UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

MICHAEL MAHONEY and SCOTT SCHULTZ, 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** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

I. INTRODUCTION 1

II. JURISDICTION AND VENUE 2

III. PARTIES 3

A. Plaintiff 3

B. Defendants 3

IV. FACTS 4

V. STATUE OF LIMITATIONS 8

VI. CLASS ALLEGATIONS 9

VII. CLAIMS FOR RELIEF 12

COUNT One — VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§ 2510, *ET SEQ*. BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS 12

COUNT Two — VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. §§ 2701, *ET SEQ*. BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS 14

COUNT Three — UNJUST ENRICHMENT BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS 15

COUNT Four — Invasion of privacy, brought by PlaintiffS ON BEHALF OF THE NATIONWIDE CLASS AGAinst all defendants. 15

COUNT Five — CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS 16

COUNT Six — VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT—WIRETAPPING LAW, CAL. PEN. CODE § 631, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS 17

COUNT Seven — VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT—ELECTRONIC TRACKING DEVICE, CAL. PEN. CODE § 637.7, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS 20

COUNT Eight — VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS 21

COUNT Nine — VIOLATION OF 815 ILL. COMP. STAT. 505/1 *ET SEQ.*, BROUGHT BY PLAINTIFF SCHULTZ AND THE ILLINOIS SUBCLASS AGAINST ALL DEFENDANTS 22

VIII. PRAYER FOR RELIEF 24

IX. JURY AND TRIAL DEMAND 24

Plaintiffs Michael Mahoney and Scott Schultz allege the following based upon personal knowledge, information and belief, the investigation of their attorneys, and publicly available materials. Plaintiffs bring this case on behalf of themselves and all others similarly situated, against Defendants The Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, "Defendants").

I. INTRODUCTION

1. Without Plaintiffs' knowledge or consent, Defendants collected and sold their personal data, along with "trillions of miles" worth of "driving behavior" data collected from mobile devices, in-car devices, and vehicles.[1]

2. Defendants achieved this by developing and integrating software into third-party mobile applications such as Routely, Life360, GasBuddy, and Fuel Rewards.

3. Once integrated into such third-party software, Defendants could surreptitiously collect a multitude of highly valuable data directly from consumers' mobile phones.

4. Such data includes 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.

5. On information and belief, Defendants paid app developers millions of dollars to integrate Defendants' software into their apps. Defendants further incentivized developer participation by creating generous bonus incentives for increasing the size of their dataset.

[1] ARITY, https://arity.com/ (last visited Feb. 6, 2025).

6. Defendants boast that their software integration allows them to "capture[] [data] every 15 seconds or less" from "40 [million] active mobile connections."[2]

7. Defendants monetized Plaintiffs' data by selling it to other insurance companies.

8. Plaintiffs did not consent to, nor were they aware of Defendants' collection and sale of immeasurable amounts of their sensitive data. Defendants never informed consumers, including Plaintiffs, about such extensive data collection or how Plaintiffs' sensitive personal data would be used, analyzed, and monetized.

9. Defendants' conduct violated numerous federal and state laws and invaded the Plaintiffs' privacy.

10. This invasion of privacy occurred without Plaintiffs' knowledge or consent. As a result, in addition to their loss of privacy, Plaintiffs have seen their auto insurance premiums increase and have had trouble securing coverage.

II. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because at least one member of the proposed class is a citizen of a state different from that of defendants; the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs; and the proposed class comprises more than 100 class members. The Court also has federal question jurisdiction because Plaintiffs bring claims that arise under federal law.

12. This Court has personal jurisdiction over Defendants because each Defendant has its principal headquarters in Illinois, does business in Illinois, directly or through agents, and has

[2] "Real Time Insights," arity, https://arity.com/solutions/real-time-insights/ (last visited Feb. 11, 2025).

sufficient minimum contacts with Illinois such that it has intentionally availed itself of the laws of the United States and Illinois.

13. Venue is proper under 28 U.S.C. § 1391(b)(1) & (2) because a substantial part of the events or omissions giving rise to the claims occurred in Illinois, where each Defendant is headquartered and conducted business.

