IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

DEMETRIC SIMS, individually and on behalf of all similarly situated persons,

Plaintiffs,

v.

THE ALLSTATE CORPORATION,
ALLSTATE INSURANCE COMPANY,
ALLSTATE VEHICLE AND PROPERTY INSURANCE COMPANY,
ARITY, LLC,
ARITY 875, LLC, and
ARITY SERVICES, LLC,

Defendants.

CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

Civil Action No.

CLASS REPRESENTATION

Jury Trial Demanded

Plaintiff Demetric Sims ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against the Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, "Allstate" or "Defendants"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for surveillance of insureds and invasion of their clients' privacy by collecting data on their clients' location and driving habits, surreptitiously, and without clients' consent.

2. Defendants, each a company owned by The Allstate Corporation, an insurance company, conspired to secretly collect and sell "trillions of miles" of consumers' "driving behavior" data from mobile devices, in-car devices, and vehicles. Defendants used the illicitly obtained data to build the "world's largest driving behavior database," housing the driving behavior of over 45 million Americans. Defendants created the database for two main purposes: (1) to support Allstate Defendants' car insurance business, including relative to under-writing and coverage decisions, and (2) profit from selling the driving behavior data to third parties, including other car insurance carriers ("Insurers").

3. Through the software integrated into the third-party apps, Defendants directly pulled a litany of valuable data directly from consumers' mobile phones. The data included a phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy ("Driving Data").

4. To encourage developers to adopt Defendants' software, Defendants paid app developers millions of dollars to integrate Defendants' software development kits ("SDK") into their apps. In general, SDKs can provide app developers a helpful tool to build and develop their apps. SDKs usually consist of a set of tools (APIs, software, etc.) with preprogrammed functions that are integrated into an app and operate in the background.

5. Defendants further incentivized software developer usage of their SDK by creating generous bonus incentives for increasing the size of their dataset. According to Defendants, the apps in to which their SDK is integrated currently allow them to "capture[] [data] every 15 seconds or less" from "40 [million] active mobile connections."[1]

[1] "Why Arity?". Arity, https://arity.com/solutions/real-time-insights/ (last accessed on January 13, 2025).

6. Once collected, Defendants found several ways to monetize the ill-gotten Driving Data, including by selling access to the Driving Data to other insurers and using the data for Allstate Defendants' own insurance underwriting and coverage decisions. If a consumer requested a car insurance quote or had to renew their coverage, Insurers would access that consumer's driving behavior in Defendants' database. Insurers then secretly used that consumer's data to justify increasing their car insurance premiums, denying them coverage, or dropping them from coverage.

7. Defendants marketed and sold the data obtained through third-party apps as "driving" data reflecting consumers' driving habits, despite the data being collected from and about the location of a person's phone.

8. Consumers did not consent to, nor were aware of Defendants' collection and sale of Driving Data. Defendants never informed consumers about their extensive data collection, nor did Defendants obtain consumers' consent to engage in such data collection. Defendants never informed consumers as to how they would analyze, use, and monetize their sensitive data.

9. The putative Class is comprised of millions of Americans who were never informed about, nor consented to, Defendants' continuous collection and sale of their Driving Data. Through this action, Plaintiff and Class Members seek damages for the losses suffered as a result of Defendants' misconduct, as well as injunctive relief aimed at preventing Defendants from engaging in such practices in the future.

PARTIES

10. Plaintiff Demetric Sims is an individual who, at all material times, resided in Fulton County, Georgia. Sims is a client of Defendant The Allstate Corporation, from whom he has purchased auto and rental insurance. Sims has used Sirius XM app, and was never notified that his Driving Data was shared with Defendants.

11. Defendant The Allstate Corporation is a United States public corporation headquartered in Glenview, Illinois, and incorporated under the laws of Illinois. Together with its subsidiaries, Defendant The Allstate Corporation provides insurance products, including car insurance, throughout the United States.

