UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: ALLSTATE & ARITY CONSUMER PRIVACY LITIGATION	Master Docket No. 1:25-cv-00407 **CONSOLIDATED CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF** **JURY TRIAL DEMANDED**

TABLE OF CONTENTS

Plaintiffs Michelle Anderson, Delia Arellano, Michael Azar, Amanda Bare, Matthew Baumgartner, Danny Carroll, Beth DeValkeneer, Kimberleigh Duffield, James Eppley, Toyette Flowers, Christopher Freel, Jade Gable, Christy Hartline, Eddie Hernandez, Joseph Jackson, Kimberly Kelley, Daniel Kilgo, Michael Mahoney, Sofia Malvar, James McNeill, Jennifer Monilaw, Amanda Quam, Annette Rastrelli, Nicole Rehfuss, Dorian Rochester, Robert Sanginito, Scott Schultz, Chrystie Seay, Ashika Singh, Antonette Slater, Kayla Smith, Robert Smith, Rita Streifel, Kimberly Summersill, Valencia Tucker, Tracy Tupper, James Williams, Jacob Winkelvoss, and Eboni Wright, individually and on behalf of all others similarly situated (collectively, "Consolidated Plaintiffs" or "Plaintiffs"), bring this Consolidated Class Action Complaint[1] against The Allstate Corporation, Allstate Insurance Company, Allstate Vehicle and Property Insurance Company, Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, "Defendants"). Plaintiffs allege the following facts based upon personal knowledge, investigation by counsel, and on information and belief:

I. NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendants seeking to redress the harms caused by Defendants' surreptitious, and unconsented, collection of Plaintiffs' personal information. The consumer driving data Defendants collected is highly invasive and personal, including information about what consumers did inside their cars each and every time they drove or rode in a vehicle sufficient to "fingerprint" (i.e., identify) each individual driver. The data Defendants harvested from each consumer was tied to individuals and included geolocation, route history, driving schedule, fuel or charging levels, phone usage, hard braking events, hard

[1] This is a corrected version of this Consolidated Complaint filed earlier today. This corrected version fixes numbering issues and adds an omitted signature.

acceleration events, tailgating, time spent idle, speeds over 80 miles per hour, vehicle speed, average speed, late night driving, driver attention, and more (hereinafter, "Driving Data"). Defendants collected consumer Driving Data from consumers' own mobile devices, in-car devices and apps, and the vehicles they drove—without consumers' knowledge or consent—and then used that personally identifying information for their own purposes (including to calculate insurance rates for Plaintiffs) or sold the data to third parties for profit.

2. Defendants Allstate Insurance Company and Allstate Vehicle and Property Insurance Company are all insurance companies and are subsidiaries of and owned by Defendant The Allstate Corporation (collectively, the "Allstate Defendants"). The Allstate Defendants sell vehicle insurance policies to individual consumers, pricing their insurance policies based on factors such as the driver's age, where they live, what type of vehicle they drive, and their driving record. Consumers provide this information to Allstate Defendants when they apply for an insurance policy.

3. Defendants Arity, LLC, Arity 875, LLC, and Arity Services, LLC (collectively, the "Arity Defendants") are all technology companies and are subsidiaries of and owned by Defendant The Allstate Corporation. Arity Defendants collect personal information from consumers via their mobile apps and websites, third-party mobile apps, Arity's software development kit ("SDK"), or via devices installed in consumers' vehicles.[2]

[2] Arity, "Privacy Statement," (effective date: November 1, 2024), https://arity.com/privacy/ (last accessed on May 22, 2025).

4. Together, Defendants conspired to collect and sell the driving behavior data of at least 40 million consumers, totaling "2 trillion miles," collecting more than one billion miles of driving data every single day.[3]

5. Defendants collect this data in part by developing and embedding their own software into third-party apps. Once a consumer downloaded one of those apps onto their phone, Defendants' software was downloaded as well, enabling Defendants to maintain a connection with the consumer's phone, whether the consumer wanted it or not. Using the embedded software, Defendants monitor the consumer's location and behavior in real time and by pulling a trove of personal data directly from the consumer's phone.

