IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

SHAWNAY RAY 3 HIGH HAVEN PLACE, APT. 1C NOTTINGHAM, MD 21236 KANTICE JOYNER 310 LORD WILLOUBHBY WAY EDGEWOOD, MD 21040 *on their own behalf and on behalf of all others similarly situated,* Plaintiffs, v. T-MOBILE US, INC. 3650 131st AVENUE SE BELLEVUE, WA 98006 Serve on: CSC-LAWYERS INCORPORATING SERVICE COMPANY 7 ST. PAUL STREET SUITE 820 BALTIMORE, MD 21202 Defendant	JURY TRIAL DEMANDED CASE NO. _____

CLASS ACTION COMPLAINT

Plaintiffs Shawnay Ray and Kantice Joyner ("Plaintiffs" or "Named Plaintiffs"), on their own behalf and on behalf of all others similarly situated, through their 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 T-Mobile US, Inc. (hereinafter "T-Mobile" or "Defendant") and for support states as follows:

I. PRELIMINARY STATEMENT

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

2. Plaintiffs and Class Members are T-Mobile 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. T-Mobile 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 T-Mobile.

5. This is an action seeking damages for T-Mobile'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 Plaintiffs are citizens of Maryland and because T-Mobile 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 T-Mobile conducts substantial business in, and may be found in, this district, and Plaintiffs and members of the proposed class had their geolocation data collected within the State of Maryland.

III. PARTIES

9. Plaintiff Shawnay Ray is a natural person currently residing in Baltimore County, Maryland.

10. Plaintiff Kantice Joyner is a natural person currently residing at Harford County, Maryland.

11. Defendant T-Mobile is a domestic corporation that was formed in Delaware and that lists its principal place of business as Bellevue, Washington. T-Mobile does substantial business within the State of Maryland.

IV. FACTUAL ALLEGATIONS

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

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

13. 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."

14. 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."

15. 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."

16. 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.

17. 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.

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

19. 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.

20. 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).

21. As further alleged below, T-Mobile violated FCA § 222 and the CPNI Rules when it disclosed CPNI and CPI to third-parties without Plaintiffs' authorization or permission.

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

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

23. A true and correct copy of the Privacy Policy in effect in March 2019 available at https://www.t-mobile.com/responsibility/privacy/privacy-policy is attached hereto as **Exhibit A**.

24. A true and correct copy of the COBC in effect in April 2019 available at https://www.snl.com/Cache/1500087866.PDF?O=PDF&T=&Y=&D=&FID=1500087866&iid=4091145 is attached hereto as **Exhibit B**.

25. In its Privacy Policy and COBC, T-Mobile makes binding promises and commitments to Plaintiffs, as its customer, that it will protect and secure the confidentiality of its customers' information.

26. The Privacy Policy defines "Personal Information" as "information that we directly associate with a specific person or entity (for example, name; addresses; telephone numbers; email address; Social Security Number; call records; wireless device location). The Privacy Policy notes that "a subset of Personal Information is . . . CPNI." "Personal Information" thus, by T-Mobile's own admission, includes both CPI and CPNI under FCA § 222 and the CPNI Rules.

27. In its Privacy Policy, T-Mobile promises that it does "not sell, license, rent, or otherwise provide your Personal Information to unaffiliated third-parties (parties outside the T-Mobile corporate family) to market their services or products to you without your consent."

28. T-Mobile's COBC also makes binding commitments to Plaintiffs and all Class Members, as T-Mobile customers, that it will protect the confidentiality of its customers' information and that it will adhere to all of its legal obligations. (**Exhibit B, at 8**) ("We share customer information only if the customer says we can or we're allowed to by the law, our Terms & Conditions, or Privacy policies.). Those legal obligations include FCA § 222, the CPNI Rules, and other legal obligations that govern protection of confidential and private information.

29. As alleged below, T-Mobile flagrantly and repeatedly violated its commitments made to Plaintiffs in its Privacy Policy and COBC, as well as its legal obligations under the FCA and the CPNI Rules by willingly disclosing Plaintiffs CPNI to unauthorized third-parties.

The First Discovery of Unauthorized Disclosure of CPNI

30. On May 8, 2018, Senator Ron Wyden sent a letter ("the Wyden Letter") to T-Mobile President and CEO John Legere. The Wyden Letter (attached hereto as **Exhibit C**). In the Letter, Senator Wyden expressed, in very clear terms, great concern with T-Mobile'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."

31. 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."

32. 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 T-Mobile does not sufficiently control access to [its] customers' private information."

33. 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 T-Mobile's customers "through a third party location aggregator that has a commercial relationship with the major wireless carriers . . . ."

34. T-Mobile had no active oversight or direction in Securus' use of T-Mobile customer location data.

35. In the Wyden Letter, Senator Wyden demanded that T-Mobile "undertake a comprehensive audit of each third party" with whom T-Mobile 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."

36. On June 15, 2018, T-Mobile sent a reply letter to Senator Wyden (hereinafter "the First T-Mobile Letter") (attached hereto as **Exhibit D**). In the First T-Mobile Letter, after representing that it "takes the privacy and security of our customers' data very seriously," T-Mobile maintained that it had "never approved" the use of its customer data for the Securus web portal. T-Mobile also represented that it had "quickly shut down any transmission of our customers' location data to Securus."

37. T-Mobile went on to detail how it shares its customers' data: "T-Mobile partners with two location aggregators, LocationSmart and Zumigo. The aggregators then partner with service providers, who have a direct relationship with the consumers and offer them specific location-based services . . . . In response to a specific service provider request, via a location

aggregator, we share cell tower location information for the customer's phone number that was associated with the request . . . ."

38. Next, T-Mobile 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.

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

40. T-Mobile concluded by stating that "[g]oing forward, [T-Mobile] will continue to monitor our program and take appropriate steps to ensure that our customer can receive the location-based services they desire in a manner that is consistent with applicable law, their privacy expectations and our high standards for service to our customers."

41. Thereafter, T-Mobile CEO John Legere tweeted on Twitter: "I've personally evaluated this issue & have pledged that @tmobile will not sell customer location data to shady middlemen."

The Second Discovery of Unauthorized Disclosure of CPNI

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

43. In the Article, the journalist gave a bounty hunter $300 to locate a T-Mobile 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]."

44. 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."

45. 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."

46. 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."

47. In response to a request for comment, T-Mobile told Motherboard that "While T-Mobile does not have a direct relationship with Microbilt, our vendor Zumigo was working with them and has confirmed with us that they have already shut down all transmission of T-Mobile data. T-Mobile has also blocked access to device location data for any request submitted by Zumigo on behalf of Microbilt as an additional precaution."

48. 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.

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

50. One of the data aggregators with whom T-Mobile contracted is called Zumigo. Zumigo contracted with 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.

51. In essence, T-Mobile 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.

52. 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 F**), 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."

53. The Commissions are currently investigating each of the major wireless carriers, including T-Mobile.

The Second Correspondence between T-Mobile and Senator Wyden

54. On January 17, 2019, Senator Wyden sent another letter (hereinafter "the Third Wyden Letter") to T-Mobile to "express disbelief and disappointment regarding T-Mobile's continued partnership with companies that have enabled spying on Americans without their knowledge or consent." He noted that T-Mobile's "continued sale of customer location data to these so-called 'location aggregators' is in direct contradiction of your 'personal evaluation' of the issue six months ago." Senator Wyden took particular issue with T-Mobile's failure to keep its May 2018 promise to stop selling location data to aggregators. He noted that "in spite of your public promise, your company did not in fact take swift action. Instead, your company now claims

that it plans to stop selling location data to aggregators in March of this year, nine months after your original tweet." (Emphasis in original).

55. In response, on February 15, 2019, T-Mobile sent Senator Wyden another letter (hereinafter "Second T-Mobile Letter") (attached hereto as **Exhibit G**). explaining that as of February 8, 2019, "T-Mobile [had] terminated all service provider access to location data . . . , and T-Mobile's [location-based service] contract with the Location Aggregators will officially sunset on March 9." The Second T-Mobile Letter identified five instances of misuse of T-Mobile customer location information under their location aggregation program. T-Mobile admitted that "in all but one of these instances, the LBS provider was using T-Mobile customer location data in a manner that T-Mobile had not reviewed or approved as required under the LBS provider's respective agreements with the Location Aggregators."

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

57. The Fourth 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."

58. On March 26, 2019, the FTC issued an order to T-Mobile, 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

59. Plaintiffs bring this action on behalf of a Class which consists of:

> All T-Mobile customers located in any of the United States, including the District of Columbia, between May 3, 2015 and March 9, 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.

60. The Class, as defined above, is identifiable. Plaintiffs are members of the Class.

61. The Class consists, at a minimum, of fifty million (50,000,000) individuals and is thus so numerous that joinder of all members is clearly impracticable.

62. 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.

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

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

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

64. Claims of Plaintiffs 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.

65. Plaintiffs will fairly and adequately protect the interests of the Class.

66. Plaintiffs are committed to vigorously litigating this matter.

67. Further, Plaintiffs have secured counsel experienced in handling consumer class actions and complex consumer litigation.

68. Neither Plaintiffs, nor their counsel, have any interests which might cause them not to vigorously pursue this claim.

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

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

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

72. Counsel for Plaintiffs 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)

73. Plaintiffs incorporate by reference all of the allegations herein as if each and every allegation is set forth fully herein.

74. T-Mobile 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.

75. 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."

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

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

78. The information disclosed by T-Mobile to third-parties, including but not limited to data aggregators, without Plaintiffs' consent was CPI and CPNI under FCA § 222.

79. T-Mobile failed to protect the confidentiality of Plaintiffs 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.

80. Through its negligent and deliberate acts, including inexplicable failures to follow its own Privacy Policy, T-Mobile permitted access to Plaintiffs and Class Members' CPI and CPNI.

81. T-Mobile profited from the sale and unauthorized dissemination of Plaintiff and Class Members' CPI and CPNI.

82. As a direct consequence of T-Mobile's violations of the FCA, Plaintiffs and Class Members have been damaged, in an amount to be proven at trial.

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

84. Plaintiffs and Class Members are also entitled to attorney's fees under the FCA.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray 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: May 2, 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

Plaintiffs request a jury trial for any and all Counts for which a trial by jury is permitted by law.

/s/ 28191
Cory L. Zajdel, Esquire