aggregators is insufficient to warrant dismissal here, where AT&T's location data practices continue to harm Plaintiffs and create a real and imminent threat of future injury.

[6] Plaintiffs seek several, additional types of injunctive relief, including, *inter alia*, an order (i) enjoining AT&T's illegal conduct, (ii) requiring AT&T to ensure that any current or historical location data is properly safeguarded and secured, and (iii) restraining AT&T from further disobedience of the FCC's regulations regarding CPNI pursuant to the FCA. Compl., ¶¶ 279(j), 285, 299, 311, 342.

[7] While AT&T makes much of ending its contracts with aggregators, its unlawful conduct—and the allegations in the Complaint—are not cabined to data sales made to or through these entities. *See, e.g.*, Compl., ¶¶ 1, 5, 83, 118, 126, 145-147, 154, 189, 238, 240, 242, 270, 276. The fact that the Complaint is replete with examples of how AT&T's sales through aggregators led to unlawful data access is a consequence of the limited information available to Plaintiffs before any discovery occurred. *Id.*, ¶ 154 ("Plaintiffs do not, and indeed cannot, known how many and which third parties—*in addition to the Aggregator Defendants*—accessed their sensitive location data. AT&T, the Aggregator Defendants, and the third parties with whom they contract to sell Plaintiffs' and Class members' location data are the sole parties with access to that information about whose data was sold, when, and to whom") (emphasis added). AT&T's sales to aggregators were the subject of ongoing media reporting. But the FCC's investigation—and jurisdictional discovery—revealed that AT&T is also engaged in direct sales of location data. *See* NAL, ¶ 17; Ognibene Decl., Ex. B.

A. Plaintiffs have standing to seek injunctive relief regarding AT&T's sale and safeguarding of its customers' location data.

In the Ninth Circuit, the relevant jurisdictional inquiry is whether plaintiffs have shown "either 'continuing, present adverse effects' due to [their] exposure to [the defendant's] past illegal conduct or 'a sufficient likelihood that [they] will again be wronged in a similar way.'" *Villa v. Maricopa Cty.*, 865 F.3d 1224, 1229 (9th Cir. 2017) (first quoting *O'Shea v. Littleton*, 414 U.S. 488, 495-96 (1974); then quoting *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983)). The inquiry is not whether a defendant voluntarily ceased the conduct at issue before the complaint was filed. Here, the facts demonstrate that Plaintiffs face *both* ongoing risks of further disclosure and a likelihood of future harm, providing two independent bases for this Court's jurisdiction.

1. Plaintiffs face an ongoing risk of further location data disclosure.

Plaintiffs allege, and facts obtained by the FCC and during jurisdictional discovery demonstrate, that they are at substantial risk of ongoing harm due to AT&T's location data practices. AT&T continues to collect its customers' location data, sell it to third parties, utilize the same faulty consent mechanisms that enabled its unauthorized dissemination, and neglect its duty to ensure against downstream disclosure. *See* Section II.E., *supra*. As such, Plaintiffs face an ongoing risk of disclosure and continue to pay for mobile services with inadequate safety features.

a. AT&T's continues to access and sell customers' location data.

AT&T does not assert that it has stopped selling customers' location data. It represents that it has cut off only a sub-section of sales—sales to the data aggregators. Mot. at 7-8; Hill Decl., ¶ 3. A recent Ninth Circuit decision, *Campbell*, 951 F.3d at 1106, demonstrates that plaintiffs have standing to seek injunctive relief despite a defendant's half-hearted change in practice. In *Campbell*, the plaintiffs alleged that Facebook violated privacy and consumer protection statutes by scanning its users' private messages to increase third parties' "Like" counters. *Id.* at 1112. By the time the plaintiffs filed suit, "some (but not all) of Facebook's challenged uses of private message URL data had ended." *Id.* at 1120. Facebook was still "accessing private messages—conduct that [it had] never claimed to have ceased" and its "ongoing retention of the data . . . meant that there was a risk that it would resume using the data for 'Like' counters, resume sharing the data with third parties, or begin

using the data for some other purpose." *Id.* The district court held,[8] and the Ninth Circuit affirmed, that this "combination of continuing harm plus likelihood of future harm was sufficient for Plaintiffs to have standing to seek injunctive relief." *Campbell*, 951 F.3d at 1120.