6. In order to ensure their software was included in third-party apps, Defendants paid app developers millions of dollars to integrate Defendants' SDK into the third-party apps. Defendants also provided bonuses to these app developers as an additional incentive to participate in this integration. The success of Defendants' efforts to expand the reach of their software can be seen in their own claim that their software enables them to "capture data" in "real-time" from "40 [million] active mobile connections."[4]

7. The personal data collected by Defendants included information that together would be used to create a profile of a consumer's driving behavior, such as a phone's geolocation data, as well as phone usage, driver attention, accelerometer data, magnetometer data, and gyroscopic data, which monitors details such as the phone's altitude, longitude, latitude, bearing, GPS time, speed, and accuracy.

[3] Arity, "8 facts for 8 years of Arity!," https://arity.com/move/8-facts-for-8-years-of-arity/(last accessed on May 22, 2025).

[4] Arity, https://arity.com/solutions/real-time-insights/ (last accessed on May 22, 2025).

8. Defendants also harvested additional identifying information, including first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), and device ID (together, "Identity Information").

9. Defendants used the Driving Data and Identity Information (together, "Personal Data") to build a driving behavior database consisting of the "largest driving behavior dataset tied to insurance claims," which they used to both support and expand their own insurance business and to sell to third parties for profit.[5]

10. Defendants marketed and sold the Personal Data obtained through third-party apps as "driving" data purportedly reflecting consumers' driving habits. The Personal Data, however, was and is fundamentally flawed.

11. For example, the Personal Data was used and sold as "driving" data even though the data was collected from, and in reality, reflected the location, usage, and movement of consumers' phones—not the consumer's driving behavior. Thus, Defendants collected the consumer's data and attributed it to individuals regardless of whether that individual was in fact operating a vehicle at that time. For example, Defendants collected and reported data as reflecting an individual's driving behavior even when the individual was riding as a passenger in a motor vehicle, or even riding a roller coaster.[6]

12. The Driving Data was and is further decontextualized from the ways that vehicle owners can and must safely operate their vehicles. For example, a "hard braking event" may in fact be a safe and appropriate response to driving conditions—if, for example, a child or animal

[5] Arity, *supra* n.2.

[6] 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-cutsdriving-score-man-riding-the-beast-kings-island/75554987007/.

suddenly enters the roadway—but such an event could still have a negative impact on the individual's risk score, as assigned by Defendants.

13. Defendants have recently begun to expand the sources of their data by buying vehicle data directly from car manufacturers, such as Toyota, Lexus, Mazda, Chrysler, Dodge, Fiat, Jeep, Maserati, and Ram.

14. Defendants used this Personal Data to make insurance coverage decisions for consumers who sought vehicle insurance with them. They would also sell this data to other insurers, enabling those insurers to make their own coverage decisions about individual consumers. Defendants and other insurers used consumers' Personal Data to decide whether to market insurance products to individual consumers, how much to increase a consumer's insurance premium or whether to provide them with insurance at all. These decisions were made without the consumer's knowledge that their Personal Data had been collected and used by Defendants to affect their insurance coverage.

15. Consumers were not informed of and did not consent to this collection and use of their Personal Data.

16. The putative Class is comprised of millions of Americans who were not informed of, did not consent to, and suffered harms as a result of Defendants' ongoing collection, use, and sale of their Personal Data. Plaintiffs and Class Members seek compensatory, consequential, statutory, punitive, general, and nominal damages, disgorgement and restitution, and injunctive relief on behalf of all consumers whose data was captured, collected, stored, and sold by Defendants without their knowledge and consent.

II. PARTIES

A. Plaintiffs

17. **Plaintiff Michelle Anderson** is an adult individual and a natural person, citizen of Michigan, where she resides and intends to stay.

18. In or around 2021, Plaintiff Anderson downloaded and used Life360 ("Apps") on her mobile phone. Plaintiff Anderson downloaded the Apps for personal use. Plaintiff Anderson reviewed the prominent information about the nature and function of the Apps presented to Plaintiff Anderson prior to downloading and using the Apps. Plaintiff Anderson was not provided meaningful notice that Defendants would use the Apps to collect and share her Personal Data.

19. Plaintiff Anderson is informed and believes that the Apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Anderson's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

20. Plaintiff Anderson was unaware that Allstate and Arity's SDK had been integrated into the Apps at the time she installed, and later when she used the Apps. Through the Apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Anderson's driving behavior, without Plaintiff Anderson's knowledge or consent.