III. PARTIES

A. Plaintiff

14. Plaintiff Michael Mahoney resides in San Francisco, California. He downloaded the GasBuddy app in 2011 and has used it for the last several years while in the car to find competitive gas prices. He did not know of, much less consent to, Defendants' data practices.

15. Plaintiff Scott Schultz resides in Highland Park, Illinois. He downloaded the GasBuddy app in 2021 and has used it for the past several years while in his own and other people's vehicles to find competitive gas prices. He did not know of, much less consent to, Defendants' data practices.

B. Defendants

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

2. **Defendant Allstate Insurance Company** is a wholly owned subsidiary of The Allstate Corporation, which 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, including Illinois.

3. **Defendant Allstate Vehicle and Property Insurance Company** is a subsidiary of The Allstate Corporation, which 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, including Illinois.

4. **Defendant Arity, LLC,** was founded by The Allstate Corporation in 2016 and is a wholly owned subsidiary of The Allstate Corporation. Its headquarters are in Northbrook, 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, including the State of Illinois.

5. **Defendant Arity 875, LLC** is a subsidiary of The Allstate Corporation and is headquartered in Illinois and incorporated under the laws of Delaware. Arity 875 is the developer of the Routely application and is registered as a data broker in California.

6. **Defendant Arity Services, LLC** is a subsidiary of The Allstate Corporation and is headquartered in Illinois, and incorporated under the laws of Delaware. Arity is a Consumer Reporting Agency as defined by the Fair Credit Reporting Act.

IV. FACTS

7. Defendants conspired to collect drivers' geolocation and movement data from mobile devices, in-car devices, and vehicles.

8. To do so, Defendants designed a software development kit that could be integrated into third-party mobile apps such as Routely, Life360, GasBuddy, and Fuel Rewards.

A. The Routely app is a free navigation app that helps users understand how far and how often they drive, as well as identify speeding, braking, and distracted driving. The app is available for iOS and Android devices.

B. Life360 is a location-sharing app that helps families stay connected and safe. It allows users to share their location and receive alerts when they arrive at or leave certain places. The app is available for iOS and Android devices.

C. The GasBuddy app is a free app that helps users find and pay for gas. It also provides information about gas station locations and prices. The app is available for iOS and Android devices.

D. The Fuel Rewards app is a free loyalty program that helps users save money on gas at Shell stations. The app is available for iOS and Android devices.

9. A software development kit ("SDK") is a collection of software tools that helps developers create applications for a specific platform, operating system, or programming language. SDKs are implemented within apps yet run separate software code.

10. SDKs are commonly used by software developers to, for example, add additional features, provide analytics, and store data about users' application activities.

11. On information and belief, Defendants' SDK was designed to and does collect data including, but not limited to:

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

B. Cell phone accelerometer, magnetometer, and gyroscopic data;

C. "Trip attributes," such as start and end locations, trip distance, trip duration, and start and end times;

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, User ID, device type, app version, and operating system type and version information.

12. Defendants paid third-party app developers millions of dollars to integrate their SDK into their apps.

13. On information and belief, Defendants specifically sought out apps that already contained location-based features to avoid alerting consumers of Defendants' wrongful data collection scheme.

14. Under Defendants' agreements with the third-party app developers, Defendants own the data collected by Defendants' SDK. Defendants licensed or transferred subsets of the SDK Data to third-party app developers to use to support features in such apps, such as displaying a summary of a user's trip and fuel efficiency.

15. Once Defendants' SDK was integrated into third-party mobile apps, individuals would unknowingly download Defendants' SDK software whenever downloading or updating the third-party app on their phone.

16. When Plaintiffs use third-party apps that have integrated Defendants' SDK, Defendants could collect real-time data on their locations and movements and surreptitiously collect highly sensitive and valuable data directly from Plaintiffs' mobile phones.

17. Defendants never informed consumers that they were collecting highly sensitive personal data using Defendants' SDK, never obtained informed consent to do so, and never informed Plaintiffs of the ways Defendants would use and monetize their private, personal data.

