IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

TYLER MORRISON 4217 SKYVIEW BALTIMORE, MD 21211 *on his own behalf and on behalf of all others similarly situated,* Plaintiffs, v. AT&T MOBILITY, LLC 1025 Lenox Park Blvd. Atlanta, GA 30319 Serve on: Department of Assessment and Taxation Corporate Charter Division 301 W. Preston Street Room 801 Baltimore, MD 21201 Defendant.	JURY TRIAL DEMANDED CASE NO. _____

CLASS ACTION COMPLAINT

Plaintiff Tyler Morrison ("Plaintiff" or "Named Plaintiff"), on his own behalf and on behalf of all others similarly situated, through his attorneys, Cory L. Zajdel, Esq., Jeffrey C. Toppe, Esq., and David M. Trojanowski, Esq., and Z LAW, LLC, hereby submit this Class Action Complaint against Defendant AT&T Mobility, LLC (hereinafter "AT&T" or "Defendant") and for support states as follows:

I. PRELIMINARY STATEMENT

1. Plaintiff, both individually and on behalf of those similarly situated persons (hereafter "Class Members"), brings this Class Action to secure redress against AT&T for its reckless and negligent violations of customer privacy rights.

2. Plaintiff and Class Members are AT&T customers.

3. This action arises out of Defendant's collection of geolocation data and the unauthorized dissemination to third-parties of the geolocation data collected from its users' cell phones.

4. AT&T admittedly sells customer geolocation data to third-parties, including but not limited to data aggregators, who in turn, are able to use or resell the geolocation data with little or no oversight by AT&T.

5. This is an action seeking damages for AT&T's gross failure to safeguard highly personal and private consumer geolocation data in violation of federal law.

II. JURISDICTION

6. This Court has original federal subject-matter jurisdiction over this class action pursuant to 28 U.S.C. § 1331 as the sole cause of action pled in this case arises under federal law.

7. This Court has personal jurisdiction over the parties because Plaintiff is a citizen of Maryland and because AT&T transacts substantial business within the State of Maryland.

8. Venue in this judicial district is proper pursuant to 28 U.S.C. § 1391(a) because AT&T conducts substantial business in, and may be found in, this district, and Plaintiff and Class Members had their geolocation data collected within the State of Maryland.

III. PARTIES

9. Plaintiff Morrison is a natural person currently residing in Baltimore City, Maryland.

10. Defendant AT&T is a domestic limited liability company that was formed in Delaware and that lists its principal place of business as Atlanta, Georgia. AT&T does substantial business within the State of Maryland.

IV. FACTUAL ALLEGATIONS

AT&T's Statutory Obligation to Protect Customers' Personal Network Information Under the Federal Communications Act

11. As a common carrier, AT&T is obligated to protect the confidential personal information of its customers under the Federal Communications Act ("FCA"), 47 U.S.C. § 222.

12. FCA § 222(a) provides that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to . . . customers . . . ." The "confidential proprietary information" referred to in FCA § 222(a) is abbreviated herein as "CPI."

13. FCA § 222(c) additionally provides that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories." The "customer proprietary network information" referred to in FCA § 222(c) is abbreviated herein as "CPNI."

14. FCA § 222(h)(1) (emphasis added) defines CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, **location**, and amount of use 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; and (B) information contained in the bills pertaining to telephone exchange service

or telephone toll service received by a customer of a carrier, except that term does not include subscriber list information."

15. The Federal Communication Commissions ("FCC") has promulgated rules to implement FCA § 222 "to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI." *See* 47 CFR § 64.2001, *et seq*. ("CPNI Rules"); CPNI Order, 13 FCC Rcd. at 8195 ¶ 193.

16. The CPNI Rules limit disclosure and use of CPNI without customer approval to certain limited circumstances (such as cooperation with law enforcement), none of which are applicable to the facts here. CPNI Rules § 64.2005.

17. The CPNI Rules §§ 64.2009(b), (d), and (e) require carriers to implement safeguards to protect customers' CPNI.

18. These safeguards include: (i) training personnel "as to when they are and are not authorized to use CPNI[;]" (ii) establishing "a supervisory review process regarding carrier compliance with the rules[;]" and (iii) filing annual compliance certificates with the FCC.

19. The CPNI Rules § 64.2010 further require carriers to implement measures to prevent the disclosure of CPNI to unauthorized individuals. For example, "carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI." CPNI Rules § 64.2010(a).

20. As further alleged below, AT&T violated FCA § 222 and the CPNI Rules when it disclosed CPNI and CPI to third-parties without Plaintiff and Class Members' authorization or permission.

AT&T's Stated Privacy and Security Commitments
to Customers in its Privacy Policy and Code of Business Conduct

21. In its Privacy Policy ("Privacy Policy") and Code of Business Conduct ("COBC"), AT&T acknowledges its responsibilities to protect customers' "Personal Information" under the FCA, the CPNI Rules, and other regulations.

22. A true and correct copy of the Privacy Policy in effect in April 2019 available at http://about.att.com/sites/privacy_policy is attached hereto as **Exhibit A**.

23. A true and correct copy of the COBC in effect in April 2019 available at https://ebiznet.sbc.com/attcode/index.cfm is attached hereto as **Exhibit B**.

24. In its Privacy Policy and COBC, AT&T makes binding promises and commitments to Plaintiff and Class Members, as its customers, that it will protect and secure their "Personal Information." The Privacy Policy defines "Personal Information" as "[i]nformation that identifies or reasonably can be used to identify you." AT&T states that, included in the information that it collects from and about its customers, is its customers' "wireless device location." AT&T also collects information relating to the use of its networks, products, and services. "Personal Information" thus includes both CPI and CPNI under FCA § 222 and the CPNI Rules.

25. In its Privacy Policy, AT&T promises that it takes its responsibility "to safeguard your [i.e., the customer's] Personal Information seriously" and that it will not share its customers' Personal Information except for legitimate business purposes.

26. AT & T's Privacy Policy further states that "we will not sell [users'] Personal Information to anyone, for any purpose. Period."

27. AT&T further promises that it has numerous safeguards in place to protect the Personal Information of its customers in its Privacy Policy and makes the following promises to its customers:

> We've worked hard to protect your information. And we've established electronic and administrative safeguards designed to make the information we collect secure. Some examples of those safeguards include:
>
> - All of our employees are subject to the AT&T Code of Business Conduct (COBC) (https://www.att.com/Common/about_us/downloads/att_code_of_business_conduct.pdf) and certain state-mandated codes of conduct. Under the COBC, all employees must follow the laws, rules, regulations, court and/or administrative orders that apply to our business—including, specifically, the legal requirements and company policies surrounding the privacy of communications and the security and privacy of your records. We take this seriously, and any of our employees who fail to meet the standards we've set in the COBC are subject to disciplinary action. That includes dismissal.
> - We've implemented technology and security features and strict policy guidelines to safeguard the privacy of your Personal information. Some examples are:
>   - Maintaining and protecting the security of computer storage and network equipment, and using our security procedures that require employee user names and passwords to access sensitive data;
>   - Applying encryption or other appropriate security controls to protect Personal Information when stored or transmitted by us;
>   - Limiting access to Personal Information to only those with jobs requiring such access; and
>   - Requiring caller/online authentication before providing Account Information so that only you or someone who knows your Account Information will be able to access or change this information.

28. AT&T's COBC also makes binding commitments to Plaintiff and all Class Members, as AT&T customers, that it will protect their Personal Information and that it will adhere to all of its legal obligations. Those legal obligations include FCA § 222, the CPNI Rules, and other legal obligations that govern protection of confidential and private information.

29. For example, AT&T's chairman and chief executive, Randall Stephenson, and its chief compliance officer, David Huntley promise—in a video addressing AT&T's commitment to customer privacy—that because "[o]ur customers count on us . . . , we will follow not only the letter of the law, but the spirit of the law" and "that we will always take responsibility." A transcript of the video is attached hereto as **Exhibit C,** and may be found at https://ebiznet.sbc.com/attcode/assets/2017StephensonHuntleyVideoTranscript.pdf.

30. The COBC also specifically promises that AT&T will "protect the privacy of our customers' communications" because "[n]ot only do our customers demand this, but the law requires it . . . . Maintaining the confidentiality of communication is, and always has been, a crucial part of our business." **Exhibit B** at 10.

31. AT&T further promises in the COBC that it "protect[s] the information about our customers that they entrust to us." *Id.* Acknowledging that "AT&T possesses sensitive, detailed information about our customers, who rely on AT&T to safeguard that information" and that "[l]aws and regulations tell us how to treat such data," AT&T promises Plaintiff and all Class Members, as AT&T customers, that "[a]ny inappropriate use of confidential customer information violates our customers' trust and may also violate a law or regulation. *Id.* Preserving our customers' trust by safeguarding their private data is essential to our reputation." *Id.*

32. As alleged below, AT&T flagrantly and repeatedly violated its commitments made to Plaintiff and Class Members in its Privacy Policy and COBC, as well as its legal obligations under the FCA and the CPNI Rules by willingly disclosing Plaintiff and Class Members' CPNI to unauthorized third-parties.

The First Discovery of Unauthorized Disclosure of CPNI

33. On May 8, 2018, Senator Ron Wyden sent a letter ("the Wyden Letter") to AT&T President and CEO Randall L. Stephenson. The Wyden Letter (attached hereto as **Exhibit D**). In the Letter, Senator Wyden expressed, in very clear terms, great concern with AT&T's handling of consumer information. It had come to Senator Wyden's attention that a company called Securus Technologies, a major provider of correctional-facility telephone services, purchased real-time location information from major wireless carriers, and provided that information, via a self-service web portal, to the government "for nothing more than the legal equivalent of a pinky promise."

34. In the Wyden Letter, Senator Wyden detailed how Securus confirmed to him that the web portal enabled surveillance of customers of "every major U.S. wireless carrier," which, in Senator Wyden's words, "needlessly exposes millions of Americans to potential abuse and unchecked surveillance by the government."

35. Senator Wyden also explained how wireless carriers "are prohibited from sharing certain customer information, including location data, unless the carrier either has the customer's consent or sharing is otherwise required by law." He ultimately concluded that, "the fact that Securus provide[d] this service at all suggests that AT&T does not sufficiently control access to [its] customers' private information."

36. The process by which Securus obtained access to the customers' information in the first place is part of the problem. It purchased real-time location information on AT&T's customers "through a third party location aggregator that has a commercial relationship with the major wireless carriers . . . ."

37. AT&T had no active oversight or direction in Securus' use of AT&T customer location data.

38. In the Wyden Letter, Senator Wyden demanded that AT&T "undertake a comprehensive audit of each third party" with whom AT&T shared its customers' personal information, and "terminate [its] data-sharing relationships with all third parties that have misrepresented customer consent or abused their access to sensitive customer data."

39. On June 15, 2018, AT&T sent a reply letter ("the First AT&T Letter") to Senator Wyden (hereinafter "the First AT&T Letter") (attached hereto as **Exhibit E**). In the First AT&T Letter, after representing that it "values and respects its customers' privacy," AT&T maintained that it had "never authorized the use of its customer data for the Securus web portal . . . ," and that it was "actively investigating the extent to which Securus may have obtained unauthorized access to AT&T customer location data . . . ." AT&T also represented that it had "suspended all access by Securus to AT&T customer location data."

40. AT&T went on to detail how it shares its customers' data: it "permits authorized third parties to access customer location data for location-based services . . . only where a customer consents to such disclosure . . . ." It then explained the process of data "aggregation." In AT&T's words, aggregators with whom AT&T contracted "manage[] requests for customer data across multiple carriers." The example provided by AT&T was that a data aggregator could locate a customer who required roadside assistance, and identify the carrier from which location data needed to be requested.

41. Next, AT&T stated that location-based services providers (such as Securus) are required to give customers notice and obtain consent to use location information. Evidently, Securus—and others—were not obtaining such consent or providing such notice.

42. AT&T admitted in the First AT&T Letter that it did not authorize Securus' collection of customer data for its self-service web portal.

43. AT&T concluded by stating that "AT&T has no reason to believe that there are other instances of unauthorized access to AT&T customer location data."

The Second Discovery of Unauthorized Disclosure of CPNI

44. Six months later, on January 8, 2019, Motherboard (a news outlet) ran an investigative article ("the Article") concerning major telecommunications carriers (including AT&T) selling access to geolocation data to third-parties (hereinafter "The Article") (attached hereto as **Exhibit F**).

45. In the Article, the journalist gave a bounty hunter $300 to locate a cell phone. The bounty hunter did just that using "real-time location data sold to bounty hunters that ultimately originated from the major [telecommunications carriers]."

46. The Article revealed that a company called MicroBilt was selling cell phone geolocation services with little oversight to a spread of different private industries, "ranging from car salesmen and property managers to bail bondsmen and bounty hunters . . . ." Additionally, this "spying capability is also being resold to others on the black market who are not licensed by the company to use it . . . seemingly without MicroBilt's knowledge."

47. Motherboard's investigation revealed that "a wide variety of companies can access cell phone location data, and . . . the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data."

48. Motherboard found that some of the location aggregators were so sloppy that "anyone could geolocate nearly any phone in the United States at a click of a mouse."

49. In response to a request for comment, AT&T told Motherboard that use of its customers' data by bounty hunters "would violate [its] contract and Privacy Policy."

50. The telecommunications carriers are the beginning of a dizzying chain of data selling, where data goes from company to company, and ultimately ends up in the hands of literally anybody who is looking.

51. The information a person could obtain included the name and address of an individual, and the geolocation of that individual's cell phone.

52. One of the data aggregators with whom AT&T contracted is called MicroBilt. MicroBilt was engaged in the process of selling consumer data to literally anybody who would pay for it, including the name and address of an individual, and the geolocation of that individual's cell phone. Some of the sectors that utilized MicroBilt's services were landlords, car salesmen, and others conducting credit checks.

53. In essence, AT&T was relying on the end user of the location data not to abuse the data, or not to obtain the data under false pretenses. In practice, the end users exercised no oversight over the process whatsoever.

54. Three weeks after Motherboard published its story, on January 24, 2019, Senator Wyden, along with fourteen other United States Senators, sent a letter to the FCC and Federal Trade Commission (hereinafter "Second Wyden Letter") (attached hereto as **Exhibit G**), urging the chairmen of the respective Commissions to "broadly investigate the sale of Americans' location data by wireless carriers, location aggregators, and other third parties."

55. The Commissions are currently investigating each of the major wireless carriers, including AT&T.

The Second Correspondence between AT&T and Senator Wyden

56. On February 15, 2019, AT&T sent Senator Wyden a letter concerning its relationship with MicroBilt (hereinafter "Second AT&T Letter") (attached hereto as **Exhibit H**).

In its letter, AT&T explained that in response to the January 9, 2019 Motherboard story, AT&T "immediately suspended MicroBilt's access to AT&T location information" and that it "began investigating whether any AT&T customers' location information had been transmitted without consent or for purposes beyond the limited fraud-prevention use [it] had authorized for MicroBilt."

57. In the Second AT&T Letter, AT&T also stated that:

> . . . before we provide location to any aggregator or service provider, we investigate them–i.e., their corporate history, security policies, and privacy policies–as well as their planned use of the data. We do not share location information with any entity for any purpose that has not been vetted and approved. If approved, the aggregator or service provider must provide conspicuous notice to the customer of the intended use of the information and obtain the customer's consent to that use, and they are prohibited from using it for any other purpose. Those entities must provide AT&T with a confirmation of customer consent for each request for AT&T location data, and we review those records daily.

58. Finally, AT&T stated that, "based on a review going back to January 2016, beyond the allegations of inappropriate use of location information by Securus Technologies, AT&T has not identified any use of location information where the location aggregator or another third-party obtained AT&T location information without prior customer consent."

59. On March 13, 2019, Senator Wyden responded in a letter to AT&T, and the other telecommunications carriers (hereinafter "Third Wyden Letter") (attached hereto as **Exhibit I**) seeking additional information regarding AT&T's "repeated sale and improper disclosure of customer location data" to third-parties. In the Third Wyden Letter, Senator Wyden said it was "now abundantly clear that [AT&T has] failed to be [a] good steward[] of [its] customers' private location information."

60. The Third Wyden Letter also chastised the telecommunications carriers for their failures to comply with a federal law that requires wireless carriers "to protect Customer Proprietary Network Information (CPNI), which includes location data." Wyden also noted that wireless carriers are "required to report breaches of CPNI to federal law enforcement agencies."

61. On March 26, 2019, the FTC issued an order to AT&T, among others, seeking information the agency will use to examine how it collects, retains, uses, and discloses information about consumers and their devices.

V. CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action on behalf of a Class which consists of:

> All AT&T customers located in any of the United States, including the District of Columbia, between April 30, 2015 and February 15, 2019.

Excluded from the Class are those individuals who now are or have ever been executives of the Defendant and the spouses, parents, siblings, and children of all such individuals.

63. The Class, as defined above, is identifiable. Plaintiff is a member of the Class.

64. The Class consists, at a minimum, of one hundred million (100,000,000) individuals and is thus so numerous that joinder of all members is clearly impracticable.

65. There are questions of law and fact which are not only common to the Class but which predominate over any questions affecting only individual Class members.

66. The common and predominating questions include, but are not limited to:

a) Whether AT&T violated FCA § 222 by its unauthorized disclosure of Plaintiff and Class Members' CPNI to third-parties during the class period; and

b) Whether Plaintiff and Class Members' CPNI was accessible to unauthorized third-parties during the class period.

67. Claims of Plaintiff are typical of the claims of the respective Class Members and are based on and arise out of similar facts constituting the wrongful conduct of Defendant.

68. Plaintiff will fairly and adequately protect the interests of the Class.

69. Plaintiff is committed to vigorously litigating this matter.

70. Further, Plaintiff has secured counsel experienced in handling consumer class actions and complex consumer litigation.

71. Neither Plaintiff, nor his counsel, have any interests which might cause them not to vigorously pursue this claim.

72. Common questions of law and fact enumerated above predominate over questions affecting only individual members of the Class.

73. A class action is the superior method for fair and efficient adjudication of the controversy.

74. The likelihood that individual Class Members will prosecute separate actions in court is remote due to the time and expense necessary to conduct such litigation.

75. The likelihood that individual Class Members will prosecute separate actions in court is remote.

76. Counsel for Plaintiff and the Class are experienced in class actions and foresee little difficulty in the management of this case as a class action.

VI. CAUSE OF ACTION

COUNT ONE
(Unauthorized Disclosure of Customer Confidential Proprietary Network Information in Violation of 47 U.S.C. § 222)

77. Plaintiff incorporates by reference all of the allegations herein as if each and every allegation is set forth fully herein.

78. AT&T is a telecommunications common carrier engaged in interstate commerce by wire regulated by the FCA and subject to the requirements, *inter alia,* of §§ 206 and 222 of the FCA.

79. Under FCA § 206, "[i]n case any common carriers shall do, or cause or permit it 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, together with a reasonable counsel or attorney's fee, to be fixed by the court in every case of recovery, which attorney's fee shall be taxed and collected as part of the costs in the case."

80. FCA § 222(a) requires every telecommunications carrier to protect, among other things, its customers' CPI.

81. FCA § 222(c) further requires every telecommunications carrier to protect, among other things, its customers' CPNI.

82. The information disclosed by AT&T to third-parties, including but not limited to data aggregators, without Plaintiff or Class Members' consent was CPI and CPNI under FCA § 222.

83. AT&T failed to protect the confidentiality of Plaintiff and Class Members' CPI and CPNI, including their wireless telephone numbers, account information, private

communications, and location, by divulging that information to third-parties, including but not limited to data aggregators.

84. Through its negligent and deliberate acts, including inexplicable failures to follow its own Privacy Policy, AT&T permitted access to Plaintiff and Class Members' CPI and CPNI.

85. AT&T profited from the sale and unauthorized dissemination of Plaintiff and Class Members' CPI and CPNI.

86. As a direct consequence of AT&T's violations of the FCA, Plaintiff and Class Members have been damaged, in an amount to be proven at trial.

87. As a direct consequence of AT&T's violations of the FCA, AT&T were unjustly enriched in an amount to be proven at trial.

88. Plaintiff and Class Members are also entitled to attorney's fees under the FCA.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays that this Court:

A. Assume jurisdiction of this case;

B. Enter an order certifying the Class under FED. R. CIV. P. 23(b)(3);

C. Award damages in accordance with FCA § 206; and

D. Award reasonable attorney's fees in accordance with FCA § 206.

Respectfully submitted,

Z LAW, LLC

Dated: April 29, 2019

/s/ 28191

Cory L. Zajdel (Fed. Bar #28191)
Jeffrey C. Toppe (Fed. Bar #20804)
David M. Trojanowski (Fed. Bar #19808)
2345 York Road, Ste. B-13
Timonium, MD 21093
(443) 213-1977
clz@zlawmaryland.com

jct@zlawmaryland.com
dmt@zlawmaryland.com

Attorneys for Plaintiffs

DEMAND FOR JURY TRIAL

Plaintiff requests a jury trial for any and all Counts for which a trial by jury is permitted by law.

/s/ 28191
Cory L. Zajdel, Esquire