21. Upon information and belief, insurance premiums paid by Plaintiff Anderson was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Anderson rode as a passenger numerous times while carrying Plaintiff Anderson's mobile phone, and any assumption that the movement of Plaintiff Anderson's phone during those trips reflected Plaintiff Anderson's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Anderson paid more for insurance than she otherwise would have.

22. Defendants' interception, collection, and monetization of Plaintiff Anderson's highly sensitive Personal Data without consent caused Plaintiff Anderson harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Anderson's expense.

23. Because of Defendants' conduct, Plaintiff Anderson has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

24. Defendants' secret collection of Plaintiff Anderson's Personal Data deprived Plaintiff of control over valuable personal information. Plaintiff Anderson's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing

access to such data to insurers, marketers, and other third parties. Plaintiff Anderson did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Anderson's Personal Data for Defendants' financial benefit. Plaintiff Anderson's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Anderson's knowledge, compensation, or control. Plaintiff Anderson would have expected compensation in exchange for providing Plaintiff Anderson's Personal Data to third parties looking to use it for their own benefit.

25. Plaintiff Anderson had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

26. **Plaintiff Delia Arellano** is an adult individual and a natural person, citizen of Utah, where she resides and intends to stay.

27. In or around 2019, Plaintiff Arellano downloaded and used the Life360 app on her mobile phone. Plaintiff Arellano downloaded the app for personal use. Plaintiff Arellano reviewed the prominent information about the nature and function of the app presented to Plaintiff Arellano prior to downloading and using the app. Plaintiff Arellano was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

28. Plaintiff Arellano is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Arellano's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

29. Plaintiff Arellano was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Arellano's driving behavior, without Plaintiff Arellano's knowledge or consent.

30. Upon information and belief, insurance premiums paid by Plaintiff Arellano was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Arellano rode as a passenger numerous times while carrying Plaintiff Arellano's mobile phone, and any assumption that the movement of Plaintiff Arellano's phone during those trips reflected Plaintiff Arellano's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Arellano paid more for insurance than she otherwise would have.

31. Defendants' interception, collection, and monetization of Plaintiff Arellano's highly sensitive Personal Data without consent caused Plaintiff Arellano harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Arellano's expense.

32. Because of Defendants' conduct, Plaintiff Arellano has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

33. Defendants' secret collection of Plaintiff Arellano's Personal Data deprived Plaintiff Arellano of control over valuable personal information. Plaintiff Arellano's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Arellano did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Arellano's Personal Data for Defendants' financial benefit. Plaintiff Arellano's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Arellano's knowledge, compensation, or control. Plaintiff Arellano would have expected compensation in exchange for providing Plaintiff Arellano's Personal Data to third parties looking to use it for their own benefit.

34. Plaintiff Arellano had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

35. **Plaintiff Michael Azar** is an adult individual and a natural person, citizen of California, where he resides and intends to stay.

36. In or around 2022, Plaintiff Azar downloaded and used the GasBuddy app on his mobile phone. Plaintiff Azar downloaded the app for personal use. Plaintiff Azar reviewed the

prominent information about the nature and function of the app presented to Plaintiff Azar prior to downloading and using the app. Plaintiff Azar was not provided meaningful notice that Defendants would use the app to collect and share his Personal Data.

37. Plaintiff Azar is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Azar's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

38. Plaintiff Azar was unaware that Allstate and Arity's SDK had been integrated into the app at the time he installed, and later when he used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Azar's driving behavior, without Plaintiff Azar's knowledge or consent.

39. Upon information and belief, insurance premiums paid by Plaintiff Azar was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Azar rode as a passenger numerous times while carrying Plaintiff Azar's mobile phone, and any assumption that the movement of Plaintiff Azar's phone during those trips reflected Plaintiff Azar's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Azar paid more for insurance than he otherwise would have.

40. Defendants' interception, collection, and monetization of Plaintiff Azar's highly sensitive Personal Data without consent caused Plaintiff Azar harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Azar's expense.