12. Defendant Allstate Insurance Company is a wholly owned subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Insurance Company provides insurance products, including car insurance, throughout the United States.

13. Defendant Allstate Vehicle and Property Insurance Company is a subsidiary of The Allstate Corporation and is headquartered in Northbrook, Illinois, and incorporated under the laws of Illinois. Defendant Allstate Vehicle and Property Insurance Company provides insurance products, including car insurance, throughout the United States.

14. Defendant Arity, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Chicago, Illinois, and it is incorporated under the laws of Delaware. Defendant Arity, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

15. Defendant Arity 875, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, the LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown, Julie Cho, Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang and Lisa Jillson, are

all citizens of Illinois. Defendant Arity 875, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

16. Defendant Arity Services, LLC, was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters is in Northbrook, Illinois, and it is incorporated under the laws of Delaware. Upon information and belief, the LLC's members, including Allstate, Alexandra Band, Christopher Belden, Jennifer Brown, Julie Cho, Eric Ferren, Amit Goswami, Suren Gupta, Gary Hallgren, Christina Hwang and Lisa Jillson, are all citizens of Illinois. Defendant Arity Services, LLC, is a mobility data and analytics company that, together with the other subsidiaries of Defendant The Allstate Corporation, collects and analyzes data obtained throughout the United States, and uses predictive analytics to build solutions to sell to third parties.

JURISDICTION AND VENUE

17. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed $5,000,000.00, exclusive of interest and costs, and all conditions are met. In particular, Plaintiff, and a large number of Class Members, are citizens of states different from the Defendants'.

18. This Court has jurisdiction over the Defendants as Defendants maintain their corporate headquarters in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District and Defendants are headquartered in this District.

GENERAL FACTUAL BACKGROUND

20. In their own words, Defendants have amassed the Driving Data from "130M+ average daily trips from 45M+ active geographically dispersed consumer connections", i.e., more than 45 million Americans.[2] Defendants obtained the data without consumers' knowing by integrating an SDK (a piece of software) into various mobile apps that enabled them to collect data directly from consumers' phones.

21. Defendants have monetized Class Members' Driving Data in a variety of ways, including by building the "world's largest driving behavior database,"[3] and selling access to it to other insurers.

22. Defendants never notified Plaintiff and Class Members, nor obtained their consent, to collect or sell their Driving Data.

I. Defendants Developed Software Tools to Covertly Collect Consumers' Location Data

23. On information and belief, in 2015 Allstate Defendants designed an SDK that could be integrated into mobile phone applications to collect data about the location and movements of a person's phone.

24. The SDK Defendants developed was little more than a way for Defendants to scrape user data from several third-party apps under the pretext of providing a necessary functionality. Specifically, Defendants designed the Arity Driving Engine SDK ("Arity SDK") to collect immense amounts of Driving Data, in granular form.

25. Once incorporated in a mobile app, the Arity SDK harvested several types of data, including but not limited to:

---

[2] "Benefits". Arity, https://arity.com/solutions/vehicle-miles-traveled/ (last accessed on January 13, 2025).
[3] *Id*.

a. a mobile phone's geolocation data, accelerometer data, magnetometer data, and gyroscopic data;

b. "Trip attributes," which included information about a consumer's movements, such as start and end location, distance, duration, start and end time, and termination reason code;

c. "GPS points," such as the accuracy, position, longitude, latitude, heading, speed, GPS time, time received, bearing, and altitude of a consumer's mobile phone;

d. "Derived events," such as acceleration, speeding, distracted driving, crash detection, and attributes such as start and end location, start and end time, speed attribute, rate of change attribute, and signal strength attribute; and

e. Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, device type, app version, and OS version.

26. Because the Arity SDK operated and collected data in the background, absent being notified by Defendants or the app, Plaintiff and Class Members were kept in the dark about the Arity SDK's existence. Plaintiff and Class Members were likewise unaware that Defendants were directly collecting Driving Data from their phones. Defendants never notified nor otherwise informed consumers that they were collecting their data via the Arity SDK and the apps.