18. On its own, Defendants' SDK data could not reliably be linked to specific drivers. The data collected by Defendants' SDK collects information regarding the Plaintiffs' phones regardless of whether or not they were in the driver's seat. Therefore, using only the data collected by their SDK, Defendants could not reliably distinguish, for example, whether a particular individual was the driver or the passenger in a vehicle.

19. To more reliably match Defendants' SDK data to specific individuals, Defendants purchased or licensed personal data that the third-party app developers collected from their users, such as individuals' first and last names, phone numbers, addresses, zip codes, and other highly sensitive personal data. By acquiring such personal data and linking it to their SDK data, Defendants could more readily link the SDK data to specific individuals.

20. To further reliably match Defendants' SDK data with specific individuals, Defendants also purchased data collected directly from vehicles. Defendants purchased consumers' driving-related data from car manufacturers, such as Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram. On information and belief, consumers did not consent to, nor were otherwise aware of, Defendants' purchasing their driving-related data from these car manufacturers.

21. Consumers were wholly unaware that Defendants were collecting their personal data because Defendants did not disclose their conduct and obscured how they used consumers' data.

22. Defendants did not provide consumers with any sort of notice of their data and privacy practices, the third-party mobile apps that integrated Defendants' SDK did not notify consumers about Defendants' data collection practices on Defendants' behalf, and Defendants do not provide consumers with the ability to request that Defendants stop selling their data.

23. Defendants used Plaintiffs' personal data to develop, advertise, and sell several products and services to third parties, including insurance companies, and used the Defendants' SDK Data and other data purchased from third parties for the Allstate Defendants' own underwriting purposes.

24. Defendants sold their SDK data to third parties as "driving behavior" data. For example, ArityIQ is marketed as allowing "[a]ccess [to] actual driving behavior collected from mobile phones and connected vehicles to use at time of quote to more precisely price nearly any driver."[3] Defendants also claim that the "driving behavior" they possess can improve marketing for a wide variety of industries, such as fuel and convenience brands, restaurants, and rideshare or delivery companies.[4] Defendants advertised that they collect data "every 15 seconds or less" from *40 million* "active mobile connections" and "derive[] unique insights that help insurers, developers, marketers, and communities understand and predict driving behavior at scale."[5]

V. STATUE OF LIMITATIONS

25. Defendants did not disclose how they sold or otherwise used driving data.

26. Instead, Defendants actively concealed their collection and sale of the data.

27. Defendants kept their behavior secret because they understood that drivers would not knowingly consent to this sale and use of their data.

28. As a result of defendants' fraudulent concealment of the driving data use and sale, it was not until the New York Times' widely published articles discussing Arity and Life360 that

[3] Arity, Solutions, https://arity.com/solutions/arity-iq/ (last visited Feb. 7, 2025).
[4] Arity, White paper: How driving behavior can improve marketing, https://arity.com/how-behind-the-wheel-behavior-drives-better-marketing/ (last visited Feb. 7, 2025).
[5] Arity, Real Time Insights, https://arity.com/solutions/real-time-insights/ (last visited Feb. 7, 2025).

millions of drivers understood the truth about how their phones and cars were being used to monitor their day-to-day driving.[6]

29. Before June 2024, Plaintiffs would not have reasonably discovered Defendants' practice of surreptitiously acquiring and compiling their sensitive location data without consent, selling it to third-parties, and/or compiling it in a manner that impacts their insurance premiums. The third-party apps did not advertise the integration of Defendants' SDK in the applications. The operation of Defendants' SDK was masked by legitimate app features that the users used. Data was sent to Defendants in the background without any notification.

30. Thus, all applicable statute(s) of limitations have either been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein or accrued only in June of 2024 when Defendants' wrongful data collection practices came to light.

31. Defendants' actions and omissions constituted overt acts that began a new statute of limitations because those acts advanced the unfair objectives of the scheme. Each transmission of driver data to insurance companies or other third parties was a new and independent act that perpetuated Defendants' wrongful scheme.

VI. CLASS ALLEGATIONS

32. Plaintiffs bring this case as a class action under Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3), on behalf of themselves the classes as defined as follows:

A. **The Nationwide Class:** All persons in the United States who used mobile applications with Defendants' SDK installed and whose data was obtained by Defendants.

B. **The California Subclass:** A subset of the proposed nationwide class

[6] *See* Kashmir Hill, Your Driving, Tracked, New York Times (June 9, 2024), https://www.nytimes.com/2024/06/09/briefing/driving-apps-insurance-tracking.html; *See* Kashmir Hill, Is Your Driving Being Secretly Scored?, New York Times (June 9, 2024), https://www.nytimes.com/2024/06/09/technology/driver-scores-insurance-data-apps.html.

encompassing Plaintiff Mahoney and persons who reside in California.

C. **The Illinois Subclass:** A subset of the proposed nationwide class encompassing Plaintiff Schultz and persons who reside in Illinois.

33. Plaintiffs reserve the right to expand, limit, modify, or amend these class definitions, including the addition of one or more subclasses, in connection with their motion for class certification, or at any other time, based on, *inter alia*, changing circumstances and/or new facts obtained.

34. Excluded from the proposed classes are Defendants and their officers, directors, management, employees, subsidiaries, or affiliates. Also excluded from the proposed classes are any judicial official presiding over this action, their personnel, and members of their families, and any governmental entities.

35. **Numerosity.** There are thousands of members of the proposed class and subclasses, and the class and subclasses are thus so numerous that joinder of all members is impracticable. Identification of the class and subclass members is a matter capable of determination from Defendants' records.

36. **Commonality and Predominance.** Common questions of law and fact exist as to all members of the class and subclasses. Such questions predominate over any questions solely affecting individual members of the class and subclasses. Among the questions of law and fact common to the class and subclasses are:

A. Whether Defendants collected Plaintiffs' driving data;

B. What types of driving data Defendants collected;

C. What types of driving data Defendants shared and sold;

D. Whether such practices were unfair and deceptive;

E. Whether Defendants obtained consent from members of the proposed class and subclasses to collect and sell their data;

F. Whether Defendants' practices constitute an invasion of privacy;

G. Whether Defendants' conduct was knowing and willful;

H. Whether Defendants profited from their practices;

I. Whether Plaintiffs have been harmed by Defendants' conduct;

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

K. Whether Defendants' wrongful conduct should be enjoined.

37. **Adequacy of Representation.** Plaintiffs are members of the nationwide class. Plaintiff Mahoney is a member of the proposed California subclass. Plaintiff Schultz is a member of the proposed Illinois subclass. Plaintiffs do not have interests antagonistic to, or in conflict with, the interests of the other members of the class and subclasses. Plaintiffs will fairly and adequately represent the class and subclasses, protecting the interests of the class and subclass members. Plaintiffs have retained competent counsel experienced in class action litigation and intend to prosecute this action vigorously.

38. **Typicality.** Plaintiffs' claims are typical of the claims of the members of the class and subclasses.

39. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because joinder of all members of the proposed class and subclasses would be impracticable, a class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Even if members of the class and subclasses could sustain individual litigation, that course would not be preferable to a class action because

individual litigation would increase the delay and expense to the parties due to the complex factual and legal controversies present in this matter. Here, the class action device will present far fewer management difficulties, and will provide the benefit of a single adjudication, economies of scale, and comprehensive supervision by this Court. The prosecution of separate actions by the individual members of the class and subclasses would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendants.

VII. CLAIMS FOR RELIEF

COUNT ONE — VIOLATION OF THE FEDERAL WIRETAP ACT, 18 U.S.C. §§ 2510, *ET SEQ.* BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS

40. Plaintiffs incorporate the allegations above.

41. 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.

42. Under the FWA, no person may intentionally intercept, endeavor to intercept, or procure "any wire, oral, or electronic communication," 18 U.S.C. § 2511(1)(a), and it is 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).

43. Defendants are each a "person" as defined by the FWA. 18 U.S.C. § 2510(6).

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

45. The data transmitted to and from Plaintiffs' phones constitute transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photo optical systems that affect interstate commerce and, therefore, constitute "electronic communications" as defined by the FWA. 18 U.S.C. § 2510(12).

46. Defendants have intercepted such electronic communications by using their SDKs.

47. Defendants have disclosed the contents of such electronic communications to third parties, such as other insurance companies.

48. In violation of the FWA, Defendants have intentionally used or endeavored to use the contents of the Plaintiffs' data knowing or having reason to know that the information was obtained in violation of 18 U.S.C. §2511(1)(a).

49. Defendants have used the contents of the communications described above to increase driving insurance premiums for members of the proposed class and subclasses for their own financial and commercial benefit, obtaining substantial profit.

50. As a result, Plaintiffs have suffered harm and injury due to the interception, disclosure, and/or use of communications containing their private and personal information.

51. Pursuant to 18 U.S.C. § 2520, Plaintiffs have been damaged by the interception, disclosure, and/or use of their communications in violation of the Wiretap Act and are entitled and seek 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 any profits made by Defendants as a result of the violation or (b) statutory damages for each member of the proposed class and subclasses 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 TWO — VIOLATION OF THE STORED COMMUNICATIONS ACT, 18 U.S.C. §§ 2701, *ET SEQ*. BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS

52. Plaintiffs incorporate the allegations above.

53. The Stored Communications Act ("SCA"), enacted in 1986 as part of the ECPA, creates a civil remedy for those whose stored electronic communications have been obtained by one who "intentionally accesses without authorization" or "intentionally exceeds an authorization to access" a facility through which an electronic communication service ("ECS") is provided. 18 U.S.C. §§ 2701, 2707.

54. The SCA reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of communications in electronic storage and provides a private right of action for individuals who have been harmed by knowing or intentional conduct that is in violation of the SCA. 18 U.S.C. § 2707(a).

55. Plaintiffs, as individuals, and Defendants, as corporations, are "persons" within the meaning of the SCA. 18 U.S.C. §§ 2510(6), 2707.

56. The data transmitted to and from Plaintiffs' phones constitute "electronic communications" within the meaning of the SCA. 18 U.S.C. § 2510(12).

57. Without Plaintiffs' knowledge or consent, Plaintiffs' data were intentionally intercepted by Defendants.

58. Without Plaintiffs' knowledge or consent, Plaintiffs' data were intentionally stored by Defendants.

59. Defendants intentionally exceeded their authority to access such data without authorization.

60. Defendants violated the SCA, 18 U.S.C. § 2701, by willfully and intentionally accessing Plaintiffs' private data without authorization.

61. Defendants have profited from their violation of the SCA, by, among other things, using improperly accessed communications and highly sensitive data for Defendants' commercial gain and benefit.

62. As a result of Defendants' conduct, Plaintiffs are entitled to all damages set forth in 18 U.S.C. § 2707 including declaratory and equitable relief, compensatory damages measured by actual damages and Defendants' profits of at least $1,000 per violation, reasonable attorneys' fees and costs, all available statutory relief, and punitive damages as determined by the Court.

COUNT THREE — UNJUST ENRICHMENT BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS

63. Plaintiffs incorporate the allegations above.

64. Plaintiffs unknowingly conferred the benefit of their driving data on Defendants—their highly sensitive and valuable personal data, driving data, and any other related data points harvested by Defendants' software.

65. Defendants acquired this data unlawfully and then sold it to other parties without Plaintiffs' consent.

66. Defendants knew and appreciated the benefit of harvesting Plaintiffs' data. Defendants sold the information to third parties for a profit.

67. Plaintiffs did not consent and received no benefit from such sale and use of their data. And it is inequitable for Defendants to retain such profits without payment for its value.

68. Therefore, Defendants have been unjustly enriched, and Plaintiffs are entitled to restitution and disgorgement of Defendants' ill-gotten gains.

COUNT FOUR — INVASION OF PRIVACY, BROUGHT BY PLAINTIFFS ON BEHALF OF THE NATIONWIDE CLASS AGAINST ALL DEFENDANTS.

69. Plaintiffs incorporate the allegations above.

70. Plaintiffs' driving data is sensitive information, information that Plaintiffs wished

to remain private and nonpublic.

71. Plaintiffs reasonably expected that their driving data would be protected and secured against access by others, including Defendants, and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose. Plaintiffs thus had a right against improper intrusion into their data.

72. Defendants intentionally intruded on the private affairs and concerns of Plaintiffs by improperly accessing Plaintiffs' driving data and using it for profit and to report on Plaintiffs' driving abilities to auto insurance companies. Plaintiffs did not knowingly consent to such practices.

73. Defendants' intrusions upon the private affairs and concerns of Plaintiffs were substantial and would be highly offensive to a reasonable person.

74. Defendants' intrusions harmed Plaintiffs in that their practices invaded Plaintiffs' privacy, profited from Plaintiffs' data without compensation, misreported Plaintiffs' and class members' driving abilities, and caused insurance rates to increase.

75. Plaintiffs seek appropriate relief for those injuries, including damages that that will reasonably compensate Plaintiffs for the harm to their privacy interests and disgorgement of profits made by Defendants as a result of their intrusions.

COUNT FIVE — CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS

76. Plaintiffs incorporate the allegations above.

77. Article I, section I of the California Constitution states:

> All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Cal. Const. art I § 1.

78. Plaintiffs have an interest in precluding the dissemination and misuse of their geolocation and other data by Defendants, and precluding the use of their personal property without observation, intrusion, or interference by Defendants.

79. Plaintiffs had no knowledge and neither consented nor authorized Defendants to obtain their driving telematics data or to share it with third parties.

80. Plaintiffs had an objectively reasonable expectation of privacy surrounding their personal data, including their driving data. Defendants' intrusion upon the seclusion of Plaintiffs occurred the moment Defendants began tracking their personal data, including driving telematics data.

81. Defendants' conduct was intentional and intruded on Plaintiffs' use of their own personal property and is highly offensive to a reasonable person because Defendants did so without the knowledge or consent of Plaintiffs.

82. As a direct and proximate result of Defendants' knowing and intentional invasions of privacy, Plaintiffs have suffered and will continue to suffer injury and damages, as alleged herein, including but not limited to overpayment for auto insurance services and loss of privacy.

83. Plaintiffs seek all relief available for invasion of privacy claims under the California Constitution, including nominal damages and general privacy damages.

COUNT SIX — VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT— WIRETAPPING LAW, CAL. PEN. CODE § 631, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS

84. Plaintiffs incorporate the allegations above.

85. California Penal Code Section 630 recognizes that "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the

continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

86. The California Wiretapping Act prohibits:

> any person . . . who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

87. Defendants are each a "person" within the scope of the California Wiretapping Act.

88. The data and transmissions within, to, and from Plaintiffs' and members' of the proposed California subclass phones constitute messages, reports, and/or communications, within the scope of Cal. Penal Code § 631(a), as they are transfers of signals, data, and intelligence transmitted by a wire, line, or cable system.

89. As alleged herein, Defendants intercepted, in real time and as they were transmitted, the contents of communications, and have diverted those communications to itself without consent.

90. Defendants intercepted these data transmissions by diverting them to its own servers, unbeknownst to Plaintiffs and the proposed California subclass members.

91. Defendants' SDK and associated mobile applications constitute a machine, instrument, or contrivance that taps or makes unauthorized connection to Plaintiffs' and members' of the proposed California subclass mobile phone communication system.

92. Plaintiff Mahoney and members of the proposed California subclass have a reasonable expectation of privacy within their homes and in their personal property Plaintiff Mahoney and members of the proposed California subclass reasonably expected privacy while

driving their vehicles and going about their daily lives. Further, there is a reasonable expectation that their location and other data are private.

93. In further violation of the California Wiretapping Act, Defendants have intentionally used or endeavored to use the contents of the communications described above knowing or having reason to know that the information was obtained through unlawful interception.

94. Defendants have used the contents of the communications described above by monetizing Plaintiffs' and members' of the proposed California subclass personal data for their own financial and commercial benefit, obtaining substantial profit.

95. Defendants knew or should have known that the detailed information they used was captured in secret in violation of the Act.

96. Upon information and belief, Defendants disclose and unlawfully obtain data for their own financial gain to this day.

97. Upon information and belief, Defendants disclose and unlawfully obtain data for their own financial gain to this day.

98. Neither Defendants nor any other person informed Plaintiffs and members of the proposed California subclass that Defendants were intercepting and transmitting their data. Plaintiffs and members of the proposed California subclass did not know Defendants were intercepting and recording their data, as such they could not and did not consent for their data to be intercepted and/or used by Defendants.

99. As a direct and proximate result of Defendants' violations of the Wiretapping Act, Plaintiff and members of the proposed California subclass were injured and suffered damages, a

loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

100. Defendants were unjustly enriched by their violations of the Wiretapping Act.

101. Pursuant to California Penal Code Section 637.2, Plaintiffs and members of the proposed California subclass have been injured by Defendants' violations of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief, plus reasonable attorneys' fees and costs.

COUNT SEVEN — VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT—ELECTRONIC TRACKING DEVICE, CAL. PEN. CODE § 637.7, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS

102. Plaintiffs incorporate the allegations above.

103. California Penal Code Section 637.7 prohibits any person from using an electronic tracking device to determine the location or movements of any person.

104. Defendants are each a "person" within the scope of the California Invasion of Privacy Act ("CIPA").

105. Defendants' SDK covertly integrated within third-party mobile applications and downloaded onto Plaintiffs' and members' of the proposed California subclass phones is an "electronic tracking device" as defined by CIPA as it is a device that is integrated into the user's phone and reveals the user's location, movement, and other data by the transmission of electronic signals through the intercept, collection, and dissemination of Plaintiffs' and California Subclass members' location information.

106. Defendants violated Cal. Penal Code § 637.7 by attaching Defendants' SDK to Plaintiffs' and members' of the proposed California subclass phones and thereby intercepting,

obtaining, collecting, taking, storing, using, and disseminating data belonging to Plaintiffs and members of the proposed California subclass.

107. Neither Defendants nor any other person informed Plaintiffs and members of the proposed California subclass or meaningfully disclosed that Defendants integrated their SDK, an electronic tracking device, into consumers' phones.

108. The collection of data from Plaintiffs and members of the proposed California subclass without full and informed consent violated and continues to violate Cal. Penal Code § 637.7.

109. As a direct and proximate result of Defendants' violations, Plaintiffs and California Subclass members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

110. Pursuant to Cal. Pen. Code Section 637.2, Plaintiffs and California Subclass members have been injured by Defendants' violations of the CIPA and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief, plus reasonable attorneys' fees and costs.

COUNT EIGHT — VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*, BROUGHT BY PLAINTIFF MAHONEY AND THE CALIFORNIA SUBCLASS AGAINST ALL DEFENDANTS

111. Plaintiffs incorporate the allegations above.

112. California's Unfair Competition Law (UCL) defines "unfair competition" to include any "unlawful, unfair, or fraudulent" business act or practice. Cal. Bus. & Prof. Code §§17200 et seq.

113. Defendants have engaged in acts and practices that are unfair in violation of the UCL by using Arity's software to collect, store, and sell personal data belonging to Plaintiffs.

114. Defendants acts and practices are unlawful because Defendants violate and continue to violate California common law, constitutional, and statutory rights to privacy, including but not limited to the California Constitution Article I, Section 1.

115. Defendants acted intentionally, knowingly, and maliciously, and recklessly disregarded Plaintiffs' rights because Defendants intentionally intercepted, collected, used, and sold Plaintiffs' driving data without obtaining their consent.

116. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Plaintiffs have suffered and will continue to suffer injury, including but not limited to: loss of privacy, loss of control of their private data, unauthorized dissemination of their valuable driving data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their driving data, and economic harm stemming from the exploitation of their driving data.

117. Plaintiffs seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendants' unlawful, unfair, and unconscionable practices or use of their driving data; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure section 1021.5; injunctive relief; and other appropriate equitable relief that the Court deems proper.

COUNT NINE — VIOLATION OF 815 ILL. COMP. STAT. 505/1 *ET SEQ*., BROUGHT BY PLAINTIFF SCHULTZ AND THE ILLINOIS SUBCLASS AGAINST ALL DEFENDANTS

118. Plaintiff Schultz incorporates the allegations above.

119. Defendants' deceptive scheme to collect, sell, and use driving data without Plaintiff Schultz's knowledge or consent violates the Illinois Consumer Fraud and Deceptive Business Practices Act because it is an unfair and deceptive business practice.

120. Defendants intended to profit from the data sharing practices and intended to keep

Plaintiffs in the dark about the practices. Their practices were thus deceptive.

121. Defendants intended for Plaintiff Schultz to not learn about the sale of his data to insurance companies. They did not notify Plaintiff Schultz that his information was being collected and sold, much less for purposes of increasing his car insurance rates. As a result, Plaintiff Schultz did not learn the material fact that Defendants were collecting and sharing his driving data and were harmed when their data was in fact shared.

122. Defendants' practices were also unfair. Sharing private data without a person's consent offends Illinois's public policy towards protection of and autonomy for consumer data. Defendants' practices are also unscrupulous, because they entice consumers with benefits that lead to them unwittingly offer up their data for Defendants' benefit. Finally, Defendants' practices cause substantial injury to consumers, because the practice results in the disclosure of large amounts of driving data without any benefit to consumers.

123. Defendants knew or should have known that sharing individuals' driving data inaccurately portrays Plaintiff Schultz's driving experience and can unfairly negatively impact his eligibility for and/or cost of insurance.

124. Defendants caused harm because their practices invaded the privacy of Plaintiff Schultz, profited from his data without compensation, misreported Plaintiff Schultz's driving abilities, and caused his insurance rates to increase.

125. Plaintiff Schultz would not have consented to Defendants' practices, had he known about them.

126. As a result of the violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, Plaintiff Schultz is entitled to actual damages, statutory damages, punitive damages, injunctive relief, and reasonable attorney's fees and costs.

VIII. PRAYER FOR RELIEF

127. Plaintiffs, on their own behalf and on behalf of other members of the proposed class and subclasses, asks the court for the following relief:

A. An order certifying the proposed class and subclasses under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), designating Plaintiffs as named representatives of the class and subclasses, and appointing the attorneys below as class counsel under Rule 23(g);

B. Actual damages;

C. Statutory damages;

D. Punitive damages;

E. An order enjoining Plaintiffs from sharing Plaintiffs' and the classes' driving information with third parties;

F. An order requiring Defendants to delete Plaintiffs' and class member driving data in their possession;

G. Attorneys' fees, expenses, and taxable costs;

H. Pre- and post-judgment interest; and

I. For any other relief that the court deems just and proper.

IX. JURY AND TRIAL DEMAND

128. Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs on behalf of the classes demand a trial by jury of all claims asserted in this complaint that are so triable.

MINER, BARNHILL & GALLAND, P.C.

By */s/ Robert S. Libman*

Robert S. Libman
Bernardo Lopez
325 N LaSalle, Suite 350
Chicago, IL 60654
Phone: (312) 751-1170
rlibman@lawmbg.com
blopez@lawmbg.com

KELLER ROHRBACK L.L.P.
Derek Loeser (*pro hac vice* to follow)
Cari Campen Laufenberg (*pro hac vice* to follow)
Adele Daniel (*pro hac vice* to follow)
Patrick T. Marriott (*pro hac vice* to follow)
1201 Third Avenue, Suite 3400
Seattle, WA 98101-3268
Phone: (206) 623-1900
Fax: (206) 623-3384
claufenberg@kellerrohrback.com
adaniel@kellerrohrback.com
pmarriott@kellerrohrback.com

Christopher L. Springer (*pro hac vice* to follow)
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Phone: (805) 456-1496
Fax: (805) 456-1497
cspringer@kellerrohrback.com

Attorneys for Plaintiffs