41. Because of Defendants' conduct, Plaintiff Azar has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

42. Defendants' secret collection of Plaintiff Azar's Personal Data deprived Plaintiff Azar of control over valuable personal information. Plaintiff Azar's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Azar did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Azar's Personal Data for Defendants' financial benefit. Plaintiff Azar's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Azar's knowledge,

compensation, or control. Plaintiff Azar would have expected compensation in exchange for providing Plaintiff Azar's Personal Data to third parties looking to use it for their own benefit.

43. Plaintiff Azar had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

44. **Plaintiff Amanda Bare** is an adult individual and a natural person, citizen of California, where she resides and intends to stay.

45. In or around 2023, Plaintiff Bare downloaded and used the Life360 app on her mobile phone. Plaintiff Bare downloaded the app for personal use. Plaintiff Bare reviewed the prominent information about the nature and function of the app presented to Plaintiff Bare prior to downloading and using the app. Plaintiff Bare was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

46. Plaintiff Bare is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Bare's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

47. Plaintiff Bare was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Bare's driving behavior, without Plaintiff Bare's knowledge or consent.

48. Upon information and belief, insurance premiums paid by Plaintiff Bare was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Bare rode as a passenger numerous times while carrying Plaintiff Bare's mobile phone, and any assumption that the movement of Plaintiff Bare's phone during those trips reflected Plaintiff Bare's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Bare paid more for insurance than she otherwise would have.

49. Defendants' interception, collection, and monetization of Plaintiff Bare's highly sensitive Personal Data without consent caused Plaintiff Bare harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Bare's expense.

50. Because of Defendants' conduct, Plaintiff Bare has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

51. Defendants' secret collection of Plaintiff Bare's Personal Data deprived Plaintiff Bare of control over valuable personal information. Plaintiff Bare's Personal Data has intrinsic

and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Bare did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Bare's Personal Data for Defendants' financial benefit. Plaintiff Bare's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Bare's knowledge, compensation, or control. Plaintiff Bare would have expected compensation in exchange for providing Plaintiff Bare's Personal Data to third parties looking to use it for their own benefit.

52. Plaintiff Bare had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

53. **Plaintiff Matthew Baumgartner** is an adult individual and a natural person, citizen of South Carolina, where he resides and intends to stay.

54. In or around 2015, Plaintiff Baumgartner downloaded and used the GasBuddy and Life360 apps on his mobile phone. Plaintiff Baumgartner downloaded the apps for personal use. Plaintiff Baumgartner reviewed the prominent information about the nature and function of the apps presented to Plaintiff Baumgartner prior to downloading and using the apps. Plaintiff Baumgartner was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

55. Plaintiff Baumgartner is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Baumgartner's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

56. Plaintiff Baumgartner was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Baumgartner's driving behavior, without Plaintiff Baumgartner's knowledge or consent.

57. In early 2025, Plaintiff Baumgartner purchased insurance from Allstate, or one of its subsidiaries. Plaintiff Baumgartner is an Allstate insurance subscriber, and has been continuously from his initial purchase.

58. Upon information and belief, insurance premiums paid by Plaintiff Baumgartner was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Baumgartner rode as a passenger numerous times while carrying Plaintiff Baumgartner's mobile phone, and any assumption that the movement of Plaintiff Baumgartner's phone during those trips reflected Plaintiff Baumgartner's

driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Baumgartner paid more for insurance than he otherwise would have.

59. Defendants' interception, collection, and monetization of Plaintiff Baumgartner's highly sensitive Personal Data without consent caused Plaintiff Baumgartner harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Baumgartner's expense.

60. Because of Defendants' conduct, Plaintiff Baumgartner has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

61. Defendants' secret collection of Plaintiff Baumgartner's Personal Data deprived Plaintiff Baumgartner of control over valuable personal information. Plaintiff Baumgartner's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Baumgartner did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Baumgartner's Personal Data for Defendants' financial benefit. Plaintiff Baumgartner's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Baumgartner's knowledge, compensation, or control. Plaintiff Baumgartner would have expected compensation in exchange for providing Plaintiff Baumgartner's Personal Data to third parties looking to use it for their own benefit.

62. Plaintiff Baumgartner had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

63. **Plaintiff Danny Carroll** is an adult individual and a natural person, citizen of Missouri, where he resides and intends to stay.