II. Defendants Paid App Developers to Integrate the Arity SDK into Mobile Apps

27. Since at least 2017, Defendants have been "licensing" the Arity SDK by paying app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. On information and belief, to avoid alerting consumers of their data collection, Defendants only sought to partner with apps that, prior to contracting with Defendants, already contained features that relied on location information to function properly. Defendants integrated Arity SDK into widely

popular apps, such as: Routely, Life360, GasBuddy, Sirius XM, and Fuel Rewards.

28. Once an app integrated the Arity SDK, the user was unwittingly enabling Defendants to collect the Driving Data via the Arity SDK.

29. Pursuant to their agreements with the app developers, Defendants owned any Driving Data they collected from an app user and were permitted to use the Driving Data for their own independent purposes. Defendants further agreed to license or transfer subsets of the Driving Data to the app developers to use to support specific features in their apps, such as displaying a summary of a user's trip and fuel efficiency.

30. In a further invasion of Plaintiff's and Class Members' privacy, to allow Defendants to match specific individuals to the Driving Data, the app publishers licensed the personal data that they collected from their users to Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile ad-ID, device ID, and ad-ID (collectively, "Personal Data"). Upon combining the Personal Data with the Driving Data, Defendants could more reliably identify the specific person being monitored by the Arity SDK.

III. Defendants' Products and Services Monetized Class Members' Data

31. Defendants used Class Members' Driving Data and Personal Data, alone and in conjunction with one another, to develop, advertise, and sell several different products and services to third parties, including Insurers, and used the Driving Data and Personal Data for the Allstate Defendants' own underwriting purposes. Defendants' products and services included:

a. Drivesight. In 2015, Allstate Defendants developed Drivesight to generate a driving score based on Defendants' own scoring model by analyzing data and generating driving scores that assign a

particular value to an individual's driving risk.[4]

b. ArityIQ. Defendants let companies, including Insurers, "[a]ccess actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver."[5]

c. Arity Audiences. Defendants let companies, including Insurers, "[t]arget drivers based on risk, mileage, commuting habits" and "[m]ore effectively reach [their] ideal audiences with the best offers to eliminate wasted spend, increase retention, and achieve optimal customer LTV." As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.[6]

d. Real Time Insights. Defendants advertised that their business customers could "[r]eceive granular driver probe and event data for real-time applications."[7]

e. Routely. Defendants offer consumers Routely, a "free" application which purports to provide "helpful insights" into the consumers' driver data. By contrast, when marketing to Insurers, Defendants describe Routely as "telematics in a box" that Insurers can use to "more accurately identify drivers with riskier driving profiles based on actual driving data, provide personalized discounts or surcharges at renewal, promote safer driving habits, and improve

[4] "Drivesight®". Arity, https://arity.com/solutions/drivesight/ (last accessed on January 13, 2025).
[5] "ArityIQ℠". Arity, https://arity.com/solutions/arity-iq/ (last accessed on January 13, 2025).
[6] "Arity Audiences". Arity, https://arity.com/solutions/arity-audiences/ (last accessed on January 13, 2025).
[7] "Real Time Insights". Arity, https://arity.com/solutions/real-time-insights/ (last accessed on January 13, 2025).

retention of [their] safer drivers."[8]

32. Notably, Defendants primarily marketed the Driving Data to third parties as "driving behavior" data as opposed to what the Driving Data really was: data about the movements of a person's mobile phone. On information and belief, Defendants had no way to reliably determine whether a person was driving at the time Defendants collected the Driving Data.

33. For example, if a person was a passenger in a bus, a taxi, or in a friend's car, and that vehicle's driver sped, hard braked, or made a sharp turn, Defendants would conclude that the passenger, not the actual driver, engaged in "bad" driving behavior based on the Driving Data. Defendants would then subsequently sell and share the data so it could be used to inform decisions about that passenger's insurability based on their "bad" driving behavior.

34. In a further example of Defendants' abusive practices in connection with Driving Data, a person's driving score was lowered because the "driving" behavior data collected from his phone claimed he was driving, when he was actually riding a roller coaster.[9]

IV. Defendants' Lack of Privacy Disclosures

35. Pursuant to their agreements with app developers, Defendants had varying levels of control over the privacy disclosures and consent language that app developers presented to consumers. However, neither Defendants, nor the apps running Defendants' SDK, informed Plaintiff and Class Members that Defendants were collecting Driving Data. Nor did Defendants, nor the apps on Defendants' behalf, inform Plaintiff and Class Members of the various ways that Defendants would collect, use, and ultimately monetize the Driving Data.

36. Because Defendants did not disclose their conduct, Plaintiff and Class Members

---

[8] "Routinely®". Arity, https://arity.com/solutions/routely/ (last accessed on January 13, 2025).

[9] Chad Murphy, "Sir, this is a roller coaster. Car insurance dings driving score for man riding The Beast." The Cincinnati Enquirer (October 8, 2024), https://www.cincinnati.com/story/entertainment/2024/10/08/insurance-cuts-driving-score-man-riding-the-beast-kings-island/75554987007/ (January 13, 2025).

were wholly unaware that Defendants were collecting the Driving Data from their phone. Plaintiff and Class Members were likewise wholly unaware that Defendants would use the Driving Data to create and sell several different products and services to third parties, including other insurers.

37. Defendants did not provide Plaintiff and Class Members with any sort of notice of their data and privacy practices, nor did the mobile apps notify consumers about Defendants' practices on Defendants' behalf. Similarly, neither Defendants nor the mobile apps notified consumers of the ways in which their Driving Data would be used, nor did consumers agree to have their data used for Defendants' own products or services.

38. Even if a Class Member took the extra step to investigate Defendants outside of their app, navigated to Defendants' website, and located their privacy disclosures, they would still not understand what Defendants did with their data. Consumers reading Defendants' privacy disclosures are met with a series of untrue and contradictory statements that do not reflect Defendants' practices.

39. For example, Defendants state that they "do not sell personal information for monetary value,"[10] which is untrue. Defendants sold a number of data-based products and services for monetary value that linked a specific app user to their alleged driving behavior. Further, Defendants do not provide Class Members with the ability to request that Defendants stop selling their data.

40. Defendants likewise obscured how they used Plaintiff's and Class Members' data. In Defendants' privacy disclosures, Defendants state that they "[u]se [consumers'] personal data for analytics and profiling." But in describing how Defendants "profile" consumers, Defendants fail to explain that they combine the Driving Data and Personal Data to create a database of driving

[10] "Privacy Statement". Arity. (Effective date: November 1, 2024), https://arity.com/privacy/ (last accessed on January 13, 2025).

profiles for more than 45 million Americans and selling access to said database. Rather Defendants describe their profiling activities as follows:

> "We use your personal data to assist in our development of predictive driving models. We may profile [consumers'] personal data only for the purposes of creating a driving score ('Driving Score'), which is used for our analytics purposes to develop and validate our predictive driving models."

41. In the event a Class Member took the extraordinary steps of tracking down Defendants' privacy statement, finding the subparagraph describing profiling, parsing through Defendants' convoluted description of their profiling activities, and concluding that they did not want Defendants to use their data to create a "Driving Score" about them, the Class Member still could do nothing to stop Defendants from collecting their data and creating a Driving Score. Defendants did not describe, nor provide, a method for a consumer to request that their data not be used to profile them.

42. Similarly, if a Class Member concluded they did not want Defendants to use their data for targeted advertising, Defendants instructed them that they could "[l]Learn how to opt out of targeted advertising including by opting out of the sharing or selling your personal information"[11] by visiting another link. But if the Class Member followed that link, they would be taken to a page that—instead of offering them a way to submit a request to opt out of targeted advertising—only provided them with links to several third-party websites, such as the Apple Support Center. These third-party websites merely contained explanations regarding how a consumer could turn off certain types of targeted advertising and did not contain a way for a consumer to submit a request to Defendants specifically.

[11] *Id*.

CLASS ACTION ALLEGATIONS

43. Plaintiff seeks relief in his individual capacity and as representative of all others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and (c)(4), Plaintiff seeks certification of the following class:

> All persons residing in the United States and its territories whose driving information was collected, distributed, stored, and/or sold by Defendants (the "Class").

44. Excluded from the above Class are: Defendants, including any entity in which Defendants have a controlling interest, are a parent or subsidiary, or which are controlled by the Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

45. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiff at this time, Defendants' misconducts affects millions of drivers.

46. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendants collected Plaintiff's and Class Members' Driving Data;

b. Whether Plaintiff and Class Members consented to such collection;

c. Whether Defendants were unjustly enriched;

d. Whether Defendants' conduct constitutes an invasion of privacy;

e. Whether Defendants' conduct was knowing and willful;

f. Whether Defendants are liable for damages, and the amount of such damages; and

g. Whether Defendants should be enjoined from such conduct in the future.

47. All members of the proposed Class are readily ascertainable. In the Driving Data and Personal Data they surreptitiously collected, Defendants have access to the addresses and other contact information for members of the Class, which can be used for providing notice to many Class Members.

48. Typicality. Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of the class in that all were subject to the same data collection, use, and sharing practices of Defendants.

49. Adequacy of Representation. Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including privacy litigation.

50. Superiority of Class Action. Fed. R. Civ. P. 23(b)(3). A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

51. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Nationwide Class.

52. To the extent not all issues or claims, including the amount of damages, can be resolved on a class-wide basis, Plaintiff invokes Federal Rule of Civil Procedure 23(c)(4), reserving the right to seek certification of a class action with respect to particular issues, and

Federal Rule of Civil Procedure 23(c)(5), reserving the right to divide the class into additional subclasses. To the extent Plaintiff seeks declarative or injunctive relief, Defendants have acted or refused to act on grounds that apply generally to the class, rendering certification under Rule 23(b)(2) appropriate.

COUNT I – VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§2510, *et seq.*

(On Behalf of Plaintiff and the Class)

53. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 53 as if fully set forth herein.

54. The Federal Wiretap Act ("FWA"), as amended by the Electronic Communications Privacy Act of 1986 ("ECPA"), prohibits the intentional interception, use, or disclosure of any wire, oral, or electronic communication.

55. In relevant part, the FWA prohibits any person from intentionally intercepting, endeavoring to intercept, or procuring "any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a).

56. The FWA also makes it unlawful for any person to intentionally disclose, or endeavor to disclose, to any other person or to intentionally use, or endeavor to use, the "contents of any wire, oral, or electronic communication, knowing or having reason to know that" the communication was obtained in violation of the FWA. 18 U.S.C. § 2511(1)(c) & (d).

57. The FWA provides a private right of action to any person whose wire, oral, or electronic communication is intercepted, used, or disclosed. 18 U.S.C. § 2520(a).

58. The FWA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

59. The FWA defines "electronic communication" as "any transfer of signs, signals, […] data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

60. The FWA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication." 18 U.S.C. § 2510(5).

61. The FWA defines "contents," with respect to any covered communication, to include "any information concerning the substance, purport, or meaning of that communication[.]" 18 U.S.C. § 2510(8).

62. The FWA defines "person" to include "any individual, partnership, association, joint stock company, trust, or corporation[.]" 18 U.S.C. § 2510(6).

63. Defendant corporations are each a person as defined in 18 U.S.C. §2510(6).

64. The data and transmissions within, to, and from Plaintiff's and Class Members' mobile devices constitute "electronic communications," as defined by 18 U.S.C. § 2510(12), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems that affect interstate commerce.

65. As alleged herein, Defendants intercepted, in real time and as it was transmitted, the contents of electronic communications transmitted within, to, and from Plaintiffs' mobile devices and third party apps, and diverted those communications to themselves without consent.

66. As detailed herein, the electronic communications detailed above that Defendants have intercepted are tied to individual drivers and vehicles, and not anonymized.

67. Plaintiffs and Class Members have a reasonable expectation of privacy within their vehicles, and Plaintiffs and Class Members reasonably expected privacy while driving their vehicles and using their mobile devices.

68. Common understanding and experience of how mobile apps work create a reasonable expectation that an insurer and its affiliates, such as Defendants, would not surreptitiously intercept and divert the detailed and personal electronic communications described above.

69. In further violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the electronic communications described above knowing or having reason to know that the information was obtained through interception in violation of 18 U.S.C. § 2511(1)(a). 18 U.S.C. § 2511(1)(d).

70. Specifically, Defendants used the illicitly obtained information to price insurance products sold to Plaintiff and Class Members, and sold this information to other insurers.

71. As a result, Plaintiff and Class Members have suffered harm and injury due to the interception, disclosure, and/or use of electronic communications containing their private and personal information.

72. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by Defendants' interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiffs and the Class and any profits made by Defendants as a result of the violation or (b) statutory damages for each Class Member of whichever is the greater of $100 per day per

violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II – VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. §§1030, *et seq*.

(On Behalf of Plaintiff and the Class)

73. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 53 as if fully set forth herein.

74. The Computer Fraud and Abuse Act ("CFAA"), enacted in 1986 as part of the ECPA, prohibits the intentional accessing, without authorization or in excess of authorization, of a computer under certain circumstances. 18 U.S.C. § 1030(a).

75. The CFAA specifically provides that it is unlawful to "intentionally access a computer without authorization or exceed[] authorized access, and thereby obtain[]…information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

76. Plaintiffs, as individuals, and Defendants, as corporations, are "persons" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(12).

77. A "computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." 18 U.S.C. § 1030(e)(10).

78. Plaintiff's and Class Members' cellphones are data-processing devices performing logical, arithmetic, and storage functions and thus constitute a "computer" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(1).

79. "Exceeds authorized access" is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled

so to obtain." 18 U.S.C. § 1030(e)(6).

80. A "protected computer" is defined as "a computer . . . which is used in or affecting interstate or foreign commerce or communication…, [or that] has moved in or otherwise affects interstate or foreign commerce." 18 U.S.C. § 1030(e)(2)(B).

81. They are used to send and receive information and electronic communications across state lines and internationally. Thus, they constitute "protected computers" within the meaning of the CFAA. 18 U.S.C. § 1030(e)(2)(B).

82. Through their SDK embedded in third party apps, Defendants intentionally accessed the Plaintiffs' and Class Members' cellphones without Plaintiffs' or Class Members' authorization, or in a manner that exceeded Plaintiffs' and Class Members' authorization, and obtained information therefrom in violation of the CFAA. 18 U.S.C. § 1030(a)(2)(C).

83. Plaintiffs and Class Members have suffered harm and injury due to Defendants' unauthorized access to the communications containing their private and personal information in the form of Driving Data, as well as Defendants' sale of such information to other insurers.

84. A civil action for violation of the CFAA is proper if the conduct involves "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." Because the loss to Plaintiff and Class Members during any one year period within the relevant timeframe, including the loss of their privacy interest in and control over their Driving Data, exceeded $5,000 in aggregate, Plaintiffs and the Class are entitled to bring this civil action and are entitled to economic damages, compensatory damages, injunctive, equitable, and all available statutory relief, as well as their reasonable attorney's fees and costs and other relief as permitted by the CFAA. 18 U.S.C. § 1030(g).

COUNT III – INVASION OF PRIVACY

(On Behalf of Plaintiff and the Class)

85. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 53 as if fully set forth herein.

86. Plaintiff and Class Members have a common law, legally and constitutionally protected privacy interest in their Driving Data and are entitled to the protection of their Driving Data against unauthorized access.

87. Plaintiff and Class Members have a reasonable expectation of privacy in their driving abilities, habits, patterns, and behavior engaged in while they are in their own vehicles, and in any compilation of highly personalized driving behavior profile resulting from the collection of such data.

88. As Plaintiffs and Class Members drive to work, visit family, or simply go about their days, while various third party apps incorporating Defendants' SDK are installed on their phones, they have unknowingly created troves of highly sensitive data mapping their respective personal lives which is then collected, captured, transmitted, accessed, compiled, stored, analyzed, and sold—all without their knowledge or informed consent.

89. The continued nonconsensual surveillance of an individual in their private capacity, as Defendants have done and continue to do, represents a fundamental violation of personal privacy, freedom, and autonomy.

90. As a result of Defendants' intentionally intrusive conduct, Plaintiff and Class Members have been and still remain today under pervasive surveillance compromising their privacy, autonomy, and basic human dignity.

91. Defendants intentionally invaded Plaintiff's and Class Members' privacy interests by deliberately designing SDK and agreeing with third parties to embed this SDK into third party

apps that surreptitiously obtain, improperly gain knowledge of, review, retain, package, and sell their confidential Driving Data.

92. Defendants' conduct is highly offensive to a reasonable person and constitutes an egregious breach of social norms underlying the right to privacy, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions.

93. By tracking, collecting, and storing Plaintiff's and Class Members' Driving Data without authorization or consent to do so, Defendants intentionally intruded upon Plaintiff's and Class Members' seclusion, solitude, and private life engaged in within the confines of their respective vehicles, without their knowledge or permission.

94. Defendants have improperly profited from their invasion of Plaintiff's and Class Members' privacy and their use of Plaintiffs' and Class Members' Driving Data for their economic value and their own commercial gain, including by selling Driving Data to other insurers.

95. As a direct and proximate result of Defendants' unlawful invasions of privacy, Plaintiff's and Class Members' reasonable expectations of privacy were frustrated, exploited, compromised, and defeated.

96. Plaintiff and Class Members were harmed by Defendants' wrongful conduct causing their loss of privacy and the confidentiality of their own private conduct within the confines of their own vehicle. Defendants have needlessly harmed Plaintiff and Class Members by capturing their Driving Data through their connected services. This intrusion, disclosure of information, and loss of privacy and confidentiality has caused Plaintiff and Class Members to suffer mental anguish, actual damages, loss of value of their personal data, and an invasion of their privacy in an amount to be determined at trial.

97. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will cause irreparable injury to Plaintiff and Class Members in that their Driving Data maintained by Defendants may be viewed, distributed, and used by unauthorized third parties for years to come.

98. Plaintiff and Class Members seek nominal, compensatory, and punitive damages as a result of Defendants' actions. Plaintiff and Class Members seek actual damages suffered, plus any profits attributable to Defendants' use of Plaintiff's and Class Members' Driving Data. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were done in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

COUNT IV – INVASION OF PRIVACY

(On Behalf of Plaintiff and the Class)

99. Plaintiff repeats and fully incorporates all factual allegations contained in paragraphs 1 through 53 as if fully set forth herein.

100. Defendants designed their SDK and embedded it in third party apps, by means of which they obtained Plaintiff's and Class Members' Driving Data for their own commercial use and for sale. By driving their vehicles, Plaintiff and Class Members unknowingly conferred the benefit of their Driving Data on Defendants.

101. Defendants knew and appreciated this benefit, and used it for their commercial advantage – to price insurance products and offer other products and services, and to sell this data to other insurers.

102. Plaintiff and Class Members received no benefit from this use and sale of their Driving Data. Indeed, because Plaintiff and Class Members did not consent to Defendants' collection and sale of Plaintiffs' and Class Members' Driving Data, they could not and do not

benefit from such practices. It is therefore inequitable for Defendants to retain any profit from such collection and sale without payment to Plaintiff and Class Members for the value of their Driving Data.

103. Defendants are therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on GM as a result of its wrongful conduct, including specifically the value to GM of the Driving Data that GM wrongfully intercepted, collected, used, and sold to third parties, and the profits GM received or is currently receiving from the use and sale of that Driving Data.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all Class Members proposed in this Complaint, respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff as class representative;

b. For permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein;

c. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

d. For an award of actual damages and compensatory damages, in an amount to be determined;

e. For an award of pre-judgment and post-judgment interest as allowed by law;

f. For an award of costs of suit and attorneys' fees, as allowable by law; and

g. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff demands a jury trial on all issues so triable.

DATED: January 14, 2025

Respectfully submitted,

/s/ John A. Yanchunis John A. Yanchunis jyanchunis@ForThePeople.com Ronald Podolny* ronald.podolny@forthepeople.com Riya Sharma* rsharma@forthepeople.com **MORGAN & MORGAN** **COMPLEX LITIGATION GROUP** 201 N. Franklin Street, 7th Floor Tampa, Florida 33602 Telephone: (813) 223-5505 Facsimile: (813) 223-5402	Robert A. Clifford rac@cliffordlaw.com Shannon McNulty smm@cliffordlaw.com **CLIFFORD LAW OFFICES** 120 North LaSalle Street 36th Floor Chicago, IL 60602

**pro hac vice to be filed*

Attorneys for Plaintiff and the Proposed Class

CIVIL COVER SHEET

The ILND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. ***(See instructions on next page of this form.)***

I. (a) PLAINTIFFS

DEMETRIC SIMS, individually and on behalf of all similarly situated persons

(b) County of Residence of First Listed Plaintiff
(Except in U.S. plaintiff cases)

(c) Attorneys *(firm name, address, and telephone number)*

MORGAN & MORGAN COMPLEX LITIGATION GROUP, 201 N. Franklin Street, 7th Floor, Tampa, FL 33602, Tel. 813-223-5505

DEFENDANTS

THE ALLSTATE CORPORATION, et al.

County of Residence of First Listed Defendant
(In U.S. plaintiff cases only)
Note: In land condemnation cases, use the location of the tract of land involved.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Check **one** box, only.)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government not a party.)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate citizenship of parties in Item III.)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(For Diversity Cases Only.)*

*(Check **one** box, only for plaintiff and **one** box for defendant.)*

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business in This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business in Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Check **one** box, only.)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loan (Excludes Veterans)
- ☐ 153 Recovery of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

PROPERTY RIGHTS
- ☐ 820 Copyright
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016 (DTSA)

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729 (a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act (TCPA)
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Arts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/Accommodations
- ☐ 445 Amer. w/ Disabilities-Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus – Alien Detainee (Prisoner Petition)
- ☐ 465 Other Immigration Actions

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAXES
- ☐ 870 Taxes (U.S. Plaintiff or Defendant
- ☐ 871 IRS—Third Party 26 USC 7609

V. ORIGIN *(Check **one** box, only.)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District (specify) ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION (Enter U.S. Civil Statute under which you are filing and write a brief statement of cause.)

28 U.S.C. § 1332(d)

VII. PREVIOUS BANKRUPTCY MATTERS (For nature of suit 422 and 423, enter the case number and judge for any associated bankruptcy matter previously adjudicated by a judge of this Court. Use a separate attachment if necessary.)

VIII. REQUESTED IN COMPLAINT:

☒ Check if this is a **class action** under Rule 23, F.R.C.V.P.

Demand $ 5000000

CHECK Yes only if demanded in complaint:
Jury Demand: ☒ Yes ☐ No

IX. RELATED CASE(S) IF ANY *(See instructions):*

Judge Case Number

X. Is this a previously dismissed or remanded case? ☐ **Yes** ☒ **No** **If yes, Case #** **Name of Judge**

Date: 01/14/2025

Signature of Attorney of Record /s/ John A. Yanchunis

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority for Civil Cover Sheet

The ILND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use
(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the
(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.