Plaintiffs face an even greater combination of continuing harm and likelihood of future injury than the *Campbell* plaintiffs. Plaintiffs are active AT&T customers. Compl., ¶¶ 8, 10-12; *cf. Hangarter v. Provident Life & Acc. Ins. Co.*, 373 F.3d 998, 1022 (9th Cir. 2004) (plaintiff with "no contractual relationship with Defendants" lacked standing to seek injunctive relief). AT&T continues to have constant access to Plaintiffs' location data and still operates the same underlying mechanism to disclose that sensitive information. And Plaintiffs have no ability—short of breaking their contracts[9]—to restrict that access or disclosure. Compl., ¶¶ 3, 35-40, 109; *see also* NAL, ¶ 40 ("[T]he customer has no choice but to reveal that location to the carrier."); *id.*, ¶ 11. That AT&T continues to have access to location data, and continues to use and sell it, creates a risk that AT&T will resume using it for unauthorized purposes or allow others to do so. *Campbell*, 951 F.3d at 1120. As in *Campbell*, this is sufficient to establish Plaintiffs' standing.

In light of *Campbell,* the cases AT&T relies on are inapposite. The facts here—where Plaintiffs are still customers of AT&T, which maintains the same mechanism to disclose customer data that it has for years and still discloses customer data to third parties—are a far cry from the speculation at issue in *Miller v. Time Warner Cable Inc.*, 2016 WL 7471302, at *4 (C.D. Cal. Dec. 27, 2016) (former customer's risk of "real or immediate threat of repeated injury" was "too speculative"). And Plaintiffs are in the opposite position as those in *Smart v. Sony Corp. of Am., Inc.*, 2010 WL 11508565, at *3 (S.D. Cal. Aug. 6, 2010), because the product here—customer location data—continues to be collected and sold. *Id.* (standing lacking where plaintiff sought injunctive relief concerning "products that are no longer manufactured or sold").

[8] *See Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014).

[9] *See Vianu v. AT&T Mobility LLC*, 2020 WL 3103797, at *9 (N.D. Cal. June 11, 2020) (denying AT&T's motion to dismiss for lack of standing to seek injunctive relief where plaintiffs were "current AT&T customers, allegedly locked into service plans" and noting that such "contracts are long-term contracts, and breaking them comes with a penalty").

b. AT&T has failed to remedy its inadequate data security systems.

Plaintiffs face an ongoing risk that their location data will be accessed by third parties without their authorization or legal authority—and continue to overpay for their mobile service—due to AT&T's failure to implement sufficient safeguards of their data. Compl., ¶¶ 126-44, 147-56, 194-209; NAL, ¶¶ 51-70. Courts in the Ninth Circuit have repeatedly found that plaintiffs sufficiently "allege an ongoing injury" when, "as a matter of policy, [a defendant] continues to collect and disseminate the same type of data" but "has taken no steps to ensure that such information is not disclosed again in the future." *Doe 1*, 719 F. Supp. 2d at 1109; *see also Bell v. Blizzard Entm't, Inc.*, 2013 WL 12063912, at *6 (C.D. Cal. Apr. 3, 2013) (plaintiffs had standing to assert claim for injunctive relief when "despite the past security breaches, [defendant] ha[d] made no additional effort to secure their information."). Here, AT&T has ongoing access to and collects location data, and nonetheless has failed to take adequate steps to protect it, creating an ongoing risk that Plaintiffs will be injured in at least four ways: that their data will be disclosed without their consent, that third-parties to whom their data is sold will resell it without authorization, that their data will be breached, and that data that has already been sold will not be sufficiently safeguarded.

First, because AT&T has made no changes to the way it obtains consent before disclosing location data, Plaintiffs remain at risk of unauthorized disclosures. AT&T continues to use the same system, including the same API and same notice and consent mechanisms, that it relied on in the past. Ognibene Decl., Ex. C-D. As the FCC confirmed, AT&T does not obtain notice and consent directly from its customers. NAL, ¶¶ 16, 55-56. Instead, it improperly relies on "the companies seeking to access customers' real-time location data" to do so. Compl., ¶ 127; *see also* NAL, ¶ 56 (AT&T's "safeguard relied almost entirely on the unverified assertions of the Aggregators and location-based service providers to whom AT&T sold access to customer location information."). While AT&T's contracts require its location data clients to obtain customer consent, AT&T has a policy of not "verify[ing] the consent before providing access to the location data; instead it claimed to verify on a daily basis that each request for information was tied to a consent record." NAL, ¶ 16; *see also id.*, ¶ 59. By failing to check the content of the consent records, and instead verifying only that they exist, AT&T abandons its obligation under federal law to obtain customers' opt-in consent

before disclosing their location data—a statutory obligation the FCC found AT&T could not avoid "by assigning . . . to a third party." NAL, ¶ 47; *see also id.*, ¶¶ 5, 55-56; 47 U.S.C. § 222(c)(1). This system is legally insufficient. For example, the "consent records" uploaded by Sheriff Hutcheson *for four years* were not even facially valid—they were pages from his insurance manual and other random documents. *Id.*, ¶ 21; *see also id.*, ¶ 56 (finding that AT&T's "practice of reviewing consent records allowed . . . breaches to continue for at least four years without AT&T's knowledge"); Compl., ¶ 47. In condemning this "clear abuse" of the federal consent requirement, Senator Ron Wyden described it as "the legal equivalent of a pinky promise." *Id.*, ¶ 144. Plaintiffs allege—and the FCC found—that AT&T's practice of delegating its consent responsibility failed to protect AT&T customers' sensitive location data, as third parties routinely failed to obtain consent before accessing the data or selling it downstream. NAL, ¶¶ 55-60; Compl., ¶¶ 82, 134-35, 140-44.

AT&T has failed to rectify its faulty consent mechanisms, despite years of notice that they were woefully inadequate. As the FCC stressed, "the apparent failure of AT&T to impose reasonable safeguards on its program to sell access to customer location information after the New York Times article is not merely a matter of theory." NAL, ¶ 65. The FCC's investigation determined that even after AT&T was on notice that "the 'consent records' it received through indirect arrangements with location-based service provers were not reliable indicia of customer consent," it nonetheless failed to implement a new notice and consent mechanism that would comply with the law. *Id.*, ¶ 32; *see id.*, ¶ 25 ("In November 2018, AT&T told Enforcement Bureau staff that it planned to implement 'enhanced' notice and consent measures for location information-sharing in 2019, but has offered no evidence that it did so."); ¶ 68 ("[T]here is no evidence that AT&T ever implemented any of these modifications to its consent verification process."); *see also* Ognibene Dec., Ex. E (August 2020 letter from FCC commissioner noting that AT&T failed to implement enhanced notice and consent). Indeed, the shortcomings of the consent mechanisms—and AT&T's failure to change its system in response to widespread unauthorized access—was central to the FCC's finding that the company failed to adopt reasonable measures to protect its customers' location data. *See* NAL, ¶¶ 51-70 (detailing the myriad ways AT&T failed to protect consumer location data). Nonetheless, AT&T

continues to rely on this same system, and Plaintiffs continue to pay for mobile service with inadequate data safeguards, placing their sensitive data at risk.[10]

Second, because AT&T has failed to implement any new safeguards preventing the resale of customer location data by third parties, plaintiffs face an ongoing risk of downstream disclosure of their data by third parties who continue to receive it. Ognibene Decl., Exs. B-C; Compl., ¶¶ 83, 139. Even though it continues to sell customer location data to multiple third parties, AT&T does not detail in its declaration what, if any, steps the company has taken to ensure that the data is properly safeguarded and not resold. Even if AT&T had sufficient consent mechanisms—which it does not—the FCC has stressed that "reliance on the opt-in approval requirement alone is insufficient to protect customers' interest in the privacy of their CPNI" and carriers must also "take reasonable measures to *discover* and *protect* against attempts to gain unauthorized access to CPNI." NAL, ¶ 7 (emphasis in original). The obligation to "take reasonable measures to protect the confidentiality of CPNI" is a "*permanent and ongoing obligation* to police disclosures and ensure proper functioning of security measures." *Id.*, ¶ 8 (emphasis added). AT&T has failed to put in place any downstream protections and, as a result, has "no other visibility or apparent awareness into how the location data it sold was used or protected." *Id.*, ¶ 59. AT&T's absent oversight of downstream disclosure is well-documented, and the facts show that it has done nothing to prevent the same behavior from recurring. *Id.*, ¶ 66 (concluding that additional, unauthorized downstream sales continued even after previous breaches "had demonstrated serious systemic flaws in AT&T's safeguards to protect CPNI," and yet "AT&T continued to rely on those same safeguards *so that it could continue to sell access*[.]"(emphasis added)).

Third, Plaintiffs face ongoing risks from AT&T's failure to store location data in a secure manner. Compl., ¶¶ 52-56, 210-13, 218. One of AT&T's aggregator clients hosted a demonstration on its public website, whereby users could try out its location targeting technology. *Id.*, ¶ 55. Due to woefully inadequate data security, "[a]nyone with a modicum of knowledge about how Web sites

[10] In its investigation, the FCC found that "[i]n general, AT&T relied on the same safeguards before and after" the media exposed widespread and ongoing breaches of customer location data, NAL, ¶ 53, and that it "failed to demonstrate that its safeguards were reasonable." *Id.*, ¶ 60.

work" could bypass the website's consent structure and obtain *any* AT&T customer's location data without their consent or knowledge. *Id.*, ¶ 56. The demo remained live for at least *16 months* without any action from AT&T. *Id.* This breach reflects a glaring defect in AT&T's security safeguards, thereby increasing Plaintiffs' risk of a data breach. *Id.*, ¶ 236. Additionally, AT&T has failed to ensure that the third parties to whom it sells location data store AT&T customers' data in a secure manner, as reflected by a May 2018 breach of a third-party's server, which exposed log-in credentials and provided access to all AT&T customers' location data. *Id.*, ¶ 52.

Finally, despite vague promises to verify that its location data clients abide by contractual obligations to delete previously-obtained location data, AT&T has failed to take any meaningful action to secure historical location data. *See* Hill Decl., Ex. 1 at 2 (ECF No. 73-2). These failures provide an independent basis for the Court's jurisdiction. *See Doe 1*, 719 F. Supp. 2d at 1109 (plaintiffs established ongoing injury where defendant "made no effort to retrieve" information that had been wrongfully disseminated, "or prevent its further republication"); *Matera v. Google Inc.*, 2016 WL 5339806, at *19 (N.D. Cal. Sept. 23, 2016) (plaintiff had standing to seek injunctive relief requiring defendant to destroy unlawfully-obtained data).[11] As the FCC found, AT&T's "contractual safeguard alone was insufficient to prevent the misuse of the customer location information to which AT&T sold access." NAL, ¶ 54. Cutting off the aggregators does nothing to secure data that has already been wrongfully disclosed. As the FCC has recognized, "a carrier cannot simply rectify the harms resulting from a breach by terminating its agreement." *Id.*, ¶ 16. Nonetheless, AT&T has failed to take adequate steps to protect this data, and Plaintiffs allege a continuing risk of access and misuse. Compl., ¶¶ 158, 299.

In its Motion, AT&T does not claim to have either (i) addressed these security deficiencies, or (ii) ceased the unlawful conduct alleged in the Complaint, which discovery has shown continues. It asserts only that it has stopped providing location data to one category of third parties: the location

[11] Like the defendant in *Doe 1*, AT&T argued to the FCC that "it has no control over the third parties which possess such information." *Doe 1*, 719 F. Supp. 2d at 1109; *see* NAL, ¶ 63. As in *Doe 1*, there is no evidence that AT&T "requires 'permission' to take action to prevent [third parties] from republishing [AT&T customers'] confidential . . . data," and thus this does not defeat standing. *Doe 1*, 719 F. Supp. 2d at 1109.

data aggregators. Mot. at 7-8; Hill Decl., ¶ 3. This narrow fact is insufficient to deny Plaintiffs standing, where continuing data sales and inadequate security safeguards put them at ongoing risk.

2. Plaintiffs face a real and immediate threat of future injury.

As an independent basis for this Court's jurisdiction, Plaintiffs allege that they face a "real and immediate threat of repeated injury." *O'Shea*, 414 U.S. at 496. While AT&T maintains that the only relevant fact concerning the risk of future injury is whether it has ceased its sales to aggregators, the Ninth Circuit has instructed that in analyzing the threat of repeated injury, courts "must be careful not to employ too narrow or technical an approach. Rather, we must examine the questions realistically: we must reject the temptation to parse too finely, and consider instead the context of the inquiry." *Armstrong*, 275 F.3d at 867.

In evaluating the risk of future injury, "an essential consideration is whether it would have been possible for Defendants to reoffend as to [plaintiffs] at the time [they] filed the complaint." *Norton v. LVNV Funding, LLC*, 396 F. Supp. 3d 901, 920 (N.D. Cal. 2019). If AT&T truly has ceased all of the unlawful conduct alleged—and AT&T has neither asserted nor presented any evidence that it has—nothing in the Complaint supports finding that AT&T could not again (i) intrude on Plaintiffs' privacy by allowing unconsented access to their location data, (ii) fail to implement sufficient safeguards, or (iii) misrepresent its data location practices and security features.

a. AT&T's inadequate safeguards are the product of its policies and practices.

In *Armstrong*, the Ninth Circuit outlined two ways that plaintiffs can show that an injury is likely to reoccur. 275 F.3d at 861. *First*, they may show that the defendant had, at the time of the injury, a written policy, and that the injury "stems from" that policy. *Id. Second*, they may demonstrate that the harm is part of a "pattern of officially sanctioned . . . behavior, violative of the plaintiffs' [federal] rights." *Id.* (quoting *LaDuke v. Nelson*, 762 F.2d 1318, 1323 (9th Cir. 1985)).

AT&T's repeated failures to protect its customers' location data by outsourcing that duty to third parties via contract amounts to a policy that failed to protect customer location data. *See* Section V.A.1.b., *supra*. AT&T's widespread breaches were not happenstance occurences, they were the consequence of its written policies and written contracts with its location data clients, which

allowed AT&T to abdicate its responsibility for obtaining customer consent prior to location data disclosures. Compl., ¶¶ 43, 86, 154, 251; *see also* NAL, ¶¶ 16, 55-59. Where, as here, "the harm alleged is directly traceable to a written policy, there is an implicit likelihood of its repetition in the immediate future." *Armstrong*, 275 F.3d at 861 (citation and quotation omitted).

Plaintiffs also allege that AT&T's privacy violations were a part of the company's pattern of repeatedly failing to protect customers' data. AT&T knew for years that its security practices were insufficient, and yet it failed to take appropriate remedial action–or update its misleading public statements about the adequacy of those systems. *See* Section II.E., *supra*. While "past wrongs do not in themselves amount to [a] real and immediate threat of injury necessary to make out a case or controversy," *Lyons*, 461 U.S. at 103, they are "evidence bearing on whether there is a real and immediate threat of repeated injury." *O'Shea*, 414 U.S. at 496. AT&T's pattern of unreasonable conduct increases the risk of future injury because, "where the defendants have repeatedly engaged in the injurious acts in the past, there is a sufficient possibility that they will engage in them in the near future to satisfy the 'realistic repetition' requirement." *Armstrong*, 275 F.3d at 861. Courts in this district have found that where, as here, a defendant's "faulty security practices in collecting and storing plaintiff's information," causes repeated injury, the "repetitive losses of users' privacy [sic] supplies a long-term need for supervision[.]" *Adkins v. Facebook, Inc*., 424 F. Supp. 3d 686, 659-80, 698 (N.D. Cal. 2019).

AT&T's failure to safeguard customers' location data is a continuation of a long history of data security lapses. For example, in 2015, AT&T faced an FCC enforcement action, and paid a $25 million fine, when it failed to properly protect almost 280,000 customers' CPNI from data breaches. Compl., ¶ 228. There, as here, the FCC found that the breaches were the result of AT&T's "failure to reasonably secure customers' proprietary information" and "constitute[d] an unjust and unreasonable practice in violation of the [FCA]." *Id.*, ¶ 229. Despite agreeing to develop and implement improved privacy and data security practices to safeguard customers' sensitive data from similar breaches in the future, AT&T faced an additional $27 million FCC fine—again for failing to protect its customers' data—fewer than five years later. *See, generally*, NAL.

b. AT&T does not admit to any wrongdoing, nor has it committed to change its policies and practices to comply with federal law.

AT&T only ceased providing aggregators with access to its customers' location data when its practices were exposed by the media and condemned by FCC commissioners and members of Congress. Compl., ¶¶ 42-82. Even then, AT&T stopped short of admitting wrongdoing or announcing permanent changes in its practices or policies, such as implementing enhanced safeguarding or minimal compliance with 47 U.S.C. § 222's notice and consent requirements. *See* Hill Decl. (asserting *only* that AT&T stopped selling location data to aggregators).

While "past conduct alone is insufficient to support a claim for injunctive relief … '[a] trial court's wide discretion in fashioning remedies is not to be exercised to deny relief altogether by lightly inferring an abandonment of the unlawful activities from a cessation which seems timed to anticipate suit.'" *Norton*, 396 F. Supp. 3d at 920 (quoting *United States v. Parke, Davis & Co.*, 362 U.S. 29, 48 (1960)); *see also S.E.C. v. Koracorp Indus., Inc.*, 575 F.2d 692, 698 (9th Cir. 1978) ("Promises of reformation and acts of contrition are relevant in deciding whether an injunction shall issue, but neither is conclusive or even necessarily persuasive, especially if no evidence of remorse surfaces until the violator is caught.").

Here, AT&T has made no representations that its voluntary cessation of location sales to aggregators is permanent. As Senator Wyden pointedly explained, "[T]here is a real pattern now in the technology space where essentially these companies get caught in irresponsible conduct . . . they apologize . . . and they pledge it won't happen again. But of course, it does it happen again. *You can almost set your clock by it*." Compl., ¶ 257 (emphasis added); *see also In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *31 (N.D. Cal. Aug. 30, 2017) (standing established where defendants failed to take remedial action and "continued to dispute the scope of their responsibility"); *cf. Matera*, 2016 WL 5339806, at *15 n.3 (jurisdiction lacking where defendant's attorney represented to the court that it would not restart the complained-of program);[12] *Khan v. K2*

[12] *Matera* is distinguishable from this case. In *Matera*, the plaintiffs sought an injunction to end a specific practice: scanning incoming emails for certain Google educational products. 2016 WL 5339806 at *15-16. Unlike in *Matera*, plaintiffs here seek an injunction broadly requiring AT&T to

Pure Sols., LP, 2013 WL 6235572, at *3 (N.D. Cal. Dec. 2, 2013) (plaintiff lacked standing for injunctive relief where defendant made "representations to the Court that it will not seek to enforce the non-compete agreements" at issue); *Howard v. Octagon, Inc.*, 2013 WL 5122191, at *4 (N.D. Cal. Sept. 13, 2013) (plaintiff lacked standing for declaratory relief under the UCL where defense counsel "represented to the court, both in its papers filed in support of the present motion, and in open court . . . that it does not intend to seek to enforce" the challenged agreement).

At the time the Complaint was filed, AT&T still had not updated its privacy policy or made any public declaration of an intent to permanently end its location data sales. In these circumstances, Plaintiffs face "a sufficient likelihood that [they] will again be wronged in a similar way." *Lyons*, 461 U.S. at 111. The Court should not infer that AT&T has permanently abandoned its unlawful location data practices and should instead give weight to Plaintiffs' well-pleaded claims concerning the ongoing risks they face as a result of AT&T's conduct.

B. Plaintiffs have standing to seek injunctive relief regarding AT&T's public misrepresentations and omissions concerning its location data practices.

This Court also has jurisdiction to enjoin AT&T from further public misrepresentations concerning its sales and safeguarding of location data. AT&T challenges only this Court's jurisdiction to grant Plaintiffs relief concerning "misrepresentations in connection with providing information to data aggregators," arguing that such relief is "derivative of conduct that AT&T already stopped before Plaintiffs filed this lawsuit." Mot. at 8, n.5.[13] But in the Ninth Circuit, plaintiffs have standing to seek an injunction against a defendant's misrepresentations and have established a threat of future harm when they plausibly allege that they "will be unable to rely on the product's advertising or labeling in the future[.]" *Davidson*, 889 F.3d at 970. Where, as here, the plaintiff is a current customer and "nothing indicates that she wants to stop being a customer," an

---

comply with the FCA and related CPNI regulations prohibiting disclosure without customer notice and consent. Plaintiffs' injunctive relief is not limited to narrowly prohibiting disclosure of their location data to aggregators.

[13] Plaintiffs also seek to enjoin AT&T's from misrepresenting its data security practices. Compl., ¶¶ 299, 342; *Tyler Barnett PR, LLC v. Facebook Inc.*, 2018 WL 2974695, at *3 (N.D. Cal. June 1, 2018). But because AT&T does not challenge this relief, Plaintiffs do not address their standing to seek it here.

inability to rely on the veracity of a defendant's representations is sufficient to establish standing. *Eiess v. USAA Fed. Sav. Bank*, 404 F. Supp. 3d 1240, 1258 (N.D. Cal. 2019); *see also Vianu*, 2020 WL 3103797, at *9 ("Existing customers who may renew again with appropriate disclosures seem sufficiently analogous at the pleadings stage to *Davidson* to clear the standing hurdle.").

Plaintiffs have shown that AT&T's location data sales and security failings were a part of a pattern of misconduct that has left them unable to rely on AT&T's representations, establishing an ongoing harm to Plaintiffs and the public. Compl., ¶¶ 279(j) ("AT&T has made repeated misrepresentations about when it would end the privacy-violative acts complained of herein, and how. Due to these continuous misrepresentations, Plaintiffs have no basis to believe that AT&T will cease its practices on a voluntary basis"); ¶ 254 ("Moreover, AT&T repeatedly represented that it would stop selling access to Plaintiffs' and similarly situated customers' location data to the Aggregator Defendants *and all third parties*. These representations were false") (emphasis added); ¶ 258 ("Plaintiffs and AT&T customers therefore have no reason to believe AT&T's continuous representations that it would or will end the sale of real-time location data are credible").

AT&T has repeatedly misrepresented or failed to disclose material details concerning its location sales and disclosure practices (Compl., ¶¶ 235, 241-47) and its sale of location data to third parties (*id*., ¶¶ 254-58). AT&T publicly promised its customers that it would not sell their "personal information to anyone for any purpose[,]" despite doing exactly that, *for years*. *Id.*, ¶¶ 1, 157. Plaintiffs have a heightened reliance on the veracity of AT&T's representations regarding its location data practices because AT&T continues to have access to their location data, Plaintiffs cannot prevent such access, and breaches occur without their knowledge. *Id*., ¶¶ 3, 5, 10-12, 35-40, 109, 154; *cf. Smart*, 2010 WL 11508565, at *4 (jurisdiction over injunctive relief claims lacking where the "chances that defendants will disseminate false representations" are "not high" because the defendants "no longer market, manufacture, nor sell" the product at issue). Even if AT&T claimed to have stopped providing location data to all third parties and to have heightened its notice and consent procedures—which it does not—Plaintiffs cannot trust Defendants' representations. *Yahoo!*, 2017 WL 3727318, at *31. Absent injunctive relief, Plaintiffs and the public will have "no way of determining" whether or not AT&T has improved its safety and security protocols and truly ceased

its location sales—to the aggregators or any third party. *Davidson*, 873 F.3d at 1115; *see also Shank v. Presidio Brands, Inc.*, 2018 WL 1948830, at *5 (N.D. Cal. Apr. 25, 2018). Plaintiffs have therefore established their standing to seek injunctive relief.

C. Leave to amend should be granted if AT&T's motion is granted.

"[D]ismissal without leave to amend is improper unless it is clear . . . that the complaint could not be saved by any amendment." *Petersen v. Boeing Co.*, 715 F.3d 276, 280 (9th Cir. 2013) (leave to amend "should be granted with extreme liberality."); Fed. R. Civ. P. 15(a)(2). Amendment here would not be futile, and Plaintiffs should be afforded an opportunity to allege more facts as needed to cure any issues and avoid dismissal. *See, e.g.*, *Ramirez v. Manpower, Inc.*, 2014 WL 116531, at *7 (N.D. Cal. Jan. 13, 2014) (granting plaintiffs leave to amend claim for injunctive relief); *Cunha v. IntelliCheck, LLC*, 254 F. Supp. 3d 1124, 1140 (N.D. Cal. 2017) (same).

VI. CONCLUSION

For the foregoing reasons, Plaintiffs ask this Court to find that it has subject matter jurisdiction over their well-pleaded claims for injunctive relief and to deny AT&T's motion in its entirety.

Date: October 9, 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 (admitted *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

Attorneys for Plaintiffs and the Putative Class