64. In or around 2020, Plaintiff Carroll downloaded and used the GasBuddy and Fuel Rewards apps on his mobile phone. In addition, in or around 2024, Plaintiff Carroll downloaded and used the SiriusXM app. Plaintiff Carroll downloaded the apps for personal use. Plaintiff Carroll reviewed the prominent information about the nature and function of the apps presented to Plaintiff Carroll prior to downloading and using the apps. Plaintiff Carroll was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

65. Plaintiff Carroll is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Carroll's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

66. Plaintiff Carroll was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Carroll's driving behavior, without Plaintiff Carroll's knowledge or consent.

67. Upon information and belief, insurance premiums paid by Plaintiff Carroll was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Carroll rode as a passenger numerous times while carrying Plaintiff Carroll's mobile phone, and any assumption that the movement of Plaintiff Carroll's phone during those trips reflected Plaintiff Carroll's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Carroll paid more for insurance than he otherwise would have.

68. Defendants' interception, collection, and monetization of Plaintiff Carroll's highly sensitive Personal Data without consent caused Plaintiff Carroll harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Carroll's expense.

69. Because of Defendants' conduct, Plaintiff Carroll has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

70. Defendants' secret collection of Plaintiff Carroll's Personal Data deprived Plaintiff Carroll of control over valuable personal information. Plaintiff Carroll's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing

access to such data to insurers, marketers, and other third parties. Plaintiff Carroll did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Carroll's Personal Data for Defendants' financial benefit. Plaintiff Carroll's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Carroll's knowledge, compensation, or control. Plaintiff Carroll would have expected compensation in exchange for providing Plaintiff Carroll's Personal Data to third parties looking to use it for their own benefit.

71. Plaintiff Carroll had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

72. **Plaintiff Beth DeValkeneer** is an adult individual and a natural person, citizen of Pennsylvania, where she resides and intends to stay.

73. In or around 2019, Plaintiff DeValkeneer downloaded and used Life360 ("Apps") on her mobile phone. Plaintiff DeValkeneer downloaded the Apps for personal use and was not provided meaningful notice that Defendants would use the Apps to collect and share her Personal Data.

74. Plaintiff DeValkeneer is informed and believes that the Apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff DeValkeneer's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

75. Plaintiff DeValkeneer was unaware that Allstate and Arity's SDK had been integrated into the Apps at the time she installed, and later when she used the Apps. Through the Apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff DeValkeneer's driving behavior, without Plaintiff DeValkeneer's knowledge or consent.

76. Upon information and belief, insurance premiums paid by Plaintiff DeValkeneer was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff DeValkeneer paid more for insurance than she otherwise would have.

77. Defendants' interception, collection, and monetization of Plaintiff DeValkeneer's highly sensitive Personal Data without consent caused Plaintiff DeValkeneer harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff DeValkeneer's expense.

78. Because of Defendants' conduct, Plaintiff DeValkeneer has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

79. Defendants' secret collection of Plaintiff DeValkeneer's Personal Data deprived Plaintiff DeValkeneer of control over valuable personal information. Plaintiff DeValkeneer's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff DeValkeneer did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff DeValkeneer's Personal Data for Defendants' financial benefit. Plaintiff DeValkeneer's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff DeValkeneer's knowledge, compensation, or control.

80. Plaintiff DeValkeneer had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

81. **Plaintiff Kimberleigh Duffield** is an adult individual and a natural person, citizen of California, where she resides and intends to stay.

82. In or around 2017, Plaintiff Duffield downloaded and used the Life360 app on her mobile phone. Plaintiff Duffield downloaded the app for personal use. Plaintiff Duffield reviewed the prominent information about the nature and function of the app presented to Plaintiff Duffield prior to downloading and using the app. Plaintiff Duffield was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

83. Plaintiff Duffield is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Duffield's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

84. Plaintiff Duffield was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Duffield's driving behavior, without Plaintiff Duffield's knowledge or consent.

85. Upon information and belief, insurance premiums paid by Plaintiff Duffield was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Duffield rode as a passenger numerous

times while carrying Plaintiff Duffield's mobile phone, and any assumption that the movement of Plaintiff Duffield's phone during those trips reflected Plaintiff Duffield's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant Duffield's covert collection and use of her Personal Data, Plaintiff Duffield paid more for insurance than she otherwise would have.

86. Defendants' interception, collection, and monetization of Plaintiff Duffield's highly sensitive Personal Data without consent caused Plaintiff Duffield harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Duffield's expense.

87. Because of Defendants' conduct, Plaintiff Duffield has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

88. Defendants' secret collection of Plaintiff Duffield's Personal Data deprived Plaintiff Duffield of control over valuable personal information. Plaintiff Duffield's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Duffield did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Duffield's Personal Data for Defendants' financial benefit. Plaintiff Duffield's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Duffield's knowledge, compensation, or control. Plaintiff Duffield would have expected compensation in exchange for providing Plaintiff Duffield's Personal Data to third parties looking to use it for their own benefit.

89. Plaintiff Duffield had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

90. **Plaintiff James Eppley** is an adult individual and a natural person, citizen of Pennsylvania, where he resides and intends to stay.

91. In or around 2021, Plaintiff Eppley downloaded and used the GasBuddy and Fuel Rewards apps on his mobile phone. Plaintiff Eppley downloaded the apps for personal use. Plaintiff Eppley reviewed the prominent information about the nature and function of the apps presented to Plaintiff Eppley prior to downloading and using the apps. Plaintiff Eppley was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

92. Plaintiff Eppley is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Eppley's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

93. Plaintiff Eppley was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Eppley's driving behavior, without Plaintiff Eppley's knowledge or consent.

94. Upon information and belief, insurance premiums paid by Plaintiff Eppley was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Eppley rode as a passenger numerous times while carrying Plaintiff Eppley's mobile phone, and any assumption that the movement of Plaintiff Eppley's phone during those trips reflected Plaintiff Eppley's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Eppley paid more for insurance than he otherwise would have.

95. Defendants' interception, collection, and monetization of Plaintiff Eppley's highly sensitive Personal Data without consent caused Plaintiff harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Eppley's expense.

96. Because of Defendants' conduct, Plaintiff Eppley has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

97. Defendants' secret collection of Plaintiff Eppley's Personal Data deprived Plaintiff Eppley of control over valuable personal information. Plaintiff Eppley's Personal Data has

intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Eppley did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Eppley's Personal Data for Defendants' financial benefit. Plaintiff Eppley's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Eppley's knowledge, compensation, or control. Plaintiff Eppley would have expected compensation in exchange for providing Plaintiff Eppley's Personal Data to third parties looking to use it for their own benefit.

98. Plaintiff Eppley had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

99. **Plaintiff Toyette Flowers** is an adult individual and a natural person, citizen of Wisconsin, where she resides and intends to stay.

100. In or around 2022, Plaintiff Flowers downloaded and used the SiriusXM and Routely apps on her mobile phone. Plaintiff Flowers downloaded the apps for personal use. Plaintiff Flowers reviewed the prominent information about the nature and function of the apps presented to Plaintiff Flowers prior to downloading and using the apps. Plaintiff Flowers was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

101. Plaintiff Flowers is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Flowers' phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

102. Plaintiff Flowers was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Flowers' driving behavior, without Plaintiff Flowers' knowledge or consent.

103. Upon information and belief, insurance premiums paid by Plaintiff Flowers was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Flowers rode as a passenger numerous times while carrying Plaintiff Flowers' mobile phone, and any assumption that the movement of Plaintiff Flowers' phone during those trips reflected Plaintiff Flowers' driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Flowers paid more for insurance than she otherwise would have.

104. Defendants' interception, collection, and monetization of Plaintiff Flowers' highly sensitive Personal Data without consent caused Plaintiff Flowers harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Flowers' expense.

105. Because of Defendants' conduct, Plaintiff Flowers has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

106. Defendants' secret collection of Plaintiff Flowers' Personal Data deprived Plaintiff Flowers of control over valuable personal information. Plaintiff Flowers' Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Flowers did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Flowers' Personal Data for Defendants' financial benefit. Plaintiff Flowers' Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Flowers' knowledge, compensation, or control. Plaintiff Flowers would have expected compensation in exchange for providing Plaintiff Flowers' Personal Data to third parties looking to use it for their own benefit.

107. Plaintiff Flowers had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

108. **Plaintiff Christopher Freel** is an adult individual and a natural person, citizen of Texas, where he resides and intends to stay.

109. In or around 2020, Plaintiff Freel downloaded and used the Life360 on his mobile phone. Plaintiff downloaded the app for personal use. Plaintiff Freel reviewed the prominent

information about the nature and function of the app presented to Plaintiff Freel prior to downloading and using the app. Plaintiff Freel was not provided meaningful notice that Defendants would use the app to collect and share his Personal Data.

110. Plaintiff Freel is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Freel's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

111. Plaintiff Freel was unaware that Allstate and Arity's SDK had been integrated into the app at the time he installed, and later when he used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Freel's driving behavior, without Plaintiff Freel's knowledge or consent.

112. Upon information and belief, insurance premiums paid by Plaintiff Freel was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Freel rode as a passenger numerous times while carrying Plaintiff Freel's mobile phone, and any assumption that the movement of Plaintiff Freel's phone during those trips reflected Plaintiff Freel's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Freel paid more for insurance than he otherwise would have.

113. Defendants' interception, collection, and monetization of Plaintiff Freel's highly sensitive Personal Data without consent caused Plaintiff Freel harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Freel's expense.

114. Because of Defendants' conduct, Plaintiff Freel has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

115. Defendants' secret collection of Plaintiff Freel's Personal Data deprived Plaintiff Freel of control over valuable personal information. Plaintiff Freel's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Freel did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Freel's Personal Data for Defendants' financial benefit. Plaintiff Freel's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Freel's knowledge,

compensation, or control. Plaintiff Freel would have expected compensation in exchange for providing Plaintiff Freel's Personal Data to third parties looking to use it for their own benefit.

116. Plaintiff Freel had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

117. **Plaintiff Jade Gable** is an adult individual and a natural person, citizen of Arizona, where she resides and intends to stay.

118. In or around 2024, Plaintiff Gable downloaded and used the Life360 app on her mobile phone. Plaintiff Gable downloaded the app for personal use. Plaintiff Gable reviewed the prominent information about the nature and function of the app presented to Plaintiff Gable prior to downloading and using the app. Plaintiff Gable was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

119. Plaintiff Gable is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Gable's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

120. Plaintiff Gable was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Gable's driving behavior, without Plaintiff Gable's knowledge or consent.

121. Upon information and belief, insurance premiums paid by Plaintiff Gable was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Gable rode as a passenger numerous times while carrying Plaintiff Gable's mobile phone, and any assumption that the movement of Plaintiff Gable's phone during those trips reflected Plaintiff Gable's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Gable paid more for insurance than she otherwise would have.

122. Defendants' interception, collection, and monetization of Plaintiff Gable's highly sensitive Personal Data without consent caused Plaintiff Gable harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Gable's expense.

123. Because of Defendants' conduct, Plaintiff Gable has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

124. Defendants' secret collection of Plaintiff Gable's Personal Data deprived Plaintiff Gable of control over valuable personal information. Plaintiff Gable's Personal Data has intrinsic

and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Gable did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Gable's Personal Data for Defendants' financial benefit. Plaintiff Gable's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Gable's knowledge, compensation, or control. Plaintiff Gable would have expected compensation in exchange for providing Plaintiff Gable's Personal Data to third parties looking to use it for their own benefit.

125. Plaintiff Gable had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

126. **Plaintiff Christy Hartline** is an adult individual and a natural person, citizen of Oregon, where she resides and intends to stay.

127. In or around 2022, Plaintiff Hartline downloaded and used the Life360 and SiriusXM apps on her mobile phone. Plaintiff Hartline downloaded the apps for personal use. Plaintiff Hartline reviewed the prominent information about the nature and function of the apps presented to Plaintiff Hartline prior to downloading and using the apps. Plaintiff Hartline was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

128. Plaintiff Hartline is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Hartline's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

129. Plaintiff Hartline was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Hartline's driving behavior, without Plaintiff Hartline's knowledge or consent.

130. Upon information and belief, insurance premiums paid by Plaintiff Hartline was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Hartline rode as a passenger numerous times while carrying Plaintiff Hartline's mobile phone, and any assumption that the movement of Plaintiff Hartline's phone during those trips reflected Plaintiff Hartline's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Hartline paid more for insurance than she otherwise would have.

131. Defendants' interception, collection, and monetization of Plaintiff Hartline's highly sensitive Personal Data without consent caused Plaintiff Hartline harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Hartline's expense.

132. Because of Defendants' conduct, Plaintiff Hartline has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

133. Defendants' secret collection of Plaintiff Hartline's Personal Data deprived Plaintiff Hartline of control over valuable personal information. Plaintiff Hartline's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Hartline did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Hartline's Personal Data for Defendants' financial benefit. Plaintiff Hartline's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Hartline's knowledge, compensation, or control. Plaintiff Hartline would have expected compensation in exchange for providing Plaintiff Hartline's Personal Data to third parties looking to use it for their own benefit.

134. Plaintiff Hartline had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

135. **Plaintiff Eddie Hernandez** is an adult individual and a natural person, citizen of California, where he resides and intends to stay.

136. In or around 2020, Plaintiff Hernandez downloaded and used Life360 on his mobile phone. As well, in or around 2022, Sirius XM (collectively with Life360, the "Apps"). Plaintiff

Hernandez downloaded the Apps for personal use. Plaintiff Hernandez reviewed the prominent information about the nature and function of the Apps presented to Plaintiff Hernandez prior to downloading and using the Apps. Plaintiff Hernandez was not provided meaningful notice that Defendants would use the Apps to collect and share his Personal Data.

137. Plaintiff Hernandez is informed and believes that the Apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Hernandez's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

138. Plaintiff Hernandez was unaware that Allstate and Arity's SDK had been integrated into the Apps at the time he installed, and later when he used the Apps. Through the Apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Hernandez's driving behavior, without Plaintiff Hernandez's knowledge or consent.

139. Upon information and belief, insurance premiums paid by Plaintiff Hernandez was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Hernandez rode as a passenger numerous times while carrying Plaintiff Hernandez's mobile phone, and any assumption that the movement of Plaintiff Hernandez's phone during those trips reflected Plaintiff Hernandez's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Hernandez paid more for insurance than he otherwise would have.

140. Defendants' interception, collection, and monetization of Plaintiff Hernandez's highly sensitive Personal Data without consent caused Plaintiff Hernandez harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Hernandez's expense.

141. Because of Defendants' conduct, Plaintiff Hernandez has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

142. Defendants' secret collection of Plaintiff Hernandez's Personal Data deprived Plaintiff Hernandez of control over valuable personal information. Plaintiff Hernandez's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Hernandez did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Hernandez's Personal Data for Defendants' financial benefit. Plaintiff Hernandez's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using

that data without Plaintiff Hernandez' knowledge, compensation, or control. Plaintiff Hernandez would have expected compensation in exchange for providing Plaintiff Hernandez's Personal Data to third parties looking to use it for their own benefit.

143. Plaintiff Hernandez had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

144. **Plaintiff Joseph Jackson** is an adult individual and a natural person, citizen of California, where he resides and intends to stay.

145. In or around 2015, Plaintiff Jackson downloaded and used the SiriusXM app on his mobile phone. In addition, in or about 2020, Plaintiff Jackson downloaded and used the Life360 app. Plaintiff Jackson downloaded the apps for personal use. Plaintiff Jackson reviewed the prominent information about the nature and function of the apps presented to Plaintiff Jackson prior to downloading and using the apps. Plaintiff Jackson was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

146. Plaintiff Jackson is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Jackson's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

147. Plaintiff Jackson was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Jackson's driving behavior, without Plaintiff Jackson's knowledge or consent.

148. In or around 2014, Plaintiff Jackson purchased insurance from Allstate, or one of its subsidiaries. Plaintiff Jackson is an Allstate insurance subscriber, and has been continuously from his initial purchase.

149. Upon information and belief, insurance premiums paid by Plaintiff Jackson was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Jackson rode as a passenger numerous times while carrying Plaintiff Jackson's mobile phone, and any assumption that the movement of Plaintiff Jackson's phone during those trips reflected Plaintiff Jackson's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Jackson paid more for insurance than he otherwise would have.

150. Defendants' interception, collection, and monetization of Plaintiff Jackