

PIERCE BAINBRIDGE BECK PRICE  
& HECHT LLP  
Thomas D. Warren (State Bar No. 160921)  
[twarren@piercebainbridge.com](mailto:twarren@piercebainbridge.com)  
Abbye R. Klamann Ognibene  
(State Bar No. 311112)  
[aognibene@piercebainbridge.com](mailto:aognibene@piercebainbridge.com)  
335 S. Grand Avenue, 44th Floor  
Los Angeles, CA 90071  
Telephone: (213) 262-9333  
Facsimile: (213) 297-2008

*Counsel for Plaintiffs*

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

THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA  
SAN FRANCISCO/OAKLAND 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.

Case No. 19-cv-4063

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

**TABLE OF CONTENTS**

<b>NATURE OF THE ACTION</b> .....	<b>1</b>
<b>THE PARTIES</b> .....	<b>3</b>
A. The Plaintiffs .....	3
B. The AT&T Defendants.....	4
C. The Aggregator Defendants .....	5
<b>JURISDICTION AND VENUE</b> .....	<b>8</b>
<b>DIVISION ASSIGNMENT</b> .....	<b>9</b>
<b>ALLEGATIONS APPLICABLE TO ALL COUNTS</b> .....	<b>9</b>
A. AT&T Has Access to Its Customers’ Real-Time Location Data by Virtue of Operating a Mobile Cellular Phone Network .....	9
B. Public Reports Reveal AT&T’s Sale of Access to Its Customers’ Real-Time Location Data, and the Rampant Abuses Flowing from Such Sale .....	10
C. Defendants Developed and Profit from a Robust Market for Customers’ Real-Time Location Data.....	21
D. Defendants Sell Access to Location Data Intended for Enhanced 911- Purposes.....	27
E. AT&T Allowed Unauthorized Third Parties to Access Customers’ Location Data.....	32
F. Defendants’ Sale of Access to Customers’ Location Data Is Outrageous and Harmful ...	36
G. The Sale of Location Data Violates Reasonable Expectations of Privacy and Is Highly Offensive.....	39
H. AT&T’s Misrepresentations and Omissions Concerning the Sale of Customer Location Data .....	55
I. Fraudulent Concealment and Tolling .....	62
J. Named Plaintiff Allegations .....	62
<b>CLASS ALLEGATIONS</b> .....	<b>63</b>
<b>CLAIMS FOR RELIEF</b> .....	<b>66</b>
<b>PRAYER FOR RELIEF</b> .....	<b>76</b>

## 1 NATURE OF THE ACTION

2 1. This class action arises from AT&T's<sup>1</sup> knowing, systematic, and unauthorized  
 3 sale of its wireless phone customers' sensitive location data. Despite vowing to its customers  
 4 that it does not "sell [their] Personal Information to anyone for any purpose,"<sup>2</sup> AT&T has been  
 5 selling its customers' real-time location data to credit agencies, bail bondsmen, and countless  
 6 other third parties without the required customer consent and without any legal authority.  
 7 AT&T's practice is an egregious and dangerous breach of Plaintiffs' and all AT&T customers'  
 8 privacy, as well as a violation of state and federal law.

9 2. As a telecommunications carrier, AT&T is entrusted with real-time location data  
 10 so that it can help 911 operators find its customers in the event of an emergency. Underlying this  
 11 911 data is a powerful, highly precise technology that can locate callers within a building, to the  
 12 floor or even room level. This real-time location data is highly sensitive and can reveal where  
 13 *any* AT&T customer is located—often within just a few meters—in seconds.

14 3. This precise, real-time location data is intended solely for public safety uses.  
 15 Plaintiffs and other AT&T customers have no ability to opt out of its collection. This data was  
 16 never intended for broad commercial purposes. To the contrary, federal law requires AT&T to  
 17 protect and safeguard its customers' sensitive data, and mandates that AT&T not allow third  
 18 parties to use or access customers' geolocation information except in rare public safety scenarios  
 19 or with the customer's affirmative, express consent.

20 4. AT&T has knowingly breached its duties to protect Plaintiffs' sensitive location  
 21 data in order to profit from it. Despite the recognized sensitivity of location data and AT&T's  
 22 obligations and promises to safeguard it, AT&T has been allowing unauthorized access to its  
 23 customers' precise, real-time location data to thousands of third parties for years. AT&T works  
 24 with location data aggregator companies which specialize in the commercial sale of location data  
 25 for widespread purposes. AT&T uses these aggregators, including Aggregator Defendants  
 26

27 <sup>1</sup> Defined herein to include defendants AT&T Services, Inc., AT&T Mobility LLC, and AT&T  
 28 Inc.

<sup>2</sup> AT&T, "Privacy Policy," attached hereto as Ex. A.

1 LocationSmart and Zumigo, to manage the sale of its data to thousands of entities—including bail  
 2 bondsmen, bounty hunters, and prison officials—who routinely access and use the data without  
 3 customer knowledge or consent, and without any emergency 911 basis.

4         5. Defendants’ practices allow Plaintiffs and other AT&T customers to be tracked  
 5 and targeted by unknown third parties without their knowledge. AT&T leverages the technology  
 6 embedded within a customer’s phone and its own network infrastructure to locate its customers  
 7 without any indication that AT&T is tracking them in order to sell their precise location to third  
 8 parties for non-911 purposes. Indeed, AT&T’s practices were only publicly exposed after an FBI  
 9 investigation revealed that a sheriff in Missouri had used carrier location data to stalk a Circuit  
 10 Court Judge and fellow law enforcement officers without their knowledge or consent and without  
 11 any legal authority to do so. This highly sensitive data has also been used to harass AT&T  
 12 customers and bypass the rights afforded by the Fourth Amendment.

13         6. Defendants’ sale of their customers’ real-time location data is a violation of  
 14 Plaintiffs’ reasonable expectations of privacy. Plaintiffs’ expectation is reflected in widely held  
 15 social norms and enshrined in state and federal law, including in the federal Communications  
 16 Act, which requires AT&T to protect customers’ location data precisely because it is in a  
 17 privileged position to know this information as a byproduct of operating a cellular phone service.  
 18 AT&T’s repeated promises to customers that it would safeguard the data from unauthorized  
 19 access and would not sell it only heightens the outrageousness of AT&T’s conduct.

20         7. As Federal Communications Commission Commissioner Geoffrey Starks  
 21 explained in February 2019, “It is absolutely chilling to think that a stranger can buy access to  
 22 exactly where we are at any given moment by tapping into the data on our phones without our  
 23 consent. And, now I am hearing allegations that consumers’ GPS data—data so accurate that it  
 24 can pinpoint your location the floor of a building you are in—is also available for sale. It isn’t  
 25 difficult to imagine intrusive or even downright dangerous uses of this data.”<sup>3</sup>

26  
 27  
 28 <sup>3</sup> See Email from Michael Scurato (FCC) to Joseph Cox (Motherboard) (Feb. 4, 2019), attached  
 hereto as Ex. B.

1           8.       Plaintiffs Katherine Scott, Carolyn Jewel, and George Pontis are California  
2 residents and AT&T wireless customers. Plaintiffs were unaware of and never consented to  
3 Defendants' sale of their real-time location data. To the contrary, Plaintiffs had the reasonable  
4 expectation that their sensitive, real-time location data would be protected and safeguarded by  
5 AT&T, pursuant to federal and state law and AT&T's own promises.

6           9.       Thus, entrusted with its customers' sensitive real-time location data for 911  
7 purposes, and having promised to safeguard that data, AT&T decided instead to profit from that  
8 information. It quietly sold its customers' real-time location data to third-party aggregators  
9 knowing that once sold, that sensitive location data would later enter the marketplace where it  
10 could be used for nefarious purposes. AT&T's conduct is reprehensible and must be stopped.  
11 AT&T must be held accountable.

## 12       **I.     THE PARTIES**

### 13       **A.     The Plaintiffs**

14           10.     Plaintiff Katherine Scott is an active, paying AT&T wireless customer. She is,  
15 and at all relevant times was, a resident of Santa Cruz, California. Plaintiff Scott joined AT&T  
16 approximately nine years ago while residing in California. She pays AT&T every month for her  
17 personal wireless cell phone account, which includes a fee for a limited amount of mobile data  
18 per month. Plaintiff Scott did not—and could not—know that AT&T would sell access to her  
19 real-time location data to third parties, and she at all times expected AT&T to abide by federal  
20 and state laws concerning its privacy practices. Plaintiff Scott relied on AT&T's representations  
21 about its privacy and security policies, and she would not have signed up for AT&T's wireless  
22 service, or would have paid less for the service, had she known about the acts and omissions  
23 described herein.

24           11.     Plaintiff Carolyn Jewel is an active, paying AT&T wireless customer. She is, and  
25 at all relevant times was, a resident of Petaluma, California. Plaintiff Jewel is a long-time AT&T  
26 wireless subscriber. She originally signed up for wireless service with Cellular One in 1999  
27 while residing in California. By May 2006, she was billed by and paid her wireless bills to  
28 Cingular, following changes in corporate ownership. By April 2007, she was billed by and paid

1 her wireless bills to AT&T. Plaintiff Jewel does not recall ever signing any contract with AT&T  
2 following the change in corporate ownership, but has reviewed AT&T's privacy policy, including  
3 AT&T's representations about its data privacy and data sale practices. She pays AT&T every  
4 month for her personal wireless cell phone account. Plaintiff Jewel did not—and could not—  
5 know that AT&T would sell access to her real-time location data to third parties, and she at all  
6 times expected AT&T to abide by federal and state laws concerning its privacy practices.  
7 Plaintiff Jewel relied on AT&T's representations about its privacy and security policies, and she  
8 would not have signed up for AT&T's wireless service, or would have paid less for the service,  
9 had she known about the acts and omissions described herein.

10 12. Plaintiff George Pontis is an active, paying AT&T wireless customer. He is, and  
11 at all relevant times was, a resident of San Mateo County, California. Plaintiff Pontis is a long-  
12 time AT&T wireless subscriber. He originally signed up for wireless service with Cingular  
13 Wireless while residing in California. Cingular Wireless later became a part of AT&T. Plaintiff  
14 Pontis does not recall ever signing any contract with AT&T following the change in corporate  
15 ownership, but relied on AT&T's representations about its data privacy and data sale practices in  
16 maintaining his AT&T account. He pays AT&T every month for his personal wireless cell phone  
17 account, which includes a fee for a limited amount of mobile data per month. Plaintiff Pontis did  
18 not—and could not—know that AT&T would sell access to his real-time location data to third  
19 parties, and he at all times expected AT&T to abide by federal and state laws concerning its  
20 privacy practices. He would not have signed up for AT&T's wireless service, or would have  
21 changed the way he used his phone or paid less for the service, had he known about the acts and  
22 omissions described herein.

23 **B. The AT&T Defendants**

24 13. Defendant AT&T Inc. is a Delaware corporation with its principal office or place  
25 of business in Dallas, Texas. AT&T Inc. transacts or has transacted business in this District and  
26 throughout the United States. It is the second largest wireless carrier in the United States, with  
27  
28

1 more than 153 million subscribers, earning \$160 billion in total operating revenues in 2017 and  
 2 \$170 billion in 2018. As of December 2017, AT&T had 1,470 retail locations in California.<sup>4</sup>

3 14. Defendant AT&T Inc. provides mobile wireless telecommunication services and  
 4 sells mobile wireless handsets to California consumers, including Plaintiffs, through AT&T Inc.  
 5 and its wholly owned subsidiaries, including Defendants AT&T Services, Inc. and AT&T  
 6 Mobility LLC.

7 15. Defendant AT&T Services, Inc. is a Delaware corporation with its principal office  
 8 or place of business in Dallas, Texas. AT&T Services, Inc. transacts or has transacted business in  
 9 this District and throughout the United States.

10 16. AT&T Mobility, LLC is a Delaware limited liability corporation with its principal  
 11 office or place of business in Brookhaven, Georgia. AT&T Mobility provides wireless service to  
 12 subscribers in the United States, Puerto Rico, and the U.S. Virgin Islands. AT&T Mobility is a  
 13 “common carrier” governed by the Federal Communications Act (“FCA”), 47 U.S.C. § 151 *et*  
 14 *seq.* AT&T Mobility is regulated by the Federal Communications Commission (“FCC”) for its  
 15 acts and practices, including those occurring in this District. AT&T Mobility LLC transacts or  
 16 has transacted business in this District and throughout the United States.

17 17. AT&T’s Mobility business unit “provides nationwide wireless services to  
 18 consumers and wholesale and resale wireless subscribers located in the United States or U.S.  
 19 territories” and the Mobility business unit accounted for \$71 billion in revenue in 2017 and  
 20 2018.<sup>5</sup>

21 18. AT&T’s 2018 Annual Report acknowledged that its “profits and cash flow are  
 22 largely driven by [its] Mobility business” and “nearly half of [the] company’s EBITDA (earnings  
 23 before interest, taxes, depreciation and amortization) comes from Mobility.”<sup>6</sup>

#### 24 C. The Aggregator Defendants

26 <sup>4</sup> “About Us,” AT&T, *available at* <https://engage.att.com/california/about-us/>. All URLs in this  
 27 complaint were last accessed on July 9, 2019, unless otherwise noted.

28 <sup>5</sup> *Id.*

<sup>6</sup> “2018 Annual Report,” AT&T, *available at* [https://investors.att.com/~/\\_media/Files/A/ATT-IR/financial-reports/annual-reports/2018/complete-2018-annual-report.pdf](https://investors.att.com/~/_media/Files/A/ATT-IR/financial-reports/annual-reports/2018/complete-2018-annual-report.pdf).

1           19. Defendants TechnoCom Corporation d/b/a LocationSmart (hereafter,  
2 “LocationSmart”) and Zumigo Inc. (hereafter, “Zumigo,” and together with LocationSmart,  
3 “Aggregator Defendants”) are location data aggregators, companies that specialize in the  
4 aggregation and sale of location data for myriad commercial purposes. AT&T used  
5 LocationSmart and Zumigo to manage the buying and selling of its customers’ real-time location  
6 data.<sup>7</sup>

7           20. LocationSmart is a division of Defendant TechnoCom Corporation (hereafter,  
8 “LocationSmart”).<sup>8</sup> TechnoCom Corporation is a Delaware corporation, headquartered in  
9 Carlsbad, California.

10          21. LocationSmart advertises itself as a “a comprehensive location platform[.]”<sup>9</sup> In  
11 2015, LocationSmart merged with Locaid, which was marketed at the time as “the world’s  
12 largest Location-as-a-Service platform for enterprise location[.]”<sup>10</sup> Location-as-a-Service refers  
13 to a “location data delivery model where privacy protected physical location data acquired  
14 through multiple sources including carriers, Wi-Fi, IP addresses and landlines is available to  
15 enterprise customers[.]”<sup>11</sup> LocationSmart and Locaid now operate under the LocationSmart  
16 brand, which advertises itself as the “world’s largest location-as-a-service company.”<sup>12</sup>

17          22. LocationSmart, as a location data aggregator, compiles location information from  
18 numerous sources for use by LocationSmart’s customers. On its website, LocationSmart  
19 advertised that it obtains location data from more than 175 million devices through wireless  
20

21 <sup>7</sup> Letter from Timothy McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (Feb. 15,  
22 2019), *available at* [https://www.documentcloud.org/documents/5767087-AT-T-Response-to-](https://www.documentcloud.org/documents/5767087-AT-T-Response-to-Wyden-on-Phone-Location-Data.html)  
23 [Wyden-on-Phone-Location-Data.html](https://www.documentcloud.org/documents/5767087-AT-T-Response-to-Wyden-on-Phone-Location-Data.html).

24 <sup>8</sup> “TechnoCom Rebrands Platform as LocationSmart,” LocationSmart (April 16, 2012), *available*  
25 *at* [https://www.locationsmart.com/company/news/technocom-rebrands-platform-as-](https://www.locationsmart.com/company/news/technocom-rebrands-platform-as-locationsmart)  
26 [locationsmart](https://www.locationsmart.com/company/news/technocom-rebrands-platform-as-locationsmart).

27 <sup>9</sup> “Home,” LocationSmart, *available at* <https://www.locationsmart.com/>.

28 <sup>10</sup> “LocationSmart and Locaid Announce Merger,” LocationSmart (Feb. 26, 2015), *available at*  
29 <https://www.locationsmart.com/company/news/locationsmart-and-locaid-announce-merger>.

30 <sup>11</sup> “Location as a Service,” Wikipedia, *available at*  
31 [https://en.wikipedia.org/wiki/Location\\_as\\_a\\_service](https://en.wikipedia.org/wiki/Location_as_a_service).

32 <sup>12</sup> “Location Intelligence,” LocationSmart (accessed May 9, 2019), *available at*  
33 <https://www.locationsmart.com/platform/location>.



carriers, and supplements that location data using 1.8 billion WiFi access points, GPS data, three billion IP addresses, and 3.2 billion browsers.<sup>13</sup> LocationSmart advertises to its customers that they can use this information data for various purposes, including “retail, financial services, contact centers, logistics and supply chain, transportation, gaming and roadside assistance among others.”<sup>14</sup>

23. LocationSmart’s relationship with AT&T is critical to LocationSmart’s business model, as it provides LocationSmart with direct access to AT&T customers’ location data. In May 2018, LocationSmart stated that it could “deliver access to more than 400 million mobile devices across the country, reach to over 95 percent of U.S. wireless subscribers and coverage for over 100 million landlines as a result of direct connections with all major carriers. Carrier Network Location allows enterprises to reach all devices with cellular data connections and this includes everything from smartphones and feature phones to tablets and M2M modules.”<sup>15</sup>

24. Upon information and belief, AT&T gave LocationSmart explicit and implied authority to act on AT&T’s behalf in accessing AT&T customers’ location data.

25. LocationSmart also works with carriers like AT&T to test, monitor, and report on location data accuracy for 911 emergency purposes.<sup>16</sup>

26. Defendant Zumigo is a California corporation headquartered in San Jose, California. Zumigo was founded in 2008 “with a mission to enable and secure commerce using Mobile networks.”<sup>17</sup> AT&T used Zumigo to manage the buying and selling of its customers’ real-time location data.<sup>18</sup>

---

<sup>13</sup> *Id.*

<sup>14</sup> “LocationSmart and Carrier Network Location,” LocationSmart, *available at* <https://www.locationsmart.com/resources/carrier-network-location>.

<sup>15</sup> “Carrier Network Location Collateral,” LocationSmart (archived from May 12, 2018), attached hereto as Ex. C.

<sup>16</sup> “Carrier Services,” LocationSmart, *available at* <https://www.locationsmart.com/platform/carrier-services>.

<sup>17</sup> Snehashis Khan, “Securing Transactions and Customer Applications Through Location,” Zumigo Inc. (Jan. 2017), *available at* <https://geospatialworldforum.org/speaker/SpeakersImages/securing-transactions-and-customer-applications-through-location.pdf>.

<sup>18</sup> Letter from Timothy McKone to U.S. Senator Ron Wyden (Feb. 15, 2019), *supra* at 7.

1           27.     Critical to Zumigo’s business model is its direct access to AT&T customers’  
 2 location data. Zumigo markets itself as “a trusted partner of mobile providers, credit bureaus,  
 3 financial institutions, and retail merchants”<sup>19</sup> and advertises its ability to “[r]oute traffic over the  
 4 cellular network” and utilize “realtime user identity information.”<sup>20</sup>

5           28.     Upon information and belief, AT&T gave Zumigo explicit and implied authority  
 6 to act on AT&T’s behalf in accessing AT&T customers’ location data.

7           29.     Each of the Aggregator Defendants work as an agent of AT&T. On information  
 8 and belief, AT&T and each of the Aggregator Defendants has a relationship wherein AT&T has  
 9 the right to control which third parties each Aggregator Defendant may provide with access to  
 10 AT&T’s customer location data. On information and belief, AT&T gives each Aggregator  
 11 Defendant the right to contract with third parties to access AT&T location data on AT&T’s  
 12 behalf.

13           30.     AT&T, LocationSmart, and Zumigo are collectively referred to herein as  
 14 “Defendants.”

## 15     **II.     JURISDICTION AND VENUE**

16           31.     This Court has jurisdiction over this matter under 28 U.S.C. § 1331 because this  
 17 case arises under federal question jurisdiction under the Federal Communications Act (“FCA”).  
 18 The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state law claims  
 19 because the claims are derived from a common nucleus of operative facts. The Court also has  
 20 jurisdiction over this action pursuant to 28 U.S.C. § 1332 because this is a class action in which  
 21 the matter or controversy exceeds the sum of \$5,000,000, exclusive of interests and costs, and in  
 22 which some members of the proposed Class are citizens of a different state than Defendants.

23           32.     This Court has personal jurisdiction over Defendants because Defendants  
 24 purposefully direct their conduct at California, transact substantial business in California  
 25 (including in this District), have substantial aggregate contacts with California (including in this  
 26 District), engaged and are engaging in conduct that has and had a direct, substantial, reasonably  
 27

28 <sup>19</sup> “Company,” Zumigo, *available at* <https://zumigo.com/company/>.

<sup>20</sup> “Solutions,” Zumigo, *available at* <https://zumigo.com/solutions/>.

foreseeable, and intended effect of causing injury to persons throughout the United States, including those in California (including in this District), and purposely avail themselves of the laws of California. Each of the Plaintiffs paid for AT&T services within the state, and each was injured in California where they reside. AT&T had more than 33,000 employees in California as of 2017, and 1,470 retail locations in the state.<sup>21</sup> Additionally, Defendants Zumigo and LocationSmart are headquartered in and/or have principal places of business in California.

33. In accordance with 28 U.S.C. § 1391, venue is proper in this district because a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District and Defendants transact business in this District.

### III. DIVISION ASSIGNMENT

34. Pursuant to Civil L.R. 3-2(c), assignment to this Division is proper because a substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this District. Defendants market their products throughout the United States, including in San Francisco and Alameda counties.

### IV. ALLEGATIONS APPLICABLE TO ALL COUNTS

#### A. AT&T Has Access to Its Customers' Real-Time Location Data by Virtue of Operating a Mobile Cellular Phone Network.

35. By virtue of operating a mobile phone network, AT&T knows its customers' real-time locations because it has to collect that information to provide service to its customers' cellular phones.

36. Cellular phone networks work by routing phone calls, text messages, and data for email messages, Internet browsing, mobile applications, and other operations from a network of fixed towers containing antennas to an individual customer's cell phone.

37. To receive information from fixed towers, cell phones scan their surroundings and connect with the towers providing the best signal, which are often the ones that are physically closest to the phones.

---

<sup>21</sup> "About Us," AT&T, *supra* at 4.

38. Cell phones are designed to continuously scan and connect with the cell tower providing the best signal, and they perform this task in the background without the customer's knowledge or direction. Each time a phone connects to a tower, there is a record created that details exactly when a particular cell phone connected to a fixed cellular tower, and to which tower.

39. Depending on the area and the number of cell towers present, the data can provide the real-time location of a customer's cell phone to within 50 meters.

40. Because AT&T operates a mobile phone network, it obtains troves of this precise real-time location data around the clock for each device used by every customer on its network.

**B. Public Reports Reveal AT&T's Sale of Access to Its Customers' Real-Time Location Data, and the Rampant Abuses Flowing from Such Sale.**

41. AT&T's and the Aggregator Defendants' sale of Plaintiffs' and all other AT&T wireless customers' location data was unknown to Plaintiffs and the public at large until it began to be revealed in media reports in 2018 and 2019.

**i. May 2018 Reporting Reveals AT&T's Sale of Customer Location Data to Prison Officials.**

42. In May 2018, The New York Times reported that AT&T was selling access to its customers' real-time location data to a company called Securus Technologies, Inc. ("Securus"), a company that contracts with prisons and jails to be provide inmate communication services at those facilities.<sup>22</sup>

43. Securus was obtaining access to AT&T customers' location data through intermediaries Defendant LocationSmart and a company called "3Cinteractive."<sup>23</sup> LocationSmart contracted with AT&T and had direct access to AT&T customers' real-time location data. With AT&T's permission and knowledge, LocationSmart then served as a conduit

<sup>22</sup> Jennifer Valentino-DeVries, "Service Meant to Monitor Inmates' Calls Could Track You, Too," THE NEW YORK TIMES (May 10, 2018), *available at* <https://www.nytimes.com/2018/05/10/technology/cellphone-tracking-law-enforcement.html>.

<sup>23</sup> *Id.*

1 between AT&T and hundreds of third parties—including Securus and 3Cinteractive—seeking to  
2 use AT&T customers’ location data for various commercial purposes.<sup>24</sup>

3 44. Securus went on to sell its access to AT&T customers’ location data to thousands  
4 of third parties, including local law enforcement. Figure 1 immediately below illustrates the  
5 flow of customer location information.



8  
9 *Figure 1*

10 45. This data-sharing arrangement allowed countless unknown individuals to obtain  
11 unauthorized access to AT&T customers’ real-time location data. For example, a Securus  
12 customer, former sheriff Corey Hutcheson, used carrier location data to target and track  
13 individuals’ real-time locations—including the location of a Missouri state judge and several  
14 members of law enforcement—over the course of three years, without their consent or  
15 knowledge and without legal authority to do so.<sup>25</sup>

16 46. Corey Hutcheson had access to Securus’ location services beginning in at least  
17 2014.<sup>26</sup> That same year, the FBI began investigating Hutcheson for using his access to Securus’  
18 online web portal to illegally track the location of cell phones, including the phones of a former  
19 sheriff, five state troopers, and Circuit Judge David Dolan.<sup>27</sup> The allegations raised suspicions  
20 among lawyers that Hutcheson had been using the same technology to target local suspects.<sup>28</sup>  
21 Indeed, federal authorities allege that Hutcheson “submitted *thousands* of Securus [location  
22 services] requests and obtained the location data of individual phone subscribers without valid

23 <sup>24</sup> *Id.*

24 <sup>25</sup> *Id.*

25 <sup>26</sup> See Superseding Indictment, *U.S. v. Hutcheson*, No. 1:18-cr-00041-JAR (E.D. Mo. Aug. 17, 2018) (hereafter “Hutcheson Indictment”), Dkt. No. 33 at ¶ 15.

26 <sup>27</sup> Doyle Murphy, “Sheriff Cory Hutcheson Vowed to Clean Up His Rural Missouri County. Now He’s the One Facing Prison,” *Riverfront Times* (Apr. 26, 2018), *available at*  
27 <https://www.riverfronttimes.com/stlouis/sheriff-cory-hutcheson/Content?oid=4857359&showFullText=true>.

28 <sup>28</sup> *Id.*

1 legal authorization, and, often, without the consent or even knowledge of the targeted  
2 individual.”<sup>29</sup>

3 47. Federal authorities alleged that Hutcheson had obtained access to individuals’  
4 location data by routinely uploading random documents to the Securus web portal and claiming  
5 that those documents constituted legal authority authorizing him to access other individuals’  
6 precise location data.<sup>30</sup> On the basis of those documents, Securus then provided Hutcheson with  
7 individuals’ real-time, precise location data, which was determined using their cell carriers’  
8 technology and access to their phones.<sup>31</sup>

9 48. After AT&T’s location data sharing arrangement and the resulting abuses were  
10 revealed, U.S. Senator Ron Wyden wrote a letter to AT&T Inc.’s CEO, Randall L. Stephenson.<sup>32</sup>  
11 Senator Wyden informed AT&T that it was “prohibited from sharing certain customer  
12 information, including location data, unless the carrier either has the customer’s consent or  
13 sharing is otherwise required by law” and that AT&T must “ensure surveillance of  
14 communications and call records using their facilities can only be conducted *with the direct and*  
15 *specific oversight of the provider*.”<sup>33</sup>

16 49. The fact that Securus was able to provide the location service at all, Senator  
17 Wyden stated, “suggests that AT&T does not sufficiently control access to ... customers’ private  
18 information.”<sup>34</sup> The Senator stated that no company should be able to provide customers’ private  
19 information directly to law enforcement “without AT&T’s active oversight and direction.”<sup>35</sup>

20 50. Senator Wyden also wrote to the FCC, asking the agency to “investigate abusive  
21 and potentially unlawful practices of wireless carriers” regarding their sale of access to  
22

23 <sup>29</sup> Hutcheson Indictment at ¶ 26.

24 <sup>30</sup> *Id.* at ¶¶ 19-23.

25 <sup>31</sup> *Id.* at ¶ 25.

26 <sup>32</sup> Letter from U.S. Senator Ron Wyden to Randall L. Stephenson (AT&T) (May 8, 2018),  
available at <https://www.documentcloud.org/documents/4457319-Wyden-Securus-Location-Tracking-Letter-to-AT-amp-T.html>.

27 <sup>33</sup> *Id.* (emphasis added).

28 <sup>34</sup> *Id.*

<sup>35</sup> *Id.*

1 customers' real-time location data.<sup>36</sup> Senator Wyden asserted that Securus granted law  
 2 enforcement access to the location of "any U.S. wireless phone number" if the official uploaded  
 3 "a document purporting to be an 'official document giving permission'" to access the data.<sup>37</sup>  
 4 But, as demonstrated by Sheriff Hutcheson's submissions, those documents need not *actually*  
 5 confer any legal authority at all before location data would be provided. Senator Wyden warned  
 6 that the carriers' practice of selling customer location data without determining whether there  
 7 was consent or legal authority for such access "needlessly exposes millions of Americans to  
 8 potential abuse and surveillance by the government."<sup>38</sup>

9 51. The risk that the routine sale of customers' location data presents to the public is  
 10 exemplified by Sheriff Hutcheson's tracking of judicial officials, law enforcement, and suspects.

11 52. The vulnerability of AT&T customers' location data is further illustrated by a  
 12 breach of the Securus server.<sup>39</sup> In May 2018, a hack on Securus' server exposed data concerning  
 13 thousands of Securus customers, including their login information and passwords, thereby  
 14 exposing AT&T customers' location data to countless unknown third parties.<sup>40</sup>

15 53. Strikingly, the Securus hacker reported that gaining access to AT&T's highly  
 16 sensitive location information for *millions of its customers* was "relatively simple."<sup>41</sup>

17 54. The very same day that the Securus hack was reported, a security researcher at  
 18 Carnegie Mellon University identified a security flaw in Aggregator Defendant LocationSmart's  
 19 online demonstration, which allowed any member of the public to obtain real-time location  
 20 information for AT&T customers, without the customers' knowledge or consent.<sup>42</sup> The

21 <sup>36</sup> Letter from U.S. Senator Ron Wyden to Chairman Ajit Pai (FCC) (May 8, 2018), *available at*  
 22 <https://www.wyden.senate.gov/imo/media/doc/wyden-securus-location-tracking-letter-to-fcc.pdf>.

23 <sup>37</sup> *Id.*

24 <sup>38</sup> *Id.*

25 <sup>39</sup> Joseph Cox, "Hacker Breaches Securus, the Company That Helps Cops Track Phones Across  
 the US," MOTHERBOARD (May 16, 2018), *available at*  
 26 [https://motherboard.vice.com/en\\_us/article/gykgv9/securus-phone-tracking-company-hacked](https://motherboard.vice.com/en_us/article/gykgv9/securus-phone-tracking-company-hacked).

27 <sup>40</sup> *Id.*

28 <sup>41</sup> *Id.*

<sup>42</sup> Brian Krebs, "Tracking Firm LocationSmart Leaked Location Data for Customers of All  
 Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site," KREBS ON  
 SECURITY (May 17, 2018), *available at* <https://krebsonsecurity.com/2018/05/tracking-firm->

1 researcher, Robert Xiao, had reportedly become interested in LocationSmart following reports  
2 that LocationSmart was supplying Securus with access to carrier customer location data.<sup>43</sup>

3 55. At the time of the hack, LocationSmart had a free demonstration on its website for  
4 potential customers (such as Securus) to try out its location targeting technology. LocationSmart  
5 claimed it could provide the precise location of almost any cell phone in the United States using  
6 location data from major cellphone carriers, including AT&T.<sup>44</sup> The demo, which was available  
7 to the public through LocationSmart's website, was supposed to seek consent from the targeted  
8 cell phone user via text message before supplying the location data.<sup>45</sup>

9 56. However, LocationSmart failed to properly protect the data used in the demo,  
10 thereby allowing "[a]nyone with a modicum of knowledge about how Web sites work [to] abuse  
11 the LocationSmart demo site to figure out how to conduct mobile number location lookups at  
12 will, *all without ever having to supply a password or other credentials.*"<sup>46</sup> With "minimal  
13 effort," Mr. Xiao was able to bypass the demo's text message consent structure, unlocking the  
14 ability to obtain any AT&T customer's location data *without the customer's consent or*  
15 *knowledge.*<sup>47</sup> This unsecured demo had been publicly accessible on LocationSmart's website for  
16 approximately 16 or 17 months.<sup>48</sup>

17 57. In response to reporting about Securus and LocationSmart, AT&T admitted that  
18 Securus "did not in fact obtain customer consent before collecting customers' location  
19 information" and claimed that, as a result, AT&T had "suspended all access by Securus to AT&T  
20 customer location data."<sup>49</sup>

21 [locationsmart-leaked-location-data-for-customers-of-all-major-u-s-mobile-carriers-in-real-time-](#)  
22 [via-its-web-site/](#).

23 <sup>43</sup> *Id.*

24 <sup>44</sup> *Id.*

25 <sup>45</sup> *Id.*

26 <sup>46</sup> *Id.* (emphasis added).

27 <sup>47</sup> *Id.* (emphasis added).

28 <sup>48</sup> *Id.*

<sup>49</sup> Brian Krebs, "AT&T, Sprint, Verizon to Stop Sharing Customer Location Data with Third Parties," KREBS ON SECURITY (June 19, 2018), [available at https://krebsonsecurity.com/2018/06/verizon-to-stop-sharing-customer-location-data-with-third-parties/](https://krebsonsecurity.com/2018/06/verizon-to-stop-sharing-customer-location-data-with-third-parties/).



1           58.     AT&T also claimed that Securus—rather than AT&T—was responsible for  
 2     securing a customer’s consent before sharing their real-time, precise location data.<sup>50</sup> AT&T  
 3     stated that it had taken “prompt steps to protect customer data”<sup>51</sup> and that its “top priority is to  
 4     protect our customers’ information and, to that end, [it would] be ending [its] work with  
 5     aggregators for these services as soon as practical in a way that preserves important, potential  
 6     lifesaving services like emergency roadside assistance.”<sup>52</sup> Each of these statements was false  
 7     and/or misleading, as fully alleged below.

8                   **ii.     June 2018 Reporting Reveals AT&T’s Sale of Customer Location Data**  
 9                   **to Additional Third Parties.**

10           59.     By June 2018, reporting made clear that AT&T was not just selling its customer  
 11     location data to prison officials and law enforcement for illegal and unauthorized use, but was  
 12     also selling the data on a much larger scale for much broader purposes.

13           60.     Just a few days after AT&T announced that it would stop selling customer data to  
 14     Securus and the Aggregator Defendants, reporting revealed that AT&T customers’ location data  
 15     was being sold to bail bondsmen, bounty hunters, landlords, and numerous other third parties for  
 16     wide-ranging commercial purposes.<sup>53</sup>

17           61.     Bounty hunters and bail bondsmen were accessing carrier customers’ real-time  
 18     location data through a third party (similar to Securus) called “Captira”— which advertised that it

19     <sup>50</sup> *Id.*

20     <sup>51</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
 21     2018), *available at* <https://www.wyden.senate.gov/imo/media/doc/at&t%20letter%20to%20RW%206.15.pdf>.

22     <sup>52</sup> Jon Brodtkin, “Verizon and AT&T Will Stop Selling Your Phone’s Location to Data Brokers,”  
 23     ARS TECHNICA (June 19, 2018), *available at* [https://arstechnica.com/tech-](https://arstechnica.com/tech-policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/)  
 24     [policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/](https://arstechnica.com/tech-policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/); Brian  
 25     Fung, “Verizon, AT&T, T-Mobile and Sprint Suspend Selling of Customer Location Data After  
 26     Prison Officials Were Caught Misusing It,” THE WASHINGTON POST (June 19, 2018), *available*  
 27     [at https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-](https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/?noredirect=on&utm_term=.4f7da64c1108)  
 28     [of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-](https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/?noredirect=on&utm_term=.4f7da64c1108)  
 29     [it/?noredirect=on&utm\\_term=.4f7da64c1108](https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/?noredirect=on&utm_term=.4f7da64c1108).

30     <sup>53</sup> Joseph Cox, “Bail Bond Company Let Bounty Hunters Track Verizon, T-Mobile, Sprint, and  
 31     AT&T Phones for \$7.50,” MOTHERBOARD (June 22, 2018), *available at* [https://motherboard.vice.com/en\\_us/article/9k873e/captira-phone-tracking-verizon-tmobile-](https://motherboard.vice.com/en_us/article/9k873e/captira-phone-tracking-verizon-tmobile-sprint-securus-locationsmart-bounty-hunters)  
 32     [sprint-securus-locationsmart-bounty-hunters](https://motherboard.vice.com/en_us/article/9k873e/captira-phone-tracking-verizon-tmobile-sprint-securus-locationsmart-bounty-hunters).

1 could track the location of all major carriers' cell phones (including phones in the AT&T  
2 network), to an accuracy of *2 meters*.<sup>54</sup>

3 62. Captira publicly advertised that bounty hunters had used its cell phone location  
4 services to track people across state lines.<sup>55</sup> But by 2018, Captira had removed all references to  
5 its location services from its website, and the article's sources claimed that companies with  
6 access to AT&T location data had stopped advertising their location services in 2014 or 2015 out  
7 of concern that the services were illegal.<sup>56</sup>

8 **iii. January 2019 Reporting Reveals AT&T's Customer Location Data**  
9 **Sales Are Ongoing.**

10 63. In January 2019, nearly *seven months* after AT&T had promised to stop selling  
11 information to the Aggregator Defendants, another media report revealed that AT&T was *still*  
12 selling access to customers' precise, real-time location data to location aggregators and allowing  
13 the highly-sensitive data to be bought from bounty hunters and bail bondsmen for as little as  
14 \$300.<sup>57</sup>

15 64. This new reporting further revealed that AT&T had been providing—and  
16 continued to provide—access to real-time customer location data for almost every cell phone in  
17 the United States to a robust and shadowy downstream market, all without the cell phone user's  
18 consent or knowledge.<sup>58</sup>

19 65. Reporting showed that, once again, AT&T customer location data was available to  
20 numerous industries—"ranging from car salesmen and property managers to bail bondsmen and  
21 bounty hunters"—through a chain of third parties that began with AT&T and Aggregator  
22  
23

24 <sup>54</sup> *Id.* (emphasis added).

25 <sup>55</sup> *Id.*

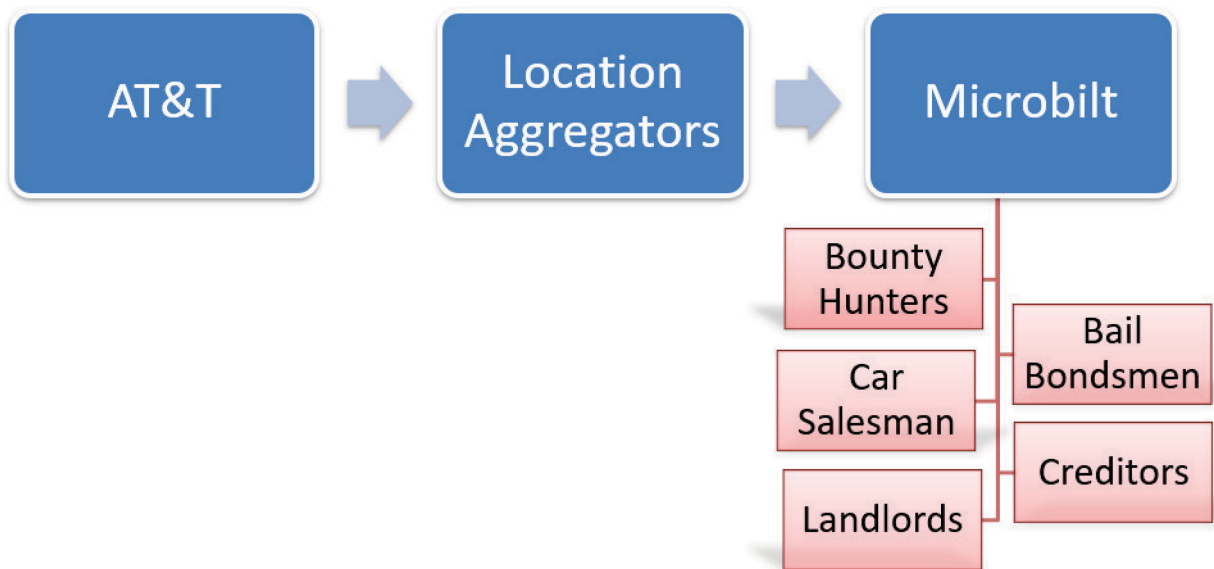
26 <sup>56</sup> *Id.*

27 <sup>57</sup> Joseph Cox, "I Gave a Bounty Hunter \$300. Then He Located Our Phone," MOTHERBOARD  
(Jan. 8, 2019), available at [https://motherboard.vice.com/en\\_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile](https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile).

28 <sup>58</sup> *Id.*

Defendant Zumigo. Zumigo then sold the data to a company called Microbilt.<sup>59</sup> AT&T confirmed that it had approved Zumigo's sale of its customers' data to Microbilt.<sup>60</sup>

66. Microbilt, in turn, sold the AT&T location data "to a dizzying number of sectors, including landlords to scope out potential renters; motor vehicle salesmen, and others who are conducting credit checks."<sup>61</sup> Figure 2 immediately below further illustrates the flow of customer location information.



*Figure 2*

67. These industries used Microbilt's services to "return a target's full name and address, geolocate a phone in an individual instance, or operate as a continuous tracking service."<sup>62</sup> As Microbilt advertised to its clients, "[y]ou can set up monitoring with control over the weeks, days and even hours that location on a device is checked as well as the start and end dates of monitoring."<sup>63</sup>

68. Included among Microbilt's customers are bail bondsmen and bounty hunters.

<sup>59</sup> *Id.*

<sup>60</sup> *Id.*

<sup>61</sup> *Id.*

<sup>62</sup> *Id.*

<sup>63</sup> *Id.*

69. In one January 2019 report, a journalist was able to find the real-time location of a phone in Queens, New York, within an accuracy of just a few blocks, by buying location data from Microbilt through a bounty hunter.<sup>64</sup> But for the reporter personally informing the phone's owner that he would be using the technology to locate her, no consent was obtained by the bounty hunter before locating the phone. The phone's owner was never informed by her carrier, the location aggregator, or the bounty hunter that her real-time location data would be or had been accessed, nor was her consent requested to do so. None of them provided her with a text message, alert, notification, or indeed *any* indication at all that they had accessed her phone and targeted her location: their access was completely invisible to her.<sup>65</sup>

70. Just as access to the carrier location data was passed down a chain, so too was the proclaimed responsibility for obtaining customer consent before accessing that data. Both the carriers and the Aggregator Defendants claimed that they required their clients "to get consent from the people they want to track," rather than obtain any direct consent themselves.<sup>66</sup>

71. A bail industry employee who used Microbilt to access cell carrier location data confirmed that the lack of a true consent structure for the real-time location data allowed the data to be used for nefarious purposes, such as allowing bounty hunters to "track[] their girlfriends."<sup>67</sup> It also allowed for a robust, unregulated black market of the data to develop. According to the source, "[t]hose third-level companies sell their services. That is where you see the issues with going to shady folks [and] for shady reasons."<sup>68</sup>

72. AT&T admitted that use of its customers' data by bounty hunters was an explicit breach of the company's policies.<sup>69</sup> However, AT&T attempted to downplay the importance of the Securus and Microbilt breaches as isolated events.

---

<sup>64</sup> *Id.*

<sup>65</sup> *Id.*

<sup>66</sup> *Id.*

<sup>67</sup> *Id.*

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*

73. In response to this latest round of reporting, fifteen U.S. senators called for an investigation into how AT&T and other wireless carriers were selling access to real-time customer location data.<sup>70</sup> Their letter stated: “It is clear that these wireless carriers have failed to regulate themselves or police the practices of their business partners, and have needlessly exposed American consumers to serious harm.”

**iv. February 2019 Reporting Reveals Scope and Nature of AT&T’s Sale of Customer Location Data to Bounty Hunters.**

74. On February 6, 2019, public reporting revealed both the large scale of cell carriers’ sale of access to their customers’ location data to bounty hunters and that AT&T was allowing the sale of a particularly precise type of location data.<sup>71</sup>

75. This round of reporting centered largely on a bail bond and bounty hunter company called CerCareOne. CerCareOne obtained access to carrier-level location data, including data from AT&T, through LocationSmart.<sup>72</sup>

76. As industry documents confirm, CerCareOne sold its access to more than 250 *bounty hunters and related businesses between 2012 and 2017*.<sup>73</sup> These companies were conducting thousands of searches for customers’ precise geolocation data (these searches are often called “pings”), with one bail bond company making more than *18,000 data requests*.

<sup>70</sup> Letter from United States Senators Ron Wyden, Edward J. Markey, Kamala D. Harris, Jeffrey A. Merkley, Sheldon Whitehouse, Charles E. Schumer, Richard Blumenthal, Patrick Leahy, Benjamin L. Cardin, Amy Klobuchar, Kirsten Gillibrand, Cory A. Booker, Jack Reed, Tina Smith, and Bernard Sanders to Joseph J. Simons (FTC) and Ajit Pai (FCC) (Jan. 24, 2019), *available at* <https://www.wyden.senate.gov/imo/media/doc/15-senators-location-aggregator-letter-to-fcc-ftc-final.pdf>.

<sup>71</sup> Joseph Cox, “Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls,” MOTHERBOARD (Feb. 6, 2019), *available at* [https://motherboard.vice.com/en\\_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls](https://motherboard.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls); Joseph Cox, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years,” MOTHERBOARD (Feb. 6, 2019), *available at* [https://motherboard.vice.com/en\\_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years](https://motherboard.vice.com/en_us/article/43z3dn/hundreds-bounty-hunters-att-tmobile-sprint-customer-location-data-years).

<sup>72</sup> Joseph Cox, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years,” *supra* at 71.

<sup>73</sup> *Id.*

1           77. This latest round of reporting also revealed that AT&T was selling access to a  
 2 particularly sensitive type of location data: “assisted GPS” or “A-GPS” data. A-GPS location is  
 3 determined using the carrier’s network infrastructure, the phone’s GPS chip, and other  
 4 technologies such as WiFi and Bluetooth. The combination can locate customers with finely-  
 5 tuned accuracy, often revealing their location *within* a building. A-GPS data is intended to be  
 6 used to help locate carrier customers when they called 911. LocationSmart confirmed that it was  
 7 in fact using A-GPS data for location tracking.<sup>74</sup>

8           78. As Colorado Law Associate Professor Blake Reid explained, “with assisted GPS,  
 9 your location can be triangulated within just a few meters. This allows constructing a detailed  
 10 record of everywhere you travel.”<sup>75</sup>

11           79. Bounty hunters bought carrier-level location data for as much as \$1,100 per ping,  
 12 and confirmed that they were reselling the location data to additional third parties.<sup>76</sup> The  
 13 articles’ sources confirmed that targeted individuals receive no text message or other warning  
 14 that their phones are being tracked.<sup>77</sup>

15           80. The companies selling access to carrier location data were attempting to keep the  
 16 sale of this data a secret.<sup>78</sup> As a condition of access to the data, CerCareOne required its  
 17 customers to agree to keep its very existence confidential.<sup>79</sup> It also designed a misleading  
 18 website: its homepage stated that the site was “under construction,” but a back-end portal  
 19 allowed its customers to log in and access call carrier customer location data.<sup>80</sup>  
 20  
 21  
 22  
 23

---

24 <sup>74</sup> *Id.*

25 <sup>75</sup> *Id.*

26 <sup>76</sup> *Id.*

27 <sup>77</sup> *Id.*

28 <sup>78</sup> *Id.*

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

1           81. In March 2019, Senator Wyden wrote to executives at AT&T, stating it was “now  
2 abundantly clear that [they] have failed to be good stewards of [their] customers’ private location  
3 information.”<sup>81</sup>

4           82. In sum, between May 2018 and March 2019, media reports revealed the existence  
5 of a vast, illegal market for the real-time location data of AT&T customers. AT&T granted direct  
6 access to this data to the Aggregator Defendants, who in turn sold such access to hundreds of  
7 third parties—including bounty hunters, bail bondsmen, landlords, and law enforcement—with  
8 AT&T’s consent. This system allowed the precise, real-time location data of millions of  
9 Americans to be bought and sold by unknowable third parties for years without customer consent  
10 or knowledge and without valid legal authority. Despite numerous representations by AT&T that  
11 it would end the Aggregator Defendants’ access to this data, the practice—and the risks it  
12 created—continued without consequence.

13           **C. Defendants Developed and Profit from a Robust Market for Customers’**  
14           **Real-Time Location Data.**

15           83. Unauthorized individuals gained access to AT&T customers’ real-time location  
16 data without consent or legal authority because of AT&T’s practice of selling access to this data  
17 to data aggregators and hundreds of additional third parties without properly protecting the data  
18 or establishing sufficient safeguards and consent mechanisms. As a result, downstream  
19 purchasers have been able to systematically gain improper access to real-time customer location  
20 data without customer knowledge or consent, and without valid legal authority for such access.

21           84. Beginning at the latest in January 2011, AT&T began using data location  
22 aggregators to manage the buying and selling of its customers’ real-time location data.<sup>82</sup>

23  
24  
25 <sup>81</sup> Letter from U.S. Senator Ron Wyden to Michel Combes (Sprint Corp.), Randall L. Stephenson  
26 (AT&T Inc.), John Legere (T-Mobile US, Inc.), and Hans Vestberg (Verizon Communications  
27 Inc.) (Mar. 13, 2019), *available at* [https://www.documentcloud.org/documents/5767085-Wyden-](https://www.documentcloud.org/documents/5767085-Wyden-Letter-to-Telecoms-March-13th-2019.html)  
28 [Letter-to-Telecoms-March-13th-2019.html](https://www.documentcloud.org/documents/5767085-Wyden-Letter-to-Telecoms-March-13th-2019.html).

<sup>82</sup> Aaron Huff, “AT&T Offers New Tracking Platform,” CCJ Digital (archived from Jan. 4, 2011), attached hereto as Ex. D.

1           85. In October 2011, LocationSmart (then known as Locaid) announced “AT&T’s  
2 adoption of [its] platform” and marketed its ability to “access location for 360 million mobile  
3 and landline devices nationwide.”<sup>83</sup> That same year, LocationSmart claimed its “crosscarrier  
4 web services platform provides instant access to nearly 90% of mobile and landline phones  
5 nationwide, including smart phones, feature phones and tablets.”<sup>84</sup>

6           86. In 2019, AT&T confirmed that it contracted with Aggregator Defendants  
7 LocationSmart and Zumigo.<sup>85</sup>

8           87. Upon information and belief, the Aggregator Defendants were given access to  
9 AT&T’s networks and infrastructure pursuant to their relationships with AT&T, allowing them to  
10 *directly access* the location data of AT&T’s customers.<sup>86</sup>

11           88. In October 2012, LocationSmart advertised that it “connects directly to all major  
12 nationwide carriers as a trusted aggregator of device location. . . . Let me share a little secret . . .  
13 you have immediate access to virtually all subscribers with minimal development.”<sup>87</sup>  
14  
15

16 <sup>83</sup> “AT&T Mobility leverages TechnoCom’s cross-carrier location platform as a key offering for  
17 its enterprise customers,” LocationSmart (Oct. 11, 2011), *available at*  
18 [https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-](https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-location-information-services)  
19 [location-information-services](https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-location-information-services); *see also* “San Diego Company, TechnoCom, Powers AT&T’s  
20 Location Information Services,” LocationSmart (Oct. 11, 2011), *available at*  
21 [https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-](https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-location-information-services)  
22 [location-information-services](https://www.locationsmart.com/company/news/san-diego-company-technocom-powers-atts-location-information-services); Letter from Timothy McKone (AT&T Services, Inc.) to U.S.  
23 Senator Ron Wyden (June 15, 2018), *supra* at 51.

24 <sup>84</sup> “Angel and TechnoCom Optimize Customer Experience with Cloud-Based Caller Location,”  
25 LocationSmart (Oct. 11, 2011), *available at*  
26 [https://www.locationsmart.com/company/news/angel-and-technocom-optimize-customer-](https://www.locationsmart.com/company/news/angel-and-technocom-optimize-customer-experience-with-cloud-based-caller-location)  
27 [experience-with-cloud-based-caller-location](https://www.locationsmart.com/company/news/angel-and-technocom-optimize-customer-experience-with-cloud-based-caller-location).

28 <sup>85</sup> Letter from Timothy McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (Feb. 15),  
2019, *supra* at 7.

<sup>86</sup> LocationSmart claimed that it first established “direct carrier connections” in 2010.  
“LocationSmart Authorized to Deliver Location Data for iGaming in New Jersey,”  
LocationSmart (Nov. 27, 2013), *available at*  
[https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-](https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-location-data-for-igaming-in-new-jersey)  
[location-data-for-igaming-in-new-jersey](https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-location-data-for-igaming-in-new-jersey).

<sup>87</sup> “LocationSmart Capabilities,” LocationSmart (archived from Oct. 31, 2012), attached hereto  
as Ex. E.



1           89. In 2013, LocationSmart advertised that it had “*direct mobile carrier connections*  
2 covering over 90% of subscribers nationwide for secure mobile phone location and messaging  
3 services” and that its platform “*utilizes direct network connections* to obtain secure cellular and  
4 assisted GPS location insight.”<sup>88</sup>

5           90. This direct access provided the Aggregator Defendants with immediate access to  
6 precise, real-time location data.

7           91. In 2018, LocationSmart advertised its ability to locate cell customers’ cell phones  
8 in 5 to 20 seconds, depending on the level of accuracy purchased.<sup>89</sup> “Network-based locates  
9 may be requested by accuracy desired. Precise, Coarse, or Best Effort requests may be made,”  
10 LocationSmart explained. “Precise requests are ≤300 meter accuracy; Coarse requests are >301  
11 meters and Best Available provides the best location possible.”<sup>90</sup>

12           92. In 2017, Zumigo advertised that it “[l]ocates a mobile phone using **mobile**  
13 **networks** – No app needed, no barriers to adoption!”<sup>91</sup> It explained that in order to locate carrier  
14 customers, it “queries mobile network and seeks location [latitude-longitude] of customer” and  
15 then “converts customer [latitude-longitude] to physical location[.]”<sup>92</sup>

16           93. Once the Aggregator Defendants obtained direct access to AT&T customers’ real-  
17 time location data, they began selling access to that location data to their own customers.

18           i. For example, Aggregator Defendant LocationSmart provided Securus  
19 with location data utilizing AT&T data.<sup>93</sup> Securus, in turn, contracted with thousands of different  
20

21           <sup>88</sup> “LocationSmart Authorized to Deliver Location Data for iGaming in New Jersey,”  
22 LocationSmart (Nov. 27, 2013), *available at*  
23 [https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-](https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-location-data-for-igaming-in-new-jersey)  
24 [location-data-for-igaming-in-new-jersey](https://www.locationsmart.com/company/news/locationsmart-authorized-to-deliver-network-location-data-for-igaming-in-new-jersey) (emphasis added).

25           <sup>89</sup> “FAQs,” LocationSmart, *available at* [https://www.locationsmart.com/cms/resources/faqs-](https://www.locationsmart.com/cms/resources/faqs-2018.pdf)  
26 [2018.pdf](https://www.locationsmart.com/cms/resources/faqs-2018.pdf).

27           <sup>90</sup> *Id.*

28           <sup>91</sup> Snehashis Khan, “Securing Transactions and Customer Applications through Location,” *supra*  
at 17 (emphasis in original).

<sup>92</sup> *Id.*

<sup>93</sup> Jennifer Valentino-DeVries, “Service Meant to Monitor Inmates’ Calls Could Track You,  
Too,” *supra* at 22.

1 clients, including detention centers, to provide inmate communications services.<sup>94</sup> While  
 2 Securus' main business was monitoring where inmates were located when they placed calls, it  
 3 offered an additional location data service (which it referred to as its "Location Based Service"  
 4 or "LBS").<sup>95</sup> In order to locate individuals through LBS, Securus granted prisons and jails  
 5 access to a web portal where they could request real-time location data, which was determined  
 6 using carrier-level technology.<sup>96</sup> This service was provided through intermediaries between the  
 7 cell carriers and Securus, including LocationSmart and 3Cinteractive.<sup>97</sup>

8 ii. Similarly, Aggregator Defendant Zumigo contracted with AT&T to obtain  
 9 access to AT&T customer real-time location data.<sup>98</sup> Zumigo then began providing access to the  
 10 data to third party Microbilt, with AT&T's approval.<sup>99</sup> Microbilt, in turn, sold the data to bounty  
 11 hunters, who sold it to bail bondsmen and—ultimately—to a journalist. Aggregator Defendant  
 12 Zumigo confirmed in 2019 that it provided the phone location to Microbilt and defended its sale  
 13 of that data to bounty hunters.<sup>100</sup>

14 iii. LocationSmart (then known as Locaid) was also responsible for selling  
 15 carrier location data to a company called CerCareOne.<sup>101</sup> For at least five years, CerCareOne  
 16 sold carrier customers' real-time location data to at least 250 bounty hunters, bail bondsmen, and  
 17 bail agents to find the real-time location of mobile phones.<sup>102</sup> CerCareOne charged up to \$1,100  
 18 per phone location request. Industry documents show—and LocationSmart admitted—that  
 19 LocationSmart continued to sell carrier data to CerCareOne after it merged with Locaid in  
 20 2015.<sup>103</sup>

21 <sup>94</sup> See Hutcheson Indictment at ¶ 11.

22 <sup>95</sup> See *id.* at ¶ 2.

23 <sup>96</sup> See *id.* at ¶¶ 3-4. As described in Sections A and C, the cell carriers' infrastructure allows the  
 carriers to determine the precise location of their customers in real time.

24 <sup>97</sup> See *id.* at ¶¶ 3-4. For more detail on this chain of access, see Section B.

25 <sup>98</sup> Letter from Timothy P. McKone to U.S. Senator Ron Wyden (Feb. 15, 2019), *supra* at 7.

26 <sup>99</sup> Joseph Cox, "I Gave a Bounty Hunter \$300. Then He Located Our Phone," *supra* at 57.

27 <sup>100</sup> *Id.*

28 <sup>101</sup> "Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer  
 Location Data for Years," *supra* at 71.

<sup>102</sup> *Id.*

<sup>103</sup> *Id.*

1           94. In each of the above examples, the carrier customers' sensitive, real-time location  
2 data was used to target and track those customers without their knowledge or consent, and  
3 without proper legal authority.

4           95. AT&T had knowledge that the Aggregator Defendants were selling access to its  
5 customers' location data information to additional companies.

6           96. AT&T admitted in 2018 that it used the Aggregator Defendants to "manage[]  
7 requests for customer data" and claimed that "[s]uch practices are common among all major  
8 carriers."<sup>104</sup>

9           97. Not only did AT&T know that the Aggregator Defendants were selling its  
10 customers' location data to other companies, it was also aware of the scale of that market because  
11 AT&T *approved* the Aggregator Defendants' customers.

12           98. Locaid, for example, informed its customers in 2011 that it would take  
13 approximately two weeks for cell carriers to approve the customers' request for access to the  
14 carrier location data.<sup>105</sup>

15           99. Similarly, LocationSmart informed potential customers in 2012 that they would  
16 need "[c]arrier review and confirmation to launch."<sup>106</sup> In 2018, they advertised that "carrier  
17 certification" takes two weeks.<sup>107</sup>

18           100. AT&T admitted in 2018 that it approved LocationSmart's sale of data to  
19 Securus.<sup>108</sup> As fully alleged above, Securus' access to carriers' location data caused *thousands* of  
20 instances of unauthorized access to carrier customers' real-time location data.

---

23 <sup>104</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
24 2018), *supra* at 51.

25 <sup>105</sup> "Mobile Location Overview," Locaid (April 2011), *available at*  
<https://cryptome.org/2014/08/locaid.pdf>.

26 <sup>106</sup> "How LocationSmart Works," LocationSmart (archived from Oct. 31, 2012), attached hereto  
as Ex. F.

27 <sup>107</sup> "FAQs," LocationSmart, *supra* at 89.

28 <sup>108</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
2018), *supra* at 51.

1           101. AT&T admitted in 2019 that it also provided access to its customer location data  
2 to Aggregator Defendant Zumigo and Microbilt.<sup>109</sup> As fully alleged above, Microbilt sold access  
3 to AT&T customers' location data to numerous third parties, including bounty hunters who resold  
4 that access without *any* customer consent or legal authority.

5           102. AT&T participated in the unlawful sale of access to its customer location data,  
6 and as the entity in control of the networks upon which such access was based, had unbridled  
7 control over the practices.

8           103. AT&T also knew that the Aggregator Defendants were using its customer location  
9 data for a broad array of purposes, including marketing.

10           104. In a 2013 public interview, LocationSmart CEO Mario Proietti advertised the  
11 marketing potential of location data, stating that “[p]recise location detection using WiFi is also  
12 ideal for proximity marketing to provide relevant promotions that enhance brand loyalty, drive  
13 in-store traffic and increase conversion rates.”<sup>110</sup>

14           105. In a 2013 YouTube video, Zumigo CEO Chirag Bakshi stated, “I’d be remiss if I  
15 didn’t mention the power of our location data for marketing. Our mobile data can make any  
16 marketing program more relevant to your customer[.]”<sup>111</sup> In a 2017 presentation, Zumigo  
17 advertised using its services to “[m]arket customers based on their current location.”<sup>112</sup>

18           106. AT&T was also aware of data aggregators' location-based capabilities and uses  
19 for the customer location data because it used the data itself. For example, one aggregator  
20 confirmed that major telecommunications carriers rely on location data aggregators and bounty  
21 hunters to use customer data—including location data—to find their own customers when those  
22

23 \_\_\_\_\_  
24 <sup>109</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (Feb. 15,  
2019), *supra* at 7.

25 <sup>110</sup> Robert Prime, “Locationsmart.net Interview with Mario Proietti,” Telematics.com (Sept. 19,  
2013), *available at* <https://www.telematics.com/location-smart-interview/>.

26 <sup>111</sup> “Launchpad 360: Zumigo,” YouTube (Nov. 6, 2013), *available at*  
27 <https://www.youtube.com/watch?v=PDVZmq-FIL0>.

28 <sup>112</sup> Snehashis Khan, “Securing Transactions and Customer Applications Through Location,”  
*supra* at 17.

1 customers fail to pay their wireless bills.<sup>113</sup> In other words, carriers are not only selling the data  
2 but actually benefiting from its use as well.

3 107. This complex chain of location data sales demonstrates AT&T's knowledge: (i)  
4 that its customers' real-time location data was being bought and sold, (ii) of the depth and  
5 breadth of that market, (iii) of the lack of diligence in verifying customers' consent, and (iv) of  
6 the various ways that the precise, real-time location data was being used.

7 **D. Defendants Sell Access to Location Data Intended for Enhanced 911-**  
8 **Purposes.**

9 108. AT&T's location data is extremely valuable to the downstream data market  
10 because it can reveal its customers' precise, real-time location information on demand.

11 109. AT&T's ability to obtain this very sensitive data was not intended for commercial  
12 sale, but rather for a much nobler purpose: to locate the carriers' customers when they call 911.  
13 For this same reason, customers have no way to opt out of the collection of this data by their  
14 wireless carriers for use in emergency situations.

15 **i. AT&T Lobbies the FCC to Allow Its Use of Precise A-GPS Data to**  
16 **Comply with E911 Regulations.**

17 110. As a telecommunications provider, AT&T is entrusted to use its cellular networks  
18 and the technology it installs within its customers' phones to determine their location in case of  
19 an emergency. This technology, called Enhanced 911 service ("E911") allows emergency  
20 response personnel to pinpoint the location of a cellular telephone caller anywhere in the United  
21 States when the caller places a 911 call.

22 111. The Federal Communications Commission ("FCC") first established E911  
23 location accuracy rules in 1997. By 2010, the FCC was concerned about the accuracy of E911  
24 data for calls placed from *inside* buildings or residences, and sought comment from carriers and  
25 the public about the feasibility of implementing accuracy rules regarding indoor 911 calls.<sup>114</sup>

26 <sup>113</sup> "I Gave a Bounty Hunter \$300. Then He Located Our Phone," Cyber Podcast (Jan. 24, 2019).

27 <sup>114</sup> Further Notice of Proposed Rulemaking and Notice of Inquiry, *In the Matter of Wireless*  
28 *E911 Location Accuracy Requirements*, 25 FCC Rcd 18957 (2010).

1 Several working groups began analyzing the issue and designing test beds for new technology.<sup>115</sup>  
 2 Aggregator Defendant LocationSmart participated in this testing<sup>116</sup> and described itself as a “key  
 3 player in the development and adoption of industry standard E911 testing methodologies.”<sup>117</sup>

4 112. In 2014, the FCC alerted wireless companies that it would indeed be updating its  
 5 E911 location accuracy rules “to ensure accurate indoor location information.”<sup>118</sup> In the near  
 6 term, the FCC proposed accuracy metrics that would allow responders to “identify floor level for  
 7 most calls from multi-story buildings.”<sup>119</sup> In the long term, it sought location information at the  
 8 room or office suite level.<sup>120</sup> The FCC sought carriers’ comments on how to meet these goals.<sup>121</sup>

9 113. In response, major telecommunications providers—including AT&T—proposed  
 10 “a new course” which would allow them to pinpoint 911 callers at the floor, suite, or apartment  
 11 level by leveraging “new technologies” that used signals from nearby fixed wireless devices,  
 12 such as increasingly prevalent Wi-Fi access points and Bluetooth Low Energy beacons to locate  
 13 carrier subscribers.<sup>122</sup> With this new technology (referred to herein as “assisted GPS” or “A-  
 14 GPS”), the carrier’s network would “automatically collect information from the wireless handset  
 15 about wireless access points within the vicinity of the wireless handset.”<sup>123</sup> Carriers, including  
 16 AT&T, would cause this information to be stored on their customers’ devices where it would be  
 17 made available to the carriers and could be shared in the event of an emergency.

18  
 19 <sup>115</sup> See, e.g., “Working Group 3, E 9-1-1 Location Accuracy Final Report v2,” Communications  
 20 Security, Reliability and Interoperability Council III (June 1, 2012), *available at*  
 21 [http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII\\_6-6-12\\_WG3-Final-Report.pdf](http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRICIII_6-6-12_WG3-Final-Report.pdf).

22 <sup>116</sup> See, e.g., Letter from Masoud Motamedi (President, TechnoCom Corporation) to Marlene H.  
 23 Dortch (Secretary, FCC) (June 23, 2014), *available at*  
 24 <https://ecfsapi.fcc.gov/file/7521337390.pdf>.

25 <sup>117</sup> “TruePosition Indoor Test Report: Wilmington, DE,” TechnoCom (June 18, 2014), attached  
 26 hereto as Ex. G.

27 <sup>118</sup> Third Further Notice of Proposed Rulemaking, *In the Matter of Wireless E911 Location*  
 28 *Accuracy Requirements*, 29 FCC Rcd 2374 ¶ 1 (2014) (hereafter “Third Further Notice”).

<sup>119</sup> *Id.*

<sup>120</sup> *Id.*

<sup>121</sup> *Id.* at ¶ 2.

<sup>122</sup> *Id.*

<sup>123</sup> Memorandum Opinion and Order, *In the Matter of Wireless E911 Location Accuracy*  
*Requirements*, 32 FCC Rcd. 9699 ¶ 5 (2017) (hereafter “NEAD Implementation Order”).

114. Once a cell phone “knows” what Wi-Fi or Bluetooth beacons are nearby, using A-GPS technology, it also needs to “know” where exactly those beacons are located (via a physical address) to provide the phone’s location. To solve this problem, the carriers proposed the creation of the National Emergency Address Database (“NEAD”) to store the physical addresses of fixed indoor beacons.<sup>124</sup> The beacons would be identified by a unique number called a MAC address, which is similar to a hardware serial number. The carriers’ networks could then query the NEAD platform for MAC addresses of beacons near the 911 caller’s phone to see if the beacons were saved in the NEAD and associated with a verified street address.”<sup>125</sup> For example, an entry in the NEAD might look like Figure 3 immediately below for a beacon located within the Library of Congress:

MAC Address	Street 1	Street 2	City	State
1a:2b:3c:4e:5f:6a	101 Independence Ave.	Fl. 3	Washington	DC

Figure 3<sup>126</sup>

115. Numerous consumer privacy organizations warned the FCC that the NEAD raised “significant privacy-related concerns.”<sup>127</sup> Specifically, the location technology underlying the NEAD could be “used to improve location accuracy not only of E911 services, but also of other services, *including commercial services, that rely on the same technology. This is concerning because consumers are highly protective of information about their location.*”<sup>128</sup>

<sup>124</sup> Roadmap at Section 2(e)(i).

<sup>125</sup> NEAD Implementation Order ¶ 5.

<sup>126</sup> Comments of Public Knowledge, Alvaro Bedoya, American Civil Liberties Union, Benton Foundation, Center For Democracy & Technology, Center For Digital Democracy, Common Sense Media, Consumer Action, Consumer Federation of America, Consumer Federation of California, Consumer Watchdog, Electronic Frontier Foundation, Electronic Privacy Information Center, New America Foundation’s Open Technology Institute Privacy Rights Clearinghouse, U.S. PIRG, and World Privacy Forum, *In the Matter of Wireless E911 Location Accuracy Requirements* (Dec. 15, 2014) at 3, available at <https://www.publicknowledge.org/documents/official-comments-on-wireless-e911-location-accuracy-requirements>.

<sup>127</sup> *Id.* at 2.

<sup>128</sup> *Id.* at 5 (emphasis added).



116. In February 2015, the FCC announced that wireless carriers would be required to provide either a dispatchable address or longitude and latitude location “within 50 meters” for a gradually increasing percentage of wireless 911 calls, ultimately aiming to achieve location data within 50 meters for 80% of wireless 911 calls by 2020.<sup>129</sup> It also set benchmarks for the development of z-axis data (*i.e.*, height or floor within a building).<sup>130</sup> Crucially, the FCC gave wireless carriers permission to develop the ability to use, and then actually use, their customers’ A-GPS data for E911 purposes.<sup>131</sup>

117. Importantly, the FCC also adopted new privacy rules that applied to the new E911 A-GPS data being developed and utilized by the carriers. The FCC required that “as a condition of using the NEAD *or any information contained therein* to meet our 911 location requirements, and prior to use of the NEAD, [wireless carriers] must certify that they will not use the NEAD *or associated data* for any purpose other than for the purpose of responding to 911 calls, except as required by law.”<sup>132</sup> AT&T, specifically, “pledg[ed] that the information contained in the NEAD will not be used for any non-emergency purposes.”<sup>133</sup>

**ii. AT&T Sold Access to E911 Data for Commercial Purposes.**

118. Despite the sensitive nature of precise E911 A-GPS location data and AT&T’s obligations and promises to protect this data from unauthorized or commercial use, AT&T began providing access to its customers’ E911 A-GPS data to the Aggregator Defendants and hundreds of third parties without proper customer consent or legal authority.

119. As confirmed by industry documents, the Aggregator Defendants’ downstream customers were obtaining access to carrier customers’ A-GPS data.<sup>134</sup>

<sup>129</sup> 47 C.F.R. § 20.18(i)(2)(i).

<sup>130</sup> 47 C.F.R. § 20.18(i)(2)(ii).

<sup>131</sup> *See, e.g.*, 47 C.F.R. § 20.18(h)(1)(v).

<sup>132</sup> 47 C.F.R. § 20.18(i)(4)(iv) (emphasis added).

<sup>133</sup> Fourth Report and Order, *In the Matter of Wireless E911 Location Accuracy Requirements*, 30 F.C.C. Rcd. 1259 ¶ 71 (2015) (“AT&T pledges that the information contained in the NEAD will not be used for any non-emergency purposes.”). AT&T filed its certification regarding the use of the NEAD at the FCC on June 1, 2018.

<sup>134</sup> “Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls,” *supra* at 71.



120. Carriers admit that this A-GPS data is intended for use in public safety scenarios. As one carrier told the FCC: “A-GPS is reasonably the foundation of wireless [emergency] 911 location for both indoor and outdoor locations.”<sup>135</sup>

121. AT&T knew that access to its customers’ A-GPS was being sold. The Aggregator Defendants publicly marketed their ability to use precise A-GPS data for commercial purposes.

122. LocationSmart’s 2018 advertising materials likewise confirmed its use of beacon-based A-GPS technology.<sup>136</sup>

123. LocationSmart advertises to customers its ability to “utilize the same technology used to enable emergency assistance and this includes cell tower and cell sector location, Assisted GPS and cell tower trilateration.”<sup>137</sup> In May 2018, LocationSmart disclosed that “[t]he data provided is based on cell tower location, cell tower trilateration and assisted GPS information gleaned from the mobile devices” and stated that its services “can pinpoint precise locations.”<sup>138</sup>

124. LocationSmart confirmed that “[c]arrier location services available through LocationSmart are based on a variety of technologies depending on each carrier’s particular location infrastructure implementation. That could include AGPS, cell tower, cell sector, or cell site trilateration.”<sup>139</sup>

125. As described by Colorado Law Associate Professor Blake Reid, “the only reason we grant carriers any access to this information is to make sure that first responders are able to locate us in an emergency. If the carriers are turning around and using that access to sell

<sup>135</sup> Letter from John T. Nakahata (Counsel to T-Mobile USA, Inc.) to Marlene H. Dortch (FCC) (Nov. 16, 2013), *available at* <https://ecfsapi.fcc.gov/file/7520958047.pdf>.

<sup>136</sup> “FAQs,” LocationSmart, *supra* at 89.

<sup>137</sup> Ex. C (LocationSmart “Carrier Network Location Collateral”).

<sup>138</sup> *Id.*

<sup>139</sup> Joseph Cox, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years,” *supra* at 71.

1 information to bounty hunters or whomever else, it is a shocking abuse of the trust that the public  
2 places in them to safeguard privacy while protecting public safety.”<sup>140</sup>

3 **E. AT&T Allowed Unauthorized Third Parties to Access Customers’ Location**  
4 **Data.**

5 126. While admitting that it allowed third parties to access its customers’ real-time  
6 location data, AT&T asserted that such access was only granted with customer consent or legal  
7 authority.<sup>141</sup> That representation was and is false. AT&T and its agents, the Aggregator  
8 Defendants, failed to obtain customer consent or obtain proper legal authority before allowing  
9 third parties to use or access carrier customers’ real-time location information.

10 127. AT&T admittedly did not seek customer consent directly. Instead, it maintained  
11 that the companies seeking to access customers’ real-time location data (such as Securus,  
12 Microbilt, and CerCareOne) were responsible for obtaining consent or legal authority for the  
13 information.<sup>142</sup>

14 128. After improperly pushing its duty to obtain consent downstream, AT&T failed to  
15 confirm that the Aggregator Defendants and/or the Aggregator Defendants’ customers (such as  
16 Microbilt, Securus, and CerCareOne) obtained any customer consent or proper legal authority  
17 before granting them access to customer location.

18 129. In fact, the Aggregator Defendants’ customers routinely failed to obtain customer  
19 consent or legal authority.

20 130. For example, as AT&T admitted in 2018, Securus “did not in fact obtain customer  
21 consent before collecting customers’ location information.”<sup>143</sup> Instead, Securus required users to  
22 upload a document showing that they had legal authority to request a specific carrier customer’s

23 \_\_\_\_\_  
24 <sup>140</sup> Joseph Cox, “Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911  
Calls,” *supra* at 71.

25 <sup>141</sup> *See, e.g.*, Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden  
(June 15, 2018), *supra* at 51.

26 <sup>142</sup> *See, e.g., id.*; Brian Krebs, “AT&T, Sprint, Verizon to Stop Sharing Customer Location Data  
with Third Parties,” KREBS ON SECURITY, *supra* at 49.

27 <sup>143</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
28 2018), *supra* at 51.

1 real-time location information. Securus officials “confirmed ... that Securus takes *no steps* to  
 2 verify” that the uploaded document *actually* provided such legal authorization and failed to  
 3 conduct “*any review* of surveillance requests.”<sup>144</sup>

4 131. Indeed, Senator Wyden stated in his letter to AT&T that “[s]enior officials from  
 5 Securus have confirmed... that it *never* checks the legitimacy of those uploaded documents to  
 6 determine whether they are in fact court orders *and has dismissed suggestions that it is obligated*  
 7 *to do so.*”<sup>145</sup> These documents did not even have to *appear* to be legitimate: federal authorities  
 8 allege that Sheriff Hutcheson uploaded documents from his health insurance plan and a sheriff’s  
 9 manual and was nonetheless granted access to nonconsenting individuals’ real-time location  
 10 data—including the location data of a judge—on the basis of those documents.<sup>146</sup>

11 132. Once any document was uploaded, all that a Securus customer had to do to access  
 12 a carrier customer’s real-time location data was check a box on the Securus portal that stated,  
 13 “[b]y checking this box, I hereby certify the attached document is an official document giving  
 14 permission to look up the location on this phone number requested.”<sup>147</sup> Once that box was  
 15 checked, the user clicked “Get Location” and Securus would use carrier-level location data to  
 16 immediately provide the longitude and latitude of the phone’s current location, as well as an  
 17 address.<sup>148</sup>

18 133. The immediate access to location information reveals that Securus never intended  
 19 to verify the legitimacy of purported legal authority before disclosing real-time location data.  
 20 Instead, Securus pushed responsibility *even further* down the chain and “relied upon law  
 21 enforcement’s representation that it had appropriate legal authority.”<sup>149</sup>  
 22  
 23

24 <sup>144</sup> Letter from U.S. Senator Ron Wyden to Randall L. Stephenson (AT&T) (May 8, 2018), *supra*  
 25 at 32 (emphasis added).

26 <sup>145</sup> *Id.* (emphasis added).

27 <sup>146</sup> Hutcheson Indictment at ¶ 22.

28 <sup>147</sup> *See id.* at ¶ 6.

<sup>148</sup> *See* Hutcheson Indictment at ¶ 7.

<sup>149</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
 2018), *supra* at 51.

1           134. In other words, in the case of the Securus breaches, the responsibility to confirm  
2 authorization for real-time location tracking was passed down every rung of the chain: from  
3 AT&T to Location Smart, from LocationSmart to 3Cinteractive, from 3Cinteractive to Securus,  
4 from Securus to correctional facilities, and from those facilities down to individual officers.

5           135. By abdicating its responsibility in this manner and failing to implement effective  
6 controls against unauthorized access to location data, AT&T failed to protect its customers’  
7 sensitive location data, and instead benefited from its dissemination.

8           136. AT&T’s dereliction of its duty has had widespread impact. Securus had  
9 thousands of customers as of 2013, each of which—on information and belief—could request  
10 access to AT&T customers’ real-time geolocation information. Upon information and belief,  
11 *none* of those customers’ representations about consent or legal authority was ever verified.

12           137. AT&T’s failures to protect its customers and obtain proper authorization before  
13 disclosing location data are further exemplified by its admissions concerning Securus’ access to  
14 its customers’ location data.

15           138. In June 2018, AT&T Services, Inc.’s Executive Vice President, Timothy McKone,  
16 wrote that “AT&T has never authorized the use of its customers data for the Securus web portal  
17 service described in [Wyden’s] letter.”<sup>150</sup>

18           139. But this representation only exemplifies the magnitude of AT&T’s extreme  
19 recklessness and knowing negligence. That Securus was able to use AT&T data on a wide scale  
20 without AT&T’s authorization reveals that AT&T’s safeguarding of access to its customers’ real-  
21 time location data and its system for obtaining and tracking customer approval before third-party  
22 use was so lax, it was unaware of how the data was used and by whom.

23           140. Securus’ ability to use AT&T data without authorization was not an isolated  
24 incident, but instead just one example of AT&T’s pattern and practice of allowing unlawful  
25 access to its customers’ sensitive real-time location information.

26  
27  
28 <sup>150</sup> *Id.*

141. For example, CerCareOne allowed more than 250 bail bond companies and bounty hunters to use carrier data “tens of thousands of times to locate phones” – often without *any* consent from the customer.<sup>151</sup>

142. Additionally, a reporter was able to obtain the precise location information of an individual—ultimately through Aggregator Defendant Zumigo’s access to cell carrier location data—without obtaining *any documented* consent from the targeted carrier customer.<sup>152</sup> The reporter personally obtained such consent, but that same consent was never itself verified, apparently, by either Zumigo or the individual’s cell carrier.

143. By providing the Aggregator Defendants direct access to customers’ location data and allowing the Aggregator Defendants’ to resell that access to additional third parties, AT&T abdicated its duty to get consent, instead allowing a chain of “consent handoffs” to develop. This led to the formation a robust market for customers’ location data with no oversight by AT&T, and a lack of proper consent or legal authority for such disclosures. This was in clear dereliction of AT&T’s duty to its customers.

144. As Senator Wyden explained, “[c]arriers are always responsible for who ends up with their customers data—it’s not enough to lay the blame for misuse on downstream companies.”<sup>153</sup> Senator Wyden stated that the carriers’ practices of attempting to delegate the responsibility for obtaining consent “skirt[ed] wireless carrier’s legal obligation to be the sole conduit by which the government conducts surveillance of Americans’ phone records[.]”<sup>154</sup> He asserted that “[w]ireless carriers have an obligation to take affirmative steps to verify law enforcement requests for customer information” and that absent such legal authority, federal law permits the disclosure of customer location data to third parties *only* when the customer consents.

<sup>151</sup> “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years,” *supra* at 71.

<sup>152</sup> Joseph Cox, “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” *supra* at 57.

<sup>153</sup> Joseph Cox, “Google Demanded That T-Mobile, Sprint Not Sell Google Fi Customers’ Location Data,” Motherboard (Jan. 11, 2019), *available at* [https://www.vice.com/en\\_us/article/d3bnyv/google-demanded-tmobile-sprint-to-not-sell-google-fi-customers-location-data](https://www.vice.com/en_us/article/d3bnyv/google-demanded-tmobile-sprint-to-not-sell-google-fi-customers-location-data).

<sup>154</sup> Letter from U.S. Senator Ron Wyden to Chairman Ajit Pai (FCC) (May 8, 2018), *supra* at 36.

1 He described the carriers' practice of pushing its obligation to get the required consent down to  
 2 other third parties as "the legal equivalent of a pinky promise." This "clear abuse" of the consent  
 3 structure and requirement for genuine legal authority, he asserted, was "only possible because  
 4 wireless carriers sell their customers' private information to companies claiming to have  
 5 consumer consent without sufficiently verifying those claims."<sup>155</sup>

6 **F. Defendants' Sale of Access to Customers' Location Data Is Outrageous and**  
 7 **Harmful.**

8 145. Plaintiffs and many other AT&T customers have been harmed by AT&T's failure  
 9 to properly protect their location data from unauthorized access, thereby disclosing Plaintiffs'  
 10 and customers' legally protected information to the Aggregator Defendants and unknown  
 11 additional other third parties.

12 146. Plaintiffs were emotionally distressed by the discovery that their location data was  
 13 sold to the Aggregator Defendants and additional unknown third parties without their consent.

14 147. Not only has AT&T customers' private location information been disclosed to  
 15 unauthorized parties—including the Aggregator Defendants—but AT&T customers are also at  
 16 substantial risk of additional, imminent future harm. Specifically, Plaintiffs and many other  
 17 AT&T customers are at substantial risk of: (i) further disclosure of their personal information to  
 18 additional third parties, (ii) disclosure of their personal information via a data breach, and (iii)  
 19 disclosure of past location data already obtained by the Aggregator Defendants and/or additional  
 20 unknown third parties.

21 148. As the FCC has recognized, the unauthorized disclosure of carrier customers'  
 22 personal information "by any method invades the privacy of unsuspecting consumers and  
 23 increases the risk of identity theft, harassment, stalking, and other threats to personal safety."<sup>156</sup>  
 24 According to the FCC, "[t]he black market for [wireless customers' proprietary network  
 25 information] has grown exponentially with an increased market value placed on obtaining this

26 <sup>155</sup> *Id.*

27 <sup>156</sup> Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of*  
 28 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers Use of*  
*Customer Proprietary Network Info. & Other Customer Info.*, 22 F.C.C. Rcd. 6927 ¶ 46 (2007)  
 (hereafter "2007 CPNI Order").

1 data, and there is concrete evidence that the dissemination of this private information does inflict  
 2 specific and significant harm on individuals, including harassment and the use of the data to  
 3 assume a customer's identity. The reality of this private information being disseminated is well-  
 4 documented and has already resulted in *irrevocable damage to customers*.”<sup>157</sup>

5 149. Senator Ron Wyden describes location tracking as a “national security and a  
 6 personal safety nightmare.”<sup>158</sup>

7 150. Congressman Frank Pallone, Jr. of New Jersey, Chairman of the House  
 8 Committee on Energy and Commerce, called for an emergency hearing on Defendants' practices  
 9 in February 2019 and stressed the “grave consequences that unauthorized sharing of customer  
 10 location data could have for public safety and national security[.]”<sup>159</sup>

11 151. FCC Commissioner Geoffrey Starks stated in February 2019 that “[i]t is  
 12 absolutely chilling to think that a stranger can buy access to exactly where we are at any given  
 13 moment by tapping into the data on our phones without our consent. And, now I am hearing  
 14 allegations that consumers' GPS data—data so accurate that it can pinpoint your location the  
 15 floor of a building you are in—is also available for sale. It isn't difficult to imagine intrusive or  
 16 even downright dangerous uses of this data.”<sup>160</sup> Separately, he called the sale of customer  
 17 location data “a matter of public safety. . . . It isn't difficult to imagine intrusive or even  
 18 downright dangerous uses of this data.”<sup>161</sup>

19 152. As the public reporting surrounding the sale of customer location data illustrates,  
 20 “as the data spreads out from the original source, being the [telecommunications providers], the  
 21 risk of abuse just dramatically increases. Not only is it ending up in the hands of bounty hunters,  
 22 but then of course those individuals might just spy on their girlfriends, as a source told [a  
 23

24 <sup>157</sup> 2007 CPNI Order ¶ 39 (emphasis added).

25 <sup>158</sup> “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” Cyber Podcast, *supra* at 113.

26 <sup>159</sup> Letter from U.S. Representative Frank Pallone, Jr. to Chairman Ajit Pai (FCC) (Feb. 19,  
 2019), attached hereto as Ex. H.

27 <sup>160</sup> Ex. B. (email from Michael Scurato (FCC) to Joseph Cox (Motherboard) (Feb. 4, 2019)).

28 <sup>161</sup> Email from Michael Scurato (FCC) to Jon Brodtkin (Ars Technica) (Feb. 13, 2010), attached  
 hereto as Ex. I.



1 Motherboard reporter] is what happens among these people. Once a person has access to that  
 2 data, they can—it appears—do whatever they want with it.”<sup>162</sup>

3 153. AT&T customers, including Plaintiffs, are at substantial risk that their location  
 4 information will be disclosed to dangerous third parties, including stalkers and/or domestic  
 5 abusers. The use of location data by stalkers and domestic abusers is well-known and  
 6 documented. A 2009 Justice Department report estimated that more than 25,000 adults in the  
 7 U.S. are victims of GPS stalking each year, including by cell phone.<sup>163</sup>

8 154. This risk is compounded by the fact that location targeting using carrier location  
 9 data occurs surreptitiously and is invisible to the phone’s user. Users do not receive any alert or  
 10 notification that their location has been accessed.<sup>164</sup> Plaintiffs do not, and indeed cannot, know  
 11 how many and which third parties—in addition to the Aggregator Defendants—accessed their  
 12 sensitive location data. AT&T, the Aggregator Defendants, and the third parties with whom they  
 13 contract to sell Plaintiffs’ and Class members’ location data are the sole parties with access to  
 14 that information about whose data was sold, when, and to whom.

15 155. The FCC has recognized that victims of cell carrier data breaches are at a  
 16 heightened risk when they are unaware that the breach has occurred.<sup>165</sup> Because Plaintiffs and  
 17 Class members are unable to identify all of the parties who purchased their real-time location  
 18 data through AT&T and its agents, they are unable to properly protect themselves.

19 156. The risk of harm from Defendants’ massive dissemination of this highly sensitive  
 20 customer location information is further compounded by the inherent and recurring hazards that:

21 i. company employees will misuse the information;<sup>166</sup> and

22 \_\_\_\_\_  
 23 <sup>162</sup> “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” Cyber Podcast, *supra* at 113.

24 <sup>163</sup> Katrina Baum, Shannan Catalano, and Michael Rand, “Stalking Victimization in the United  
 States,” Bureau of Justice Statistics, U.S. Department of Justice (Jan. 2009), *available at*  
 25 <https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf>.

26 <sup>164</sup> “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” Cyber Podcast, *supra* at 113.

27 <sup>165</sup> 2007 CPNI Order ¶¶ 26, 30.

28 <sup>166</sup> Megan Geuss, “AT&T Fined \$25 Million After Call Center Employees Stole Customers’  
 Data,” ARS TECHNICA, Apr. 8, 2015, *available at* [https://arstechnica.com/tech-](https://arstechnica.com/tech-policy/2015/04/att-fined-25-million-after-call-center-employees-stole-customers-data/)  
[policy/2015/04/att-fined-25-million-after-call-center-employees-stole-customers-data/](https://arstechnica.com/tech-policy/2015/04/att-fined-25-million-after-call-center-employees-stole-customers-data/). *See also*  
 Joseph Cox, “Snapchat Employees Abused Data Access to Spy on Users,” MOTHERBOARD, May



1           ii.           security vulnerabilities will allow data thieves to steal the information.<sup>167</sup>

2           157.   Additionally, AT&T represented to its customers that it would “not sell [their]  
3   personal information to anyone for any purpose. Period.”<sup>168</sup> Plaintiffs and other AT&T  
4   customers relied on AT&T’s misrepresentations, believing that they were protected from the  
5   risks associated with unauthorized access to their real-time location data.

6           158.   Plaintiffs and AT&T wireless customers are at a continuing risk of access and  
7   misuse of their historical location data. This location data can be personally identifying on its  
8   own or when combined with other information, such as customers’ cell phone numbers, which  
9   are used in the location data request process. AT&T customers are therefore at a continuing,  
10   substantial risk that their historical location data will be accessed and their privacy further  
11   violated due to the fact that Defendants have already allowed the data to be breached and  
12   accessed by countless unknown third parties.

13           **G.       The Sale of Location Data Violates Reasonable Expectations of Privacy and**  
14           **Is Highly Offensive.**

15           159.   Plaintiffs’ reasonable expectation of privacy in their location data is enshrined in  
16   federal, state, and common law and reflected in widespread societal norms and Supreme Court  
17   jurisprudence.

18           160.   As recently observed by the Supreme Court, cell phone location data “present[s]  
19   even greater privacy concerns than the GPS monitoring of a vehicle ... [A] cell phone—almost a  
20   ‘feature of human anatomy,’ tracks nearly exactly the movements of its owner. While individuals  
21   regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell  
22   phone faithfully follows its owner beyond public thoroughfares and into private residences,  
23

24           \_\_\_\_\_  
25   23, 2019, *available at* [https://www.vice.com/en\\_us/article/xwnva7/snapchat-employees-abused-](https://www.vice.com/en_us/article/xwnva7/snapchat-employees-abused-data-access-spy-on-users-snaplion)  
26   [data-access-spy-on-users-snaplion](https://www.vice.com/en_us/article/xwnva7/snapchat-employees-abused-data-access-spy-on-users-snaplion).

27   <sup>167</sup> Andrew Liptak, “Security Researchers Found Vulnerabilities at AT&T, T-Mobile, and Sprint  
28   That Could Have Exposed Customer Data,” THE VERGE, Aug. 25, 2018, *available at*  
29   [https://www.theverge.com/2018/8/25/17781906/att-tmobile-sprint-security-vulnerabilities-](https://www.theverge.com/2018/8/25/17781906/att-tmobile-sprint-security-vulnerabilities-customer-information)  
30   [customer-information](https://www.theverge.com/2018/8/25/17781906/att-tmobile-sprint-security-vulnerabilities-customer-information).

31   <sup>168</sup> See Ex. A (AT&T Privacy Policy).

doctors offices, political headquarters, and other potentially revealing locales.” *Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018).

161. A 2013 study, for example, found that 79% of people between the ages of 18 and 44 have their smart phones with them 22 hours out of the day.<sup>169</sup> Twenty-three percent of adults and 40 percent of teenagers say they use a mobile device within five minutes of waking up.<sup>170</sup> Low-income Americans are more likely to be smart phone dependent because their smart phone is more likely to be their primary or only method to access the Internet. As of 2019, 26% of adults living in households earning less than \$30,000 a year own a smart phone but do not have broadband internet at home (compared to only 5% of those living in households earning \$100,000 or more).<sup>171</sup>

162. Due to the ubiquity of cell phones in individuals’ lives, cell phone location data “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his ‘familial, political, professional, religious, and sexual associations.’” *Carpenter*, 138 S. Ct. at 2217. “These location records hold for many Americans the ‘privacies of life.’” *Id.* (quotation marks and citation omitted). Plaintiffs and similarly situated carrier customers therefore have a reasonable expectation of privacy in such data.

163. Plaintiffs’ expectations of privacy have long been protected by the law. Invasion of privacy has been recognized as a common law tort for more than a century. In *Griswold v. Connecticut*, 381 U.S. 479 (1965), the Supreme Court confirmed the primacy of privacy rights, explaining that the Constitution operates in the shadow of a “right to privacy older than the Bill of Rights.”

<sup>169</sup> Allison Stadd, “79% of People 18-44 Have Their Smartphones With Them 22 Hours a Day,” AD WEEK (April 2, 2013), available at <https://www.adweek.com/digital/smartphones/>.

<sup>170</sup> Niraj Chokshi, “Your Kids Think You’re Addicted to Your Phone,” THE NEW YORK TIMES (May 29, 2019), available at <https://www.nytimes.com/2019/05/29/technology/cell-phone-usage.html>.

<sup>171</sup> Monica Anderson, “Digital Divide Persists Even as Lower-Income Americans Make Gains in Tech Adoption,” PEW RESEARCH CENTER (May 7, 2019), available at <https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/>.

1           164. In *Carpenter*, the Supreme Court specifically recognized the reasonable  
 2 expectation of privacy a person has in the location information generated by her cell phone.  
 3 *Carpenter*, 138 S. Ct. 2206. The Court held that the government’s warrantless access to  
 4 customer location data invades an individual’s “reasonable expectation of privacy in the whole  
 5 of his physical movements.” *Id.* at 2219.

6           165. California also recognizes Plaintiffs’ expectations of privacy. California amended  
 7 its constitution in 1972 to specifically enumerate a right to privacy in its very first section. *See*  
 8 Cal. Const. Art. I, § 1. The California constitutional right of privacy is intended to protect  
 9 Californians from Defendants’ “misusing information gathered for one purpose in order to serve  
 10 other purposes[.]”<sup>172</sup>

11           166. The expectation of privacy in cell phone location data has been repeatedly  
 12 reiterated by federal agencies. Indeed, the FCC has stated that it “fully expect[s] carriers to take  
 13 every reasonable precaution to protect the confidentiality of proprietary or personal customer  
 14 information.”<sup>173</sup>

15           167. FCC Commissioner Jessica Rosenworcel, in a letter to AT&T Communications  
 16 CEO John Donovan regarding AT&T’s sale of access to its customers’ local data, stated that  
 17 “[r]eal-time location information is sensitive data deserving the highest level of privacy  
 18 protection.”<sup>174</sup>

19           168. The Federal Trade Commission (“FTC”) has also recognized consumers’  
 20 expectation of privacy in their location data. In 2016, the FTC entered into a settlement  
 21 agreement with a mobile advertising company charged with deceptively tracking the location  
 22  
 23  
 24

25 <sup>172</sup> Ballot Pamp., Proposed Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7,  
 26 1972), p. 27.

27 <sup>173</sup> 2007 CPNI Order ¶ 64.

28 <sup>174</sup> Letter from Commissioner Jessica Rosenworcel (FCC) to John Donovan (AT&T) (May 1,  
 2019), *available at* <https://www.documentcloud.org/documents/5985428-FCC-Commissioner-Rosenworcel-letters-to-Telecom.html>.

information of hundreds of millions of people with their knowledge or consent.<sup>175</sup> The company agreed to pay a \$950,000 civil penalty and institute a robust comprehensive privacy program.

**i. Plaintiffs' Expectations Reflect Widely Held Social Norms.**

169. A reasonable person would believe that Defendants' conduct described herein violates Plaintiffs' expectations of privacy.

170. According to a poll by the Pew Research Center, 93% of adults believe that being in control of who can get information about them is important, and 90% believe that controlling what information is collected about them is important.<sup>176</sup>

171. In a 2019 poll about location data, more than 83% of Americans responded that it was "never" okay for "companies that collect [their] location data to sell or share that data with third parties."<sup>177</sup> More than 14% responded that sharing location data was only permissible if the customer "was asked for, and gave, explicit consent (opted in)."<sup>178</sup> Respondents' top concerns regarding the collection and use of location data included: (1) general loss of privacy (61%); (2) risk of breach or that data could fall into a hacker's or thief's hands (58%); (3) unauthorized use by law enforcement or the government (43%); use by companies for profiling (48%); and (5) personal safety risks, such as use by a stalker or ex-partner (43%).<sup>179</sup>

172. Americans do not approve of observation without consent: 88% say it is important that they not have someone watch or listen to them without their permission.<sup>180</sup>

<sup>175</sup> *Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission*, Federal Trade Commission (June 22, 2016), available at <https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked>.

<sup>176</sup> Mary Madden and Lee Rainie, "Americans' Attitudes About Privacy, Security and Surveillance," PEW RESEARCH CENTER (May 20, 2015), available at <https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

<sup>177</sup> "Some Questions About Location Sharing," Consumer Action (Feb. 8 to March 4, 2019), available at <https://www.consumer-action.org/downloads/Location-tracking-survey-2019.pdf>.

<sup>178</sup> *Id.*

<sup>179</sup> *Id.*

<sup>180</sup> *Id.*

173. A 2016 survey found that more Americans are concerned about not knowing how the personal information collected about them is used than are concerned about losing their principal source of income, being a victim of crime in their community, climate change, or access to affordable health care.<sup>181</sup> Their top cause of concern “is companies collecting and sharing personal information with other companies” – the very conduct alleged here.

174. A 2016 Pew Research Poll found that “[s]ome of the most strongly negative reactions” it received to questions about privacy “came in response to scenarios involving the sharing of personal location data.”<sup>182</sup>

175. Public outcry following the exposure of Defendants’ practices, including responses from members of the United States Congress, reflect society’s expectation of privacy in location data. In a letter from fifteen sitting United States Senators calling for an investigation into Defendants’ practices, the Senators stated, “Americans expect that their location data will be protected.”<sup>183</sup>

**ii. Federal Law Requires AT&T and Its Agents to Protect Customers’ Location Data.**

176. Recognizing the sensitivity of data collected by cell carriers, Congress, through the FCA, requires telecommunications providers—including wireless cell carriers, such as AT&T—to protect their customers’ sensitive personal information to which they have access as a result of their unique position as telecommunications carriers.<sup>184</sup>

<sup>181</sup> “Study Finds More Americans Concerned About Data Privacy Than Losing Their Income,” NATIONAL CYBER SECURITY ALLIANCE (Jan. 28, 2016), *available at* <https://staysafeonline.org/press-release/americans-concerned-data-privacy/>.

<sup>182</sup> Mary Madden and Lee Rainie, *Privacy and Information Sharing*, PEW RESEARCH CENTER (Jan. 14, 2016), *available at* <https://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/>.

<sup>183</sup> Letter from United States Senators Ron Wyden et al. to Joseph J. Simons (FTC) and Ajit Pai (FCC) (Jan. 24, 2019), *supra* at 70.

<sup>184</sup> 47 U.S.C. § 222.

177. While the FCA facilitates nationwide deployment of E911 technology, Congress expressly protected the privacy of customer information.<sup>185</sup> In doing so, Congress specifically included protection for the privacy of location information pertaining to cell phone users.

178. Section 222 of the FCA, which became part of the Act in 1996, establishes carriers' duty to protect the privacy and security of information about their customers. Likewise, Section 201(b) of the Act requires AT&T's practices related to the collection of information from its customers to be "just and reasonable" and declares unlawful any practice that is unjust or unreasonable.<sup>186</sup>

179. Congress enacted Section 222 to "define[] three fundamental principles to protect all consumers. These principles are: (1) the right of consumers to know the specific information that is being collected about them; (2) the right of consumers to have proper notice that such information is being used for other purposes; and (3) the right of consumers to stop the reuse or sale of that information."<sup>187</sup> The FCA represents Congress's judgment that carrier customers' proprietary network information, including location data, should remain private.

180. Pursuant to the FCA, AT&T has a duty to protect the confidentiality of certain types of customer data, including precise location data.<sup>188</sup> This duty extends to data that AT&T provides to the Aggregator Defendants.<sup>189</sup> Under the FCA, AT&T is not just liable for its own violations of the Act, but also for violations that it "cause[s] or permit[s]."<sup>190</sup>

<sup>185</sup> See P.L. No. 106–81(2), § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222).

<sup>186</sup> 47 U.S.C. § 201(b).

<sup>187</sup> H.R. Conf. Rep. No. 458, 104th Cong., 2d Sess. 204 (1996) (Joint Explanatory Statement of the Committee of Conference); see also H.R. Rep. No. 204, 104th Cong., 1st Sess. 91 (1995); *id.* at 90 (explaining that section 222 balances "the need for customers to be sure that personal information that carriers may collect is not misused" with customers' expectation that "the carrier's employees will have available all relevant information about their service").

<sup>188</sup> 47 U.S.C. § 222(a).

<sup>189</sup> 2007 CPNI Order ¶ 39.

<sup>190</sup> See 47 U.S.C.A. § 206 (establishing that "[i]n case any common carrier shall do, or cause or permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful, or shall omit to do any act, matter, or thing in this chapter required to be done such common carrier shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter[.]")

181. One type of data that carriers must protect is called customer proprietary network information (“CPNI”). CPNI is defined 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.”<sup>191</sup>

182. The FCA and the FCC designate location information as CPNI.<sup>192</sup> AT&T receives Plaintiffs’ and Class members’ location data by virtue of its provision of telecommunications services to Plaintiffs and Class members.<sup>193</sup> As established in Section C, AT&T has implemented technology that causes location data to be stored on its customers’ device, where it is made available to AT&T.<sup>194</sup> This location information is collected from Plaintiffs’ and other AT&T’s subscribers’ mobile devices at AT&T’s direction, and AT&T and the Aggregator Defendants can access and control the information.<sup>195</sup> The FCC has warned “that location information in particular can be very sensitive customer information.”<sup>196</sup>

183. AT&T has breached its duty to protect customers’ CPNI by knowingly allowing countless third parties access to the location data. AT&T has failed in its duty to ensure that access to CPNI is only granted pursuant to the requirements of the FCA, and that the data otherwise be safeguarded against improper use. AT&T’s failure to provide proper notice, obtain

<sup>191</sup> 47 U.S.C. § 222(h)(1).

<sup>192</sup> 47 U.S.C. § 222(h)(1)(A); *see also* Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info.*, 28 F.C.C. Rcd. 9609 ¶ 22 (2013) (“The location of a customer’s use of a telecommunications service also clearly qualifies as CPNI.”); *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (“47 U.S.C. § 222 designates a customer’s cell-site location information as “customer proprietary network information” (CPNI)[.]”)

<sup>193</sup> 47 U.S.C. § 222(h)(1).

<sup>194</sup> Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Info. & Other Customer Info.*, 28 F.C.C. Rcd. 9609 ¶ 26 (2013).

<sup>195</sup> *Id.* at ¶ 16.

<sup>196</sup> *Id.* at n. 54.



proper consent, and safeguard Plaintiffs' and similarly situated customers' location data violates the FCA and its corresponding regulations.

184. FCC commissioners have publicly stated that AT&T's sale of customers' precise location data violates the FCA. Current FCC commissioner Geoffrey Starks confirmed that the sale of location data as reported in 2018 and 2019 would constitute a violation of the law: "Time and again in recent months, we've read about people's location information from use of mobile phones being for sale . . . If the allegations are true, this is against the law and violates the [FCC's] rules. It's outrageous and needs to stop."<sup>197</sup> Likewise, FCC Commissioner Jessica Rosenworcel stated that, "[s]elling location data without customers' consent is a violation of [FCC] rules."<sup>198</sup>

185. Pursuant to the FCA, the FCC has developed comprehensive rules concerning AT&T's obligations under its duty to protect customers' CPNI.<sup>199</sup> These rules require, among other things, the proper notice carriers must provide and the consent they must obtain before using, selling, or disclosing their customers' proprietary data, and the steps they must take to safeguard the proprietary data. As alleged in detail below, AT&T has failed to abide by the FCC's rules concerning notice, consent, and proper safeguarding requirements.

**a. The FCA Requires Defendants to Provide Plaintiffs Proper Notice Before Disclosing Their Location Data.**

186. The FCA requires AT&T to provide "individual notice" to customers before seeking their approval to "use, disclose, or permit access to [their] CPNI."<sup>200</sup>

<sup>197</sup> Jon Brodtkin, "Ajit Pai's Plan for Phone Location Data Never Mentions the Word 'Privacy,'" ARS TECHNICA (Mar. 14, 2019), *available at* <https://arstechnica.com/tech-policy/2019/03/despite-carriers-selling-911-location-data-fcc-ignores-privacy-in-new-rules/>.

<sup>198</sup> Jon Brodtkin, "Selling 911 Location Data is Illegal—US Carriers Reportedly Did It Anyway," ARS TECHNICA (Feb. 13, 2019), *available at* <https://arstechnica.com/tech-policy/2019/02/att-t-mobile-sprint-reportedly-broke-us-law-by-selling-911-location-data/>.

<sup>199</sup> See 47 C.F.R. § 64.2001("The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.").

<sup>200</sup> 47 C.F.R. § 64.2008(b).



187. The individual notice required by the FCA must “provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer’s CPNI.”<sup>201</sup>

188. This notice must include, *inter alia*, “the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.”<sup>202</sup> And, “[t]he notification must be comprehensible and must not be misleading.”<sup>203</sup>

189. AT&T failed to provide proper, individual notice to Plaintiffs and the Class before using, disclosing, or permitting access to their real-time location CPNI by the Aggregator Defendants and other third parties.

**b. The FCA Requires Defendants to Obtain Customers’ Knowing Consent Before Using, Disclosing, or Permitting Access to Location Data.**

190. The FCA gives customers certain rights to control use of and access to their CPNI. The statute generally forbids a carrier to “use, disclose, or permit access to” CPNI, except in limited circumstances.<sup>204</sup>

191. A carrier may only use, disclose, or permit access to customers’ CPNI: (1) as required by law; (2) with the customer’s approval; or (3) in its provision of the telecommunications service from which such information is derived, or services necessary to or used in the provision of such telecommunications service.<sup>205</sup> Beyond such use, “the Commission’s rules require *carriers* to obtain a customer’s *knowing consent* before using or disclosing CPNI.”<sup>206</sup>

192. The knowing consent requirement extends to AT&T’s sharing of CPNI with the Aggregator Defendants. In a 2007 Order, the FCC recognized the risk associated with sharing customer CPNI with third parties. Specifically, the Commission stated:

<sup>201</sup> 47 C.F.R. § 64.2008(c).

<sup>202</sup> 47 C.F.R. § 64.2008(c)(2)(emphasis added).

<sup>203</sup> 47 C.F.R. § 64.2008(c)(4).

<sup>204</sup> 47 U.S.C. § 222(c)(1).

<sup>205</sup> 47 U.S.C. § 222.

<sup>206</sup> 2007 CPNI Order ¶ 8 (emphasis added).

We find that there is a substantial need to limit the sharing of CPNI with others outside a customer's carrier to protect a customer's privacy. . . Specifically, we find that once the CPNI is shared with a joint venture partner or independent contractor, the carrier no longer has control over it and thus the potential for loss of this data is heightened. We find that a carrier's section 222 duty to protect CPNI extends to situations where a carrier shares CPNI with its joint venture partners and independent contractors.<sup>207</sup>

193. The Order further found that “by sharing CPNI with joint venture partners and independent contractors, it is clear that carriers *increase the odds of wrongful disclosure of this sensitive information*, and before the chances of unauthorized disclosure are increased, a customer's *explicit consent* should be required.”<sup>208</sup>

194. On information and belief, AT&T did not obtain such consent before disclosing Plaintiffs' and customers' CPNI to the Aggregator Defendants, nor did AT&T even put the Plaintiffs on notice that their CPNI would be sold to the Aggregator Defendants.

195. In addition to failing to obtain customers' consent before sharing their location data with the Aggregator Defendants, AT&T also failed to obtain consent before allowing the Aggregator Defendants to share the data with *additional* third parties. Instead, AT&T — by its own admission—impermissibly abdicated that responsibility and relied upon an illegal and ineffective, trust-based model to secure customer consent.

196. AT&T admits that it uses the Aggregator Defendants to “facilitate” the sale of its customers' location data and states that it requires the Aggregator Defendants to make their customers (such as Securus) obtain customer consent.<sup>209</sup> However, the plain text of the FCA and its implementing regulations requires the *carrier* to obtain a customer's knowing consent *before* that customer's CPNI is used or disclosed by any third parties, including the Aggregator Defendants.<sup>210</sup>

<sup>207</sup> *Id.* ¶ 39.

<sup>208</sup> *Id.* ¶ 46 (emphasis added).

<sup>209</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15, 2018), *supra* at 51.

<sup>210</sup> 47 U.S.C. § 222(c)(1); 2007 CPNI Order ¶ 8.

1           197. After improperly pushing its duty to obtain consent downstream, AT&T failed to  
2 confirm that the Aggregator Defendants and the Aggregator Defendants' customers (such as  
3 Microbilt, Securus, and CerCareOne) were obtaining consent or proper legal authority before  
4 granting them access to customer location.

5           198. In fact, the Aggregator Defendants' customers were failing to obtain consent or  
6 legal authority before accessing customer CPNI.

7           199. In 2018, AT&T admitted that it knew that Securus "did *not* in fact obtain customer  
8 consent before collecting customers' location information."<sup>211</sup> In a letter to the FCC, Senator  
9 Wyden stated that Securus officials "confirmed... that Securus takes *no steps* to verify" judicial  
10 authorization for real-time location surveillance and failed to conduct "*any review* of surveillance  
11 requests."<sup>212</sup> Indeed, Senator Wyden stated in a letter to AT&T that "[s]enior officials from  
12 Securus have confirmed... that it never checks the legitimacy of those uploaded documents to  
13 determine whether they are in fact court orders and has dismissed suggestions that it is obligated  
14 to do so."<sup>213</sup>

15           200. In the case of Securus, all anyone needed to do to access a carrier customer's  
16 location data was check a box on the Securus portal that stated, "[b]y checking this box, I hereby  
17 certify the attached document is an official document giving permission to look up the location  
18 on this phone number requested."<sup>214</sup> Once that box was checked, the user clicked "Get  
19 Location" and Securus would use the carrier-level location data to immediately provide the  
20 longitude and latitude of the phone's current location, as well as an address.<sup>215</sup> This was the case  
21 even when the documents purporting to show "legal authority" were absurdly deficient on their  
22  
23

24 <sup>211</sup> See, e.g., Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden  
25 (June 15, 2018), *supra* at 51 (emphasis added).

26 <sup>212</sup> Letter from U.S. Senator Ron Wyden to Chairman Ajit Pai (FCC) (May 8, 2018), *supra* at 36.

27 <sup>213</sup> Letter from U.S. Senator Ron Wyden to Randall L. Stephenson (AT&T) (May 8, 2018), *supra*  
at 32.

28 <sup>214</sup> See Hutcheson Indictment at ¶ 6.

<sup>215</sup> *Id.* at ¶ 7.

1 face, such as was the case with former Sheriff Hutcheson, who uploaded inserts from his car  
2 insurance manual as “legal authority” for phone tracking.<sup>216</sup>

3 201. Rather than verify consent or legal authority itself, Securus passed the  
4 responsibility *even further* down the chain and “relied upon law enforcement’s representation  
5 that it had appropriate legal authority[.]”<sup>217</sup>

6 202. In other words, in the case of Securus, the responsibility to confirm that a cell  
7 carrier customer had consented to real-time location tracking was pushed down every rung of the  
8 chain: from AT&T to Location Smart, from LocationSmart to 3Cinteractive, from 3Cinteractive  
9 to Securus, from Securus to correctional facilities, and from those facilities down to individual  
10 officers. Predictably, this system failed to protect AT&T’s customers’ sensitive location data.  
11 AT&T is responsible for this failure.

12 203. Securus was not an isolated incident, but instead, just one example of Defendants’  
13 pattern and practice of failing to assure that *any* consent or legal authority existed before it  
14 allowed third parties to use or access customers’ CPNI.

15 204. For example, CerCareOne allowed more than 250 bail bond companies and  
16 bounty hunters to use carrier data “tens of thousands of times to locate phones” – often without  
17 *any* consent from the customer.<sup>218</sup>

18 205. Additionally, a reporter was able to obtain the precise location information of an  
19 individual—ultimately through Aggregator Defendant Zumigo’s access to cell carrier location  
20 data—without obtaining *any documented* consent from the targeted carrier customer.<sup>219</sup> While  
21 the reporter personally obtained such consent, on information and belief, that consent was in no  
22 way verified by Zumigo or the individual’s cell carrier.

23  
24  
25 <sup>216</sup> *Id.* at ¶ 22.

26 <sup>217</sup> Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron Wyden (June 15,  
2018), *supra* at 51.

27 <sup>218</sup> Joseph Cox, “Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint  
Customer Location Data for Years,” *supra* at 71.

28 <sup>219</sup> Joseph Cox, “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” *supra* at 57.

1           206. In addition to failing to obtain the consent required by the FCA, AT&T also failed  
2 to implement a system that could accurately track consent, as required by the FCA.

3           207. In order to protect customers' rights under the FCA, the FCC has adopted rules  
4 "designed to ensure that telecommunications carriers establish effective safeguards to protect  
5 against unauthorized use or disclosure of CPNI."<sup>220</sup> The FCA requires carriers to "implement a  
6 system by which the status of a customer's CPNI approval can be clearly established *prior to* the  
7 use of CPNI."<sup>221</sup> Carriers must "design their customer service records in such a way that the  
8 status of a customer's CPNI approval can be clearly established."<sup>222</sup> The FCC's rules also  
9 "require carriers to maintain records that track access to customer CPNI records."<sup>223</sup> Carriers  
10 must "maintain a record of all instances where CPNI was disclosed or provided to third parties,  
11 or where third parties were allowed access to CPNI."<sup>224</sup>

12           208. Upon information and belief, AT&T has failed to implement such a system.

13           209. By providing the Aggregator Defendants direct access to customers' location data,  
14 AT&T allowed a chain of handoffs to develop, leading to a robust market for customers' location  
15 data with no oversight by AT&T and continuous violations of AT&T's duties under the FCA to  
16 obtain knowing consent, customer opt-in, or proper legal authority before disclosing its  
17 customers' CPNI to third parties.

18                           **c. Defendants Are Required to Safeguard Customers' Location Data.**

19           210. AT&T has also breached its duty to safeguard Plaintiffs' and Class Members'  
20 CPNI from data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

21           211. In 2007, the FCC "[made] clear that carriers' existing statutory obligations to  
22 protect their customers' CPNI include[s] a requirement that carriers take reasonable steps, which  
23  
24

25           <sup>220</sup> 2007 CPNI Order ¶ 9; *see also Id.* at ¶ 35; 47 U.S.C. § 222(c).

26           <sup>221</sup> 2007 CPNI Order ¶¶ 8-9 (emphasis added); *see also* 47 C.F.R. § 64.2009(a).

27           <sup>222</sup> 2007 CPNI Order ¶ 9.

28           <sup>223</sup> *Id.*

<sup>224</sup> *Id.*; *see also* 47 C.F.R. § 64.2009(c).

1 may include encryption, to protect their CPNI databases from hackers and other unauthorized  
 2 attempts by third parties to access CPNI.”<sup>225</sup>

3 212. LocationSmart’s failure to properly secure its API and prevent unauthorized  
 4 access to customer location data through the demo publicly available on its website is an  
 5 additional breach of the carrier’s duty to safeguard customers’ CPNI. AT&T is responsible for  
 6 this breach because LocationSmart was operating as AT&T’s agent and/or vendor.<sup>226</sup>

7 213. Additionally, AT&T and LocationSmart’s failure to protect its customers’ data—  
 8 thereby resulting in the data becoming accessible over the public internet—is an unjust and  
 9 unreasonable practice under Section 201(b) of the FCA.<sup>227</sup>

10 214. The FCC also requires AT&T to inform customers – and law enforcement –  
 11 “whenever a security breach results in that customer’s CPNI being disclosed to a third party  
 12 without that customer’s authorization.”<sup>228</sup> This requirement extends beyond hacking to any  
 13 unauthorized disclosure. On information and belief, AT&T has failed to inform Plaintiffs that  
 14 their CPNI was disclosed to the Aggregator Defendants or any other relevant third parties.

15 215. In adopting this requirement, the FCC rejected the argument that it “need not  
 16 impose new rules about notice to customers of unauthorized disclosure because competitive  
 17 market conditions will protect CPNI from unauthorized disclosure.”<sup>229</sup>

18 216. Instead, the FCC found that “[i]f customers and law enforcement agencies are  
 19 unaware of [unauthorized access], unauthorized releases of CPNI will have little impact on  
 20 carriers’ behavior, and thus provide little incentive for carriers to prevent further unauthorized  
 21 releases. By mandating the notification process adopted here, we better empower consumers to  
 22 make informed decisions about service providers and assist law enforcement with its  
 23 investigations. This notice will also empower carriers and consumers to take whatever ‘next  
 24

25 <sup>225</sup> 2007 CPNI Order ¶ 36 (citation omitted).

26 <sup>226</sup> *Id.* at ¶ 39; *see also* 47 U.S.C. § 217.

27 <sup>227</sup> *See In the Matter of Terracom, Inc. & Yourtel Am., Inc.*, 29 F.C.C. Rcd. 13325 ¶ 32 (2014).

28 <sup>228</sup> 2007 CPNI Order at ¶ 26; *see also* 47 C.F.R § 64.2011(c).

29 <sup>229</sup> 2007 CPNI Order ¶ 30.

steps' are appropriate in light of the customer's particular situation."<sup>230</sup> The FCC specifically recognized that this notice could allow consumers to take precautions or protect themselves "to avoid stalking or domestic violence."<sup>231</sup>

217. But even after documents *confirmed* that AT&T customers' location data had been accessed by CerCarOne's clients,<sup>232</sup> AT&T stated in February 2019, in a response to Senator Wyden's office, that it had not "identified any use of location information where the location aggregator or another third party obtained AT&T location information without prior customer consent."<sup>233</sup> This statement was untrue.

218. AT&T failed in its duty to safeguard its customers' CPNI from breaches and, upon information and belief, has failed to properly inform affected customers of such breaches when they occurred.

**d. Defendants Are Prohibited from Selling Customers' E911 A-GPS Data for Commercial Use.**

219. AT&T failed to protect customers' A-GPS data from unauthorized commercial use.

220. When the FCC authorized telecommunication carriers, including AT&T, to use A-GPS technology for E911 purposes, it required the carriers to certify that "*any data associated with the NEAD* may not be used for *any* non-911 purpose, except as otherwise required by law."<sup>234</sup>

221. While the collection and use of A-GPS data was allowed under the E911 and public safety exceptions of the FCA, any *other* use would violate the FCA and its corresponding regulations.

---

<sup>230</sup> *Id.*

<sup>231</sup> *Id.* at n. 100.

<sup>232</sup> Joseph Cox, "Hundreds of Bounty Hunters Had Access to AT&T, T-Mobile, and Sprint Customer Location Data for Years," *supra* at 71.

<sup>233</sup> Letter from Timothy P. McKone to U.S. Senator Ron Wyden (Feb. 15, 2019), *supra* at 7.

<sup>234</sup> NEAD Implementation Order ¶ 13 (emphasis added).

222. As industry documents confirm, AT&T allows bounty hunters, bail bondsmen, and other third parties to access customers' precise, real-time A-GPS data.<sup>235</sup>

223. This A-GPS data is data associated with the NEAD, and thus commercial sale of the data violates federal law.

224. In a letter to AT&T Communications CEO John Donovan, FCC Commissioner Jessica Rosenworcel stated, "[u]nder federal law, A-GPS data included in the [NEAD] Database for enhanced 911 services may not be used for any other purpose."<sup>236</sup>

225. This commercialization of data associated with the NEAD is in direct violation of FCC regulations.

**iii. AT&T Has Acknowledged Plaintiffs' Right to Privacy in their Proprietary Information.**

226. AT&T recognizes that its customers, including Plaintiffs, have an expectation of privacy in their proprietary data.

227. As AT&T admits to its customers, "It is your right and our duty under federal law to protect the confidentiality of your CPNI."<sup>237</sup>

228. AT&T has also previously faced an FCC enforcement action, and paid a \$25 million civil penalty, for violations of customers' privacy.<sup>238</sup> In 2015, the FCC found that AT&T failed to properly protect the confidentiality of almost 280,000 customers' CPNI in connection with data breaches at AT&T call centers in Mexico, Columbia, and Philippines.<sup>239</sup> AT&T employees had improperly used login credentials to access customer accounts and access

<sup>235</sup> "Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls," *supra* at 71.

<sup>236</sup> Letter from Commissioner Jessica Rosenworcel to John Donovan (CEO AT&T Communications) (May 1, 2019), *available at* <https://www.documentcloud.org/documents/5985428-FCC-Commissioner-Rosenworcel-letters-to-Telecom.html>.

<sup>237</sup> "Customer Proprietary Network Information (CPNI)," AT&T, *available at* [https://about.att.com/sites/privacy\\_policy/rights\\_choices?\\_gl=1\\*8s6v9t\\*\\_gcl\\_dc\\*R0NMLjE1NTQxMzU4MTEuQ0pqNHhJR25yLUVDRIZIOHN3b2R6RWJLWc.#cpni](https://about.att.com/sites/privacy_policy/rights_choices?_gl=1*8s6v9t*_gcl_dc*R0NMLjE1NTQxMzU4MTEuQ0pqNHhJR25yLUVDRIZIOHN3b2R6RWJLWc.#cpni).

<sup>238</sup> *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015).

<sup>239</sup> *Id.* at ¶ 1.



customer information that could be used to unlock the customers' devices.<sup>240</sup> The employees then sold the information they obtained from the breaches to a third party.<sup>241</sup>

229. The FCC concluded that AT&T's "failure to reasonably secure customers' proprietary information violates a carrier's statutory duty under Communications Act to protect that information, and also constitutes an unjust and unreasonable practice in violation of the Act."<sup>242</sup>

230. The FCC stressed that the FCA is intended to "ensure that consumers can trust that carriers have taken appropriate steps to ensure that unauthorized persons are not accessing, viewing or misusing their personal information."<sup>243</sup> It stressed its expectation that "telecommunications carriers such as AT&T... take 'every reasonable precaution' to protect their customers' data[.]"<sup>244</sup>

231. As a condition of its stipulated Consent Decree, AT&T agreed to develop and implement a compliance plan to ensure appropriate safeguards to protect consumers against similar breaches by improving its privacy and data security practices.<sup>245</sup>

232. This FCC enforcement action underscores AT&T's familiarity with the sensitive nature of customer CPNI, and its duties to protect and safeguard that data.

#### **H. AT&T's Misrepresentations and Omissions Concerning the Sale of Customer Location Data.**

233. AT&T's false representations concerning sale of access to Plaintiffs' and Class members' real-time location data compounds the outrageousness of its conduct.

234. AT&T's Privacy Policy, and the "Privacy Commitments" included therein, falsely represents and fails to disclose material information about its routine sale of access to customers' location data.

---

<sup>240</sup> *Id.* at ¶¶ 7, 11.

<sup>241</sup> *Id.* at ¶ 1.

<sup>242</sup> *Id.* at ¶ 2.

<sup>243</sup> *Id.*

<sup>244</sup> *Id.*

<sup>245</sup> *Id.* at ¶¶ 2, 17-18, 21.

235. In its Privacy Policy, AT&T promises not to sell customers' personal information and to protect customers' privacy and personal information. AT&T further pledges that it will allow Plaintiffs and Class members to control how their data is used. These representations created an expectation among Plaintiffs and Class members that their real-time location data would not be sold, that such data would be protected from unauthorized disclosure, and that they could control how and when such data was accessed. Figure 4, immediately below, is an excerpt from AT&T's Privacy Policy.

## Our Privacy Commitments

**Our privacy commitments are fundamental to the way we do business every day. These apply to everyone who has a relationship with us - including customers (wireless, Internet, digital TV, and telephone) and Web site visitors.**

- We will protect your privacy and keep your personal information safe. We use encryption and other security safeguards to protect customer data.
- We will not sell your personal information to anyone, for any purpose. Period.
- We will fully disclose our privacy policy in plain language, and make our policy easily accessible to you.
- We will notify you of revisions to our privacy policy, in advance. No surprises.
- You have choices about how AT&T uses your information for marketing purposes. Customers are in control.
- We want to hear from you. You can send us questions or feedback on our privacy policy.

*Figure 4<sup>246</sup>*

236. AT&T's representation that it "use[s] encryption and other security safeguards to protect customer data" is false and misleading.

<sup>246</sup> "Our Privacy Commitments," AT&T (Feb. 15, 2019), *available at* [https://about.att.com/sites/privacy\\_policy](https://about.att.com/sites/privacy_policy).

1           237. As alleged above in Section B, AT&T allowed its agent LocationSmart to store  
 2 customers' personal information—in the form of real-time location data—in a manner that  
 3 allowed it to be easily accessed without any customer consent or legal authority by “[a]nyone  
 4 with a modicum of knowledge about how Web sites work[.]”<sup>247</sup> AT&T's statement that it would  
 5 use encryption and other security safeguards to protect customers' data is therefore a material  
 6 misrepresentation.

7           238. As alleged above in Section E, AT&T failed to establish a consent mechanism  
 8 that verified proper authorization before customers' location data was disclosed to third parties.  
 9 AT&T's statement that it would use encryption and other security safeguards to protect  
 10 customers' data is therefore a material misrepresentation.

11           239. AT&T's representation that it “will protect [customers'] privacy and keep [their]  
 12 personal information safe” is false and misleading.

13           240. As alleged above in Section E, AT&T failed to establish a consent mechanism  
 14 that verified proper authorization before customers' location data was disclosed to third parties.  
 15 Real-time location data is personal information. AT&T's statement that it would protect  
 16 customers' privacy and keep their personal information safe is therefore a material  
 17 misrepresentation.

18           241. AT&T's representation that it “will not sell [customers'] personal information to  
 19 anyone, for any purpose. Period” is false and misleading.

20           242. As alleged above in Sections C-E, AT&T routinely sold access to customers' real-  
 21 time location data to the Aggregator Defendants and countless additional third parties. Real-time  
 22 location data is personal information. AT&T's statement that it would not sell customers'  
 23 personal information is therefore a material misrepresentation.

24           243. AT&T also makes numerous false or misleading representations concerning its  
 25 treatment of customers' data that qualifies as CPNI under the FCA.

26  
 27  
 28 <sup>247</sup> Brian Krebs, “Tracking Firm LocationSmart Leaked Location Data for Customers of All  
 Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site,” *supra* at 42.

1           244. AT&T explicitly and falsely represents to customers in its Privacy Policy that it  
2 does not “sell, trade or share” their CPNI without legal authority:

3                   We do not sell, trade or share your CPNI with anyone outside of  
4 the AT&T family of companies\* or our authorized agents, unless  
5 required by law (example: a court order).<sup>248</sup>

6           245. As alleged above in Sections B-E, AT&T routinely provided access to customers’  
7 CPNI, in the form of real-time location information to additional third parties through the  
8 Aggregator Defendants. This use was not required by law.

9           246. AT&T also states that it only uses CPNI “internally” and its *only* disclosed use of  
10 CPNI is “among the AT&T companies and our agents in order to offer you new or enhanced  
11 services.”<sup>249</sup>

12           247. Additionally, while the Aggregator Defendants are AT&T’s agents, the use of  
13 customer location data described herein was not for “internal” AT&T purposes, nor was it used  
14 to market AT&T services to Plaintiffs and Class members. AT&T’s statements regarding the sale  
15 and/or use of customer CPNI are therefore material misrepresentations. Its failure to disclose its  
16 sale of access to customers’ CPNI, in the form of location data, is a material omission.

17           248. AT&T also falsely represents that it “uses technology and security features, and  
18 strict policy guidelines with ourselves and our agents, to safeguard the privacy of CPNI.”<sup>250</sup>

19           249. As alleged above in Section B, AT&T’s agent, LocationSmart, did not  
20 appropriately safeguard the privacy of AT&T customers’ CPNI. Instead, it stored customer CPNI  
21 in such a way that unauthorized access was easily obtained by “[a]nyone with a modicum of  
22 knowledge about how Web sites work.”<sup>251</sup> AT&T’s statements regarding the technology and  
23 security features it uses to safeguard customer CPNI are therefore material misrepresentations.

24 <sup>248</sup> Ex. A (privacy policy) at 31. The “AT&T family of companies” is defined “those companies  
25 that provide voice, video and broadband-related products and/or services domestically and  
26 internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T  
27 Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design,  
28 market, or sell these products and/or services.” *Id.* at 32.

<sup>249</sup> *Id.* at 32.

<sup>250</sup> *Id.*

<sup>251</sup> Brian Krebs, “Tracking Firm LocationSmart Leaked Location Data for Customers of All  
Major U.S. Mobile Carriers Without Consent in Real Time Via Its Web Site,” *supra* at 42.

1           250. As alleged above in Section C, AT&T and its agent, LocationSmart, also failed to  
 2 safeguard customers' CPNI when they provided access to customer location data to companies  
 3 who failed to obtain consent or valid legal authority for such access. AT&T's statements  
 4 regarding the technology and security features it uses to safeguard customer CPNI are therefore  
 5 material misrepresentations.

6           251. AT&T has admitted that its customers' location data was used in ways that  
 7 violated its policies. A spokesperson for AT&T admitted that the sale of location data to bounty  
 8 hunters "would violate [AT&T's] contract and Privacy Policy."<sup>252</sup>

9           252. In response to public reporting about its routine sale of customers' real-time  
 10 location data, AT&T made numerous false public statements.

11           253. AT&T repeatedly asserted that, despite its sale of customers' real-time location  
 12 data, it protected Plaintiffs and its customers from unauthorized use of their location data by only  
 13 releasing such data when presented with customer consent or proper legal authority.<sup>253</sup> As  
 14 alleged in Section E, this representation was false.

15           254. Moreover, AT&T repeatedly represented that it would stop selling access to  
 16 Plaintiffs' and similarly situated customers' location data to the Aggregator Defendants and all  
 17 third parties. These representations were false.

18           255. In June 2018, AT&T stated that it had taken "prompt steps to protect customer  
 19 data" and ended Securus' access to customer location data.<sup>254</sup> In a public statement around the  
 20 same time, AT&T stated that its "top priority [was] to protect our customers' information and, to  
 21 that end, *[it would] be ending [its] work with aggregators* for these services as soon as practical  
 22  
 23

24 <sup>252</sup> Joseph Cox, "I Gave a Bounty Hunter \$300. Then He Located Our Phone," *supra* at 57.

25 <sup>253</sup> In a June 2018 letter to Senator Wyden's office, AT&T represented that it "authorized third  
 26 parties to access customer location data... only where a customer consents to such disclosure  
 27 except in limited cases where a specific provision of law or regulation requires or authorizes  
 28 access." See Letter from Timothy P. McKone (AT&T Services, Inc.) to U.S. Senator Ron  
 Wyden (June 15, 2018), *supra* at 51.

<sup>254</sup> *Id.*

1 in a way that preserves important, potential lifesaving services like emergency roadside  
2 assistance.”<sup>255</sup>

3 256. But on January 10, 2019, AT&T admitted that it had *not* ended the sale of real-  
4 time location data to location aggregators—despite its statements in June 2018 to the contrary—  
5 but insisted that it was now planning to end all customer location data sales in response to the  
6 January 2019 reporting.<sup>256</sup> But AT&T again hedged, estimating the sales would not conclude  
7 until March 2019.<sup>257</sup>

8 257. AT&T’s sale of customer location data continued. As Senator Wyden explained,  
9 “[w]e catch them in 2018, they claim that they’re going to stop—not a whole lot of qualifiers,  
10 they just say, ‘We’re going to stop’—and then we had Joe Cox and the good folks at  
11 Motherboard basically get a bounty hunter, give them a couple hundred bucks, and we saw that  
12 at least three of the four major carriers [including AT&T] had basically fed the American  
13 consumer a bunch of baloney.”<sup>258</sup> “[T]hey made these promises to me in writing in 2018. Now,  
14 they’re making these promises again, and so... permit me to be a little bit skeptical. I’ll believe it  
15 when I actually see it. And there is a real pattern now in the technology space where essentially  
16 these companies get caught in irresponsible conduct... they apologize... and they pledge it won’t  
17 happen again. But of course, it does it happen again. You can almost set your clock by it.”<sup>259</sup>

18  
19 <sup>255</sup> Jon Brodtkin, “Verizon and AT&T Will Stop Selling Your Phone’s Location to Data  
20 Brokers,” ARS TECHNICA (June 19, 2018), *available at* [https://arstechnica.com/tech-  
21 policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/](https://arstechnica.com/tech-policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/); Brian  
22 Fung, “Verizon, AT&T, T-Mobile and Sprint Suspend Selling of Customer Location Data After  
23 Prison Officials Were Caught Misusing It,” THE WASHINGTON POST (June 19, 2018), *available  
24 at* [https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-  
25 of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-  
26 it/?noredirect=on&utm\\_term=.4f7da64c1108](https://www.washingtonpost.com/news/the-switch/wp/2018/06/19/verizon-will-suspend-sales-of-customer-location-data-after-a-prison-phone-company-was-caught-misusing-it/?noredirect=on&utm_term=.4f7da64c1108).

27 <sup>256</sup> Joseph Cox, “Google Demanded That T-Mobile, Sprint Not Sell Google Fi Customers’  
28 Location Data,” MOTHERBOARD (Jan. 11, 2019), *available at* [https://motherboard.vice.com/en\\_us/article/d3bnyv/google-demanded-tmobile-sprint-to-not-sell-  
29 google-fi-customers-location-data](https://motherboard.vice.com/en_us/article/d3bnyv/google-demanded-tmobile-sprint-to-not-sell-google-fi-customers-location-data).

30 <sup>257</sup> Alfred Ng, “AT&T is Cutting Off All Location-Data Sharing Ties in March,” CNET (Jan. 11,  
31 2019), *available at* [https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-  
32 by-march/](https://www.cnet.com/news/at-t-is-cutting-off-all-location-data-sharing-ties-by-march/).

33 <sup>258</sup> “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” Cyber Podcast, *supra* at 113.

34 <sup>259</sup> *Id.*

1           258. Plaintiffs and AT&T customers therefore have no reason to believe AT&T's  
2 continuous representations that it would or will end the sale of real-time location data are  
3 credible.

4           259. Public reporting also shows that AT&T's representations throughout 2018 and  
5 early 2019—that sales of customers' location data were isolated incidents—were false, and were  
6 intended to conceal the nature and scope of AT&T's location data practices.

7           260. In response to the latest round of reporting in February and March of 2019,  
8 Senator Wyden stressed the wireless carriers' misrepresentations about the sale of their  
9 customers' location data. "Carriers assured customers location tracking abuses were isolated  
10 incidents. Now it appears that hundreds of people could track our phones, and they were doing it  
11 for years before anyone at the wireless companies took action," the Senator stated.<sup>260</sup> "That's  
12 more than an oversight—that's flagrant, wil[1]ful disregard for the safety and security of  
13 Americans."<sup>261</sup>

14           261. AT&T's misrepresentations and omissions concerning its sale of access to and  
15 safeguarding of customers' real-time location data were material. As alleged in Section G, a  
16 reasonable person would attach importance to the privacy of her sensitive location data in  
17 determining whether to contract with a wireless cell phone provider.

18           262. AT&T was obligated to disclose the nature of its location data sales practices, as  
19 AT&T had exclusive knowledge of material facts not known or knowable to its customers, AT&T  
20 actively concealed these material facts from its customers, and such disclosures were necessary  
21 to materially qualify its representations that it did not sell and took measures to protect consumer  
22 data and its partial disclosures concerning its use of customers' CPNI. Further, AT&T was  
23 obligated to disclose its practices under the FCA.

24           263. A reasonable person would be deceived and misled by AT&T's  
25 misrepresentations, which clearly indicated that AT&T would not sell, and would in fact  
26

27 <sup>260</sup> Joseph Cox, "Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911  
28 Calls," *supra* at 71.

<sup>261</sup> *Id.*



1 safeguard, its customers' personal information and CPNI. Reasonableness is heightened here,  
 2 where AT&T purported to disclose the uses for which it accessed customers' CPNI but failed to  
 3 include therein the location data sales described herein, making its partial representations likely  
 4 to mislead or deceive.

5 264. AT&T intentionally misled its customers regarding its location data practices in  
 6 order to attract customers and evade prosecution for its unlawful acts, while also profiting  
 7 unfairly from the sale of customer location data.

8 265. AT&T's representations in its privacy policies that it protected customers'  
 9 personal information, when in fact it did not, were false, deceptive, and misleading and therefore  
 10 a violation of Section 201(b) of the FCA.<sup>262</sup>

#### 11 **I. Fraudulent Concealment and Tolling.**

12 266. The applicable statutes of limitations are tolled by virtue of Defendants' knowing  
 13 and active concealment of the facts alleged above.

14 267. Plaintiffs and Class members were ignorant of the information essential to the  
 15 pursuit of these claims, without any fault or lack of diligence on their own part. The sale of  
 16 location data, as detailed in this complaint, was not known or knowable to AT&T customers and  
 17 occurred invisibly to them when using their phones. Due to the surreptitious nature of  
 18 Defendants' activities, they were difficult if not impossible for Plaintiffs and other AT&T  
 19 customers to discover.

20 268. At the time the action was filed, Defendants were under a duty to disclose the true  
 21 character, quality, and nature of their activities to Plaintiffs and Class members. Defendants are  
 22 therefore estopped from relying on any statute of limitations.

23 269. Defendants' fraudulent concealment is common to the class.

#### 24 **J. Named Plaintiff Allegations.**

25 270. Plaintiffs Scott, Jewel, and Pontis did not know—and indeed could not have  
 26 known—and did not consent to AT&T's sale of their sensitive, real-time location data to the  
 27 Aggregator Defendants and other third parties.

28 <sup>262</sup> See *In the Matter of Terracom, Inc. & Yourtel Am., Inc.*, 29 F.C.C. Rcd. 13325 ¶ 12 (2014).



1           271. When selecting and maintaining their AT&T wireless accounts, Plaintiffs relied  
2 upon their reasonable expectation—established at least in significant part by AT&T’s own  
3 representations—that their data would be safeguarded by AT&T and would not be sold.

4           272. Plaintiffs are highly privacy-conscious individuals who place value in their ability  
5 to select when and how their location data is used and by whom. Had Plaintiffs known about  
6 the real-time location practices complained of herein, they would not have signed up for AT&T  
7 wireless cell phone service or would have paid less for its services.

8           273. Plaintiffs were also harmed by the (i) unauthorized use of their AT&T wireless  
9 data, and (ii) the resulting drains on their devices’ battery.

10           274. Plaintiffs pay for a limited amount of mobile data from AT&T each month. As  
11 LocationSmart admits, when a device’s real-time location is accessed, “data or messaging  
12 charges may be incurred” by the customer, including Plaintiffs.<sup>263</sup> LocationSmart makes clear  
13 that a third-party’s “location request may use data services to deliver data from the phone to the  
14 carrier network in response to a location request, which may incur data charges according to the  
15 individual’s wireless service plan.”<sup>264</sup> As a result, in addition to having their private locations  
16 accessed, Plaintiffs and Class members are not getting the optimal performance of the mobile  
17 devices and carrier data packages they purchased, and which are marketed, in part, based on their  
18 speed, performance, and battery life.

19           275. Plaintiffs were also harmed by Defendants’ failure to adopt reasonable security  
20 practices to reduce the risk of theft of their personal data. As California courts have recognized,  
21 a company’s security practices have economic value. In subscribing to AT&T wireless services,  
22 Plaintiffs were informed of and relied upon AT&T’s assertions that it and its partners would  
23 safeguard their data. Had Plaintiffs known that AT&T would not properly safeguard their real-  
24 time location data, Plaintiffs would not have subscribed to AT&T wireless services, or would  
25 have paid less for those services.

## 26       **V. CLASS ALLEGATIONS**

27  
28 <sup>263</sup> “FAQs,” LocationSmart, *supra* at 89.

<sup>264</sup> *Id.*

1           276. Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil  
2 Procedure, individually and on behalf of all members of the following class (“Class”):

3           All natural persons who were or are AT&T wireless subscribers  
4           residing in California between 2011 and the present and whose  
5           carrier-level location data AT&T permitted or caused to be used or  
6           accessed by any third party without proper authorization.

7           277. Excluded from the Class are the following individuals: officers and directors of  
8 any Defendant and its parents, subsidiaries, affiliates, and any entity in which any Defendant has  
9 a controlling interest, and all judges assigned to hear any aspect of this litigation, as well as their  
10 immediate family members.

11           278. Plaintiffs Carolyn Jewel, Katherine Scott, and George Pontis seek to represent the  
12 Class.

13           279. This action readily satisfies the requirements set forth under Federal Rule of Civil  
14 Procedure 23:

15           a. The Class is so numerous that joinder of all members is impracticable. Upon  
16 information and belief, Class members number in the millions.

17           b. The Class is readily ascertainable, as each member is or was a customer of AT&T,  
18 and thus can be identified by AT&T’s business records and related documents.

19           c. There are questions of law or fact common to the Class. These questions include,  
20 but are not limited to, the following:

- 21           i. Whether the Aggregator Defendants acted as agents of AT&T;
- 22           ii. Whether AT&T and its agents’ acts, omissions, and practices complained  
23           of herein amount to a violation of their duty to protect their customers’  
24           CPNI, in violation of the FCA;
- 25           iii. Whether the location data described herein is “CPNI” under the FCA;
- 26           iv. Whether AT&T properly obtained consent and/or legal authority before  
27           allowing the Aggregator Defendants to access Plaintiffs’ and Class  
28           members’ CPNI;

- v. Whether AT&T and its agents properly obtained consent and/or legal authority before allowing third parties to access Plaintiffs' and Class members' CPNI;
- vi. Whether AT&T provided proper notice before accessing or permitting others to access Plaintiffs' and Class members' CPNI;
- vii. Whether Defendants' act and practices complained of herein amount to egregious breaches of social norms;
- viii. Whether Defendants acted intentionally in violating Plaintiffs' and Class members' privacy rights;
- ix. Whether AT&T and its agents had a duty to Plaintiffs and Class members to protect their location data, and if so, whether AT&T and/or its agents breached that duty;
- x. Whether AT&T made material misrepresentations or omissions to Plaintiffs and Class members;
- xi. Whether public injunctive relief should issue;
- xii. Whether Defendants fraudulently concealed their location data practices complained of herein;
- xiii. The appropriate amount of damages owed to Plaintiffs and the Class;
- xiv. Whether declaratory relief should be granted.

d. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class members, are AT&T subscribers whose privacy rights were violated and who were subjected to the deceptive conduct alleged herein.

e. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' interests do not conflict with the interests of the Class members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation, generally, and consumer privacy litigation, specifically. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Class.

1 f. Questions of law or fact common to the Class—including but not limited to the  
2 common questions outlined above—predominate over any questions affecting only individual  
3 Class members or Plaintiffs.

4 g. A class action is superior to other available methods for fairly and efficiently  
5 adjudicating the controversy complained of herein.

6 h. Like all Class members, Plaintiffs suffer a substantial risk of repeated injury in  
7 the future. AT&T has made repeated misrepresentations about when it would end the privacy-  
8 violative acts complained of herein, and how. Due to these continuous misrepresentations,  
9 Plaintiffs have no basis to believe that AT&T will cease its practices on a voluntary basis, and  
10 seek injunctive relief to protect the privacy rights of themselves and the Class of California  
11 consumers. Additionally, AT&T has not made any assurances that Plaintiffs' and Class members'  
12 historical location data will be properly secured.

13 i. In acting as alleged above, Defendants have acted on ground generally applicable  
14 to the entire Class, thereby making relief appropriate with respect to the Class as a whole. The  
15 prosecution of separate actions by individual Class members would create the risk of inconsistent  
16 or varying adjudications with respect to individual Class members that would establish  
17 incompatible standards of conduct for Defendants.

18 j. Injunctive relief is necessary to prevent further unlawful and unfair conduct by  
19 Defendants. Money damages, alone, could not afford adequate and complete relief, and  
20 injunctive relief is necessary to restrain Defendants from continuing to or commit its illegal and  
21 unfair violations of privacy and to require Defendants to take accurate steps to ensure that any  
22 current or historical location data is properly safeguarded and secured.

## 23 **VI. CLAIMS FOR RELIEF**

### 24 **COUNT I**

#### 25 **Violations of The Communications Act, 47 U.S.C. § 201 *et seq.*** 26 **(As to Defendant AT&T)**

27 280. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully  
28 set forth in this cause of action.

1           281. AT&T has violated 47 U.S.C. § 222(a) by failing to protect the confidentiality of  
2 Plaintiffs' and Class members' CPNI in the form of precise, real-time location data, as detailed  
3 herein. AT&T has also caused and/or permitted the Aggregator Defendants to fail to protect  
4 Plaintiffs' and Class members' precise, real-time location data, as detailed herein.

5           282. AT&T has violated 47 U.S.C. § 222(c) by using, disclosing, and/or permitting  
6 access to Plaintiffs' and Class members' CPNI in the form of precise, real-time location  
7 information to the Aggregator Defendants and other third parties without the notice, consent,  
8 and/or legal authorization required under the FCA, as detailed herein. AT&T also caused and/or  
9 permitted the Aggregator Defendants and other third parties to use, disclose, and/or permit access  
10 to Plaintiffs' and Class members' CPNI in the form of precise, real-time location information  
11 without the notice, consent, and/or legal authorization required under the FCA, as detailed  
12 herein.

13           283. AT&T has violated 47 U.S.C. § 222(f) by using, disclosing, and/or permitting  
14 access to Plaintiffs' and Class members' geolocation data without the express prior authorization  
15 of Plaintiffs and Class members, as detailed herein. AT&T has also caused and/or permitted the  
16 Aggregator Defendants to use, disclose, and/or permit access to Plaintiffs' and Class members'  
17 geolocation data without the express prior authorization of Plaintiffs and Class members, in  
18 violation of the FCA.

19           284. Plaintiffs and Class members have suffered injury to their person, property,  
20 health, and/or reputation as a consequence of AT&T's violations of the FCA. Plaintiffs and  
21 Class members have been harmed by the unauthorized access to their CPNI and personal  
22 information, the use of their wireless data—which they purchased from Defendant AT&T—  
23 without their consent, and AT&T's failure to secure any past location data obtained about the  
24 Plaintiffs. Additionally, Plaintiffs and Class members have suffered emotional damages,  
25 including emotional distress, mental anguish, and suffering, as a result of Defendants' acts and  
26 practices. Plaintiffs would not have purchased, or would have paid less for, AT&T wireless  
27 services had they known their location data could be sold to third parties.  
28



1           290. A reasonable person would be deceived and misled by AT&T's  
2 misrepresentations, which indicated that AT&T would not sell, and would in fact safeguard, its  
3 customers' personal and proprietary information. Reasonableness is heightened here, where  
4 AT&T purported to disclose the uses for which it accessed customers' CPNI but failed to include  
5 the location data sales described here, making its partial representations likely to mislead or  
6 deceive.

7           291. AT&T intentionally misled its customers regarding its location data practices in  
8 order to attract customers and evade prosecution for its unlawful acts, while also profiting  
9 unfairly from the sale of customer location data.

10           292. Defendants' actions detailed herein constitute an unlawful business act or practice.  
11 As alleged herein, Defendants' conduct is a violation of the California constitutional right to  
12 privacy, the FCA, the CLRA, and constitutes an intrusion upon seclusion.

13           293. Defendants' actions detailed herein constitute an unfair business act or practice.

14           294. Defendants' conduct lacks reasonable and legitimate justification in that  
15 Defendants have benefited from such conduct and practices, while Plaintiffs and Class members  
16 have been misled as to the nature and integrity of Defendants' goods and services and have, in  
17 fact, suffered injury regarding the privacy and confidentiality of their location information and  
18 the use of their device resources.

19           295. The gravity of the harm of AT&T's practices—the violations to consumers'  
20 reasonable expectations or privacy, as well as customers' loss of property and/or money—far  
21 outweigh the utility of Defendants' conduct, which was largely a profit-making scheme.  
22 Defendants' practices were contrary to the letter and the spirit of the FCA and its corresponding  
23 regulations, which require cell carriers to only disclose customers' CPNI upon proper notice,  
24 consent, and authorization, and aims to vest carrier customers with control over their data. Due  
25 to the surreptitious nature of Defendants' actions, Plaintiffs and Class members could not have  
26 reasonably avoided—and still cannot reasonably avoid—the privacy and economic harms  
27 incurred as a result.  
28

298. As established herein, Plaintiffs have suffered injury in fact and economic harm as a result of AT&T's unfair competition. Had AT&T disclosed the true nature and extent of its sale of access to its customers' real-time location data and the effect such practices had on customers' data plans, batteries, and privacy, Plaintiffs would have been aware and would not have subscribed to or paid as much money for AT&T's wireless services.

**COUNT III**  
**Intrusion Upon Seclusion**  
**(As to All Defendants)**

301. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.” Restatement (Second) of Torts, § 652B.



1           302. Plaintiffs and Class members have reasonable expectations of privacy in their  
2 mobile devices and their location data.

3           303. The reasonableness of Plaintiffs' and Class members' expectations of privacy is  
4 supported by AT&T and its agents'—the Aggregator Defendants'—unique position to monitor  
5 Plaintiffs' and Class members' behavior through its access to Plaintiffs' and Class members'  
6 private mobile devices. It is further supported by the surreptitious and non-intuitive nature of  
7 Defendants' tracking.

8           304. Defendants intentionally intruded on and into Plaintiffs' and Class members'  
9 solitude, seclusion, or private affairs by allowing third parties to access Plaintiffs' and Class  
10 members' real-time location without proper notice, consent, or authority.

11           305. These intrusions are highly offensive to a reasonable person. This is evidenced by  
12 federal legislation enacted by Congress, state constitutional law, common law, Supreme Court  
13 precedent, rules promulgated and enforcement actions undertaken by the FCC, and countless  
14 studies, op-eds, and articles decrying surreptitious location tracking.

15           306. The offensiveness of Defendants' conduct is heightened by AT&T's material  
16 misrepresentations to Plaintiffs and Class Members concerning the sale, security, and  
17 safeguarding of their location data, as alleged above.

18           307. Plaintiffs and Class members were harmed by the intrusion into their private  
19 affairs, as detailed throughout this Complaint.

20           308. Defendants' actions and conduct complained of herein were a substantial factor in  
21 causing the harm suffered by Plaintiffs and Class members.

22           309. As a result of Defendants' actions, Plaintiffs and Class members seek damages  
23 and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek  
24 punitive damages because Defendants' actions—which were malicious, oppressive, and willful—  
25 were calculated to injure Plaintiffs and Class members and made in conscious disregard of  
26 Plaintiffs' and Class members' rights. Punitive damages are warranted to deter the Defendants  
27 from engaging in future misconduct.  
28

310. Plaintiffs seek restitution for the unjust enrichment obtained by Defendants as a result of unlawfully collecting Plaintiffs' location data. These intrusions are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiffs' and Class members' personal information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously track Plaintiffs and Class members and to allow third parties to do the same, all for the sake of profit.

311. Plaintiffs, individually and on behalf of the Class, seek the full amount of damages sustained by Plaintiffs and Class members as a consequence of AT&T's intrusion upon their seclusion, as well as declaratory and injunctive relief.

**COUNT IV**  
**Violations of the California Constitutional Right to Privacy**  
**(As to All Defendants)**

312. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully set forth in this cause of action.

313. The California Constitution declares that “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” Cal. Const. Art. I, § 1.

314. Plaintiffs' and Class members' have a reasonable expectation of privacy in their location data.

315. Defendants intentionally intruded on and into Plaintiffs' and Class members' solitude, seclusion, or private affairs by allowing third parties, including the Aggregator Defendants, to access Plaintiffs' and Class members' real-time location without proper consent or authority.

316. The reasonableness of Plaintiffs' and Class members' expectations of privacy is supported by AT&T and its agents'—the Aggregator Defendants'—unique position to monitor Plaintiffs' and Class members' behavior through its access to Plaintiffs' and Class members'

1 private mobile devices. It is further supported by the surreptitious nature of Defendants'  
2 tracking.

3 317. These intrusions are highly offensive to a reasonable person. This is evidenced by  
4 federal legislation enacted by Congress, state constitutional law, common law, Supreme Court  
5 precedent, rules promulgated and enforcement actions undertaken by the FCC, and countless  
6 studies, op-eds, and articles decrying surreptitious location tracking.

7 318. The offensiveness of Defendants' conduct is heightened by AT&T's material  
8 misrepresentations to Plaintiffs and Class Members concerning the sale, security, and  
9 safeguarding of their location data.

10 319. Plaintiffs and Class members were harmed by the intrusion into their private  
11 affairs as detailed throughout this Complaint.

12 320. Defendants' actions and conduct complained of herein were a substantial factor in  
13 causing the harm suffered by Plaintiffs and Class members.

14 321. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and  
15 punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek  
16 punitive damages because Defendants' actions—which were malicious, oppressive, willful—  
17 were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive  
18 damages are warranted to deter Defendants from engaging in future misconduct.

19 **COUNT V**  
20 **(Negligence)**  
**(As to Defendant AT&T)**

21 322. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully  
22 set forth in this cause of action.

23 323. AT&T owed a duty to Plaintiffs and Class members—arising from the sensitivity  
24 of real-time location data and the foreseeability of harm to Plaintiffs and Class members should  
25 AT&T fail to safeguard and protect such data—to exercise reasonable care in safeguarding their  
26 sensitive personal information. This duty included, among other things, designing, maintaining,  
27 monitoring, and testing AT&T's and its agents', partners', and independent contractors' systems,  
28

1 protocols, and practices to ensure that Plaintiffs' and Class members' information was adequately  
2 secured from unauthorized access.

3 324. AT&T's privacy policies acknowledged its duty to adequately protect Plaintiffs'  
4 and Class members' location data.

5 325. AT&T owed a duty to Plaintiffs and Class members to implement a system to  
6 safeguard against and detect unauthorized access to Plaintiffs' and Class members' data in a  
7 timely manner.

8 326. AT&T owed a duty to disclose the material fact that its data security practices  
9 were inadequate to safeguard Plaintiffs' and Class members' location data from unauthorized  
10 access and that it was allowing access to Plaintiffs' and Class members' location data to the  
11 Aggregator Defendants and other third parties, as detailed herein.

12 327. AT&T had independent duties under the FCA and its corresponding regulations,  
13 as detailed above in Section G, which required AT&T to reasonably safeguard Plaintiffs' and  
14 Class members' location data and promptly notify them of any unauthorized accesses.

15 328. AT&T had a special relationship with Plaintiffs and Class members due to its  
16 status as their telecommunications carrier, which provided an independent duty of care.  
17 Plaintiffs' and other Class members' willingness to contract with AT&T, and thereby entrust  
18 AT&T with their location data, was predicated on the understanding that AT&T would undertake  
19 adequate security and consent precautions. Moreover, AT&T had the ability to protect its  
20 systems and the location data it stored on them from unauthorized access.

21 329. AT&T breached its duties by, *inter alia*: (a) failing to implement and maintain  
22 adequate security practices to safeguard Plaintiffs' and Class members' location data; (b) failing  
23 to detect unauthorized accesses in a timely manner; (c) failing to disclose that AT&T's data  
24 security practices were inadequate to safeguard Plaintiffs' and Class members' location data; (d)  
25 failing to provide adequate and timely notice of unauthorized access; and (e) failing to disclose  
26 its sale of access to Plaintiffs' and Class members' data.

27 330. But for AT&T's breaches of its duties, Plaintiffs' and Class members' location  
28 data would not have been accessed by unauthorized individuals.

331. Plaintiffs and Class members were foreseeable victims of AT&T's inadequate data security practices and consent mechanisms. AT&T knew or should have known that unauthorized accesses would cause damage to Plaintiffs and Class members.

332. AT&T's negligent conduct provided a means for unauthorized individuals to track Plaintiffs' and the Class's locations.

333. As a result of AT&T's willful failure to prevent unauthorized accesses, Plaintiffs and Class members suffered injury, which includes, but is not limited to: (i) past privacy violations arising from the unauthorized sale of their location data to the Aggregator Defendants and other third parties, (ii) exposure to a heightened, imminent risk of ongoing harms to their safety, security, privacy rights, and property rights, and (iii) financial harm, including but not limited to unauthorized use of their limited mobile data, for which they pay AT&T.

334. The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of AT&T's breaches of its duties.

335. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

**COUNT VI**  
**Violations of California's Consumers Legal Remedies Act ("CLRA"), California Civil Code § 1750 *et seq.***  
**(As to AT&T)**

336. Plaintiffs reallege and incorporate all of the preceding paragraphs as though fully set forth in this cause of action.

337. AT&T has engaged in unfair methods of competition and unfair or deceptive acts or practices intended to result and which did result in the sale of services to Plaintiffs and other California consumers, as detailed herein.

338. AT&T's acts and representations concerning its sale of access to its customers' real-time location data, and the safeguards around that data, is likely to mislead reasonable consumers, including Plaintiffs and members of the Class, as detailed herein.

339. AT&T has represented that its goods or services have characteristics, benefits, and/or quantities that they do not have. Cal. Civ. Code § 1770(a)(5). Specifically, as AT&T

1 represented that, in purchasing AT&T wireless cell service and using AT&T-compatible phones,  
2 Plaintiffs' and Class members' location data would be safeguarded and protected as outlined in  
3 Section H, and AT&T would not sell its customers' personal information. In actuality, as alleged  
4 in Sections B-E, AT&T's wireless service did not protect and/or safeguard Plaintiffs' and Class  
5 members' location data from unauthorized access, and AT&T did in fact sell customers' personal  
6 information, as detailed herein.

7 340. AT&T's misrepresentations and omissions concerning its sale of access to and  
8 safeguarding of customers' real-time location data were material. As alleged in Section G, a  
9 reasonable person would attach importance to the privacy of her sensitive location data in  
10 determining whether to contract with a wireless cell phone provider. AT&T was obligated to  
11 disclose the nature of its location data sales practices, as AT&T had exclusive knowledge of  
12 material facts not known or knowable to its customers, AT&T actively concealed these material  
13 facts from its customers, and such disclosures were necessary to materially qualify its  
14 representations that it did not sell and took measures to protect consumer data and its partial  
15 disclosures concerning its use of customers' CPNI. Further, AT&T was obligated to disclose its  
16 practices under the FCA.

17 341. Defendants' actions and conduct complained of herein were a substantial factor in  
18 causing the harm suffered by Plaintiffs and Class members.

19 342. Plaintiffs, individually and on behalf of the Class, seek injunctive relief for  
20 AT&T's violations of the CLRA. Plaintiffs seek public injunctive relief against AT&T's unfair  
21 and unlawful practices in order to protect the public and restore to the parties in interest money  
22 or property taken as a result of AT&T's unfair methods of competition and unfair or deceptive  
23 acts or practices. Plaintiffs and the Class seek a mandatory cessation of AT&T's practices and  
24 proper safeguarding of current and historical location data.

## 25 **VII. PRAYER FOR RELIEF**

26 343. WHEREFORE, Plaintiffs request that judgment be entered against Defendants and  
27 that the Court grant the following:  
28

- 1           A.     An order determining that this action may be maintained as a class action under  
2                 Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs are proper Class  
3                 representatives, Plaintiffs' attorneys shall be appointed as Class counsel pursuant  
4                 to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be  
5                 promptly issued;
- 6           B.     Judgment against Defendants for Plaintiffs' and Class members' asserted causes  
7                 of action;
- 8           C.     Public injunctive relief requiring cessation of Defendants' acts and practices  
9                 complained of herein pursuant to, *inter alia*, Cal. Bus. & Prof. Code § 17200, 47  
10                U.S.C. § 401(b), and Cal. Civ Code § 1780;
- 11          D.     Pre- and post-judgment interest, as allowed by law;
- 12          E.     An award of monetary damages, including punitive damages;
- 13          F.     Reasonable attorneys' fees and costs reasonably incurred, including but not  
14                 limited to attorneys' fees and costs pursuant to 47 U.S.C.A. § 206; and
- 15          G.     Any and all other and further relief to which Plaintiffs and the Class may be  
16                 entitled.

17                                 **DEMAND FOR JURY TRIAL**

18           Plaintiffs demand a trial by jury of all issues so triable.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 Dated: July 16, 2019

Respectfully submitted,

2  
3 /s/ Thomas D. Warren

Thomas D. Warren (SBN 160921)

twarren@piercebainbridge.com

4 **PIERCE BAINBRIDGE BECK PRICE**  
5 **& HECHT LLP**

355 S. Grand Avenue, 44th Floor

6 Los Angeles, CA 90071

7 Telephone: (213) 262-9333

Facsimile: (213) 279-2008

8 Deborah Renner (*pro hac vice forthcoming*)

9 drenner@piercebainbridge.com

Abbye R. Klamann Ognibene (SBN 311112)

10 aognibene@piercebainbridge.com

11 Claiborne R. Hane (*pro hac vice*  
*forthcoming*)

12 chane@piercebainbridge.com

13 **PIERCE BAINBRIDGE BECK PRICE**  
14 **& HECHT LLP**

277 Park Avenue, 45th Floor

15 New York, NY 10172

Telephone: (212) 484-9866

16 Facsimile: (646) 968-4125

17 Aaron Mackey (SBN 286647)

18 amackey@eff.org

Andrew Crocker (SBN 291596)

19 andrew@eff.org

Adam D. Schwartz (SBN 309491)

20 adam@eff.org

21 **ELECTRONIC FRONTIER**  
22 **FOUNDATION**

815 Eddy Street

23 San Francisco, California 94109

24 Telephone: (415) 436-9333

25 Facsimile: (415) 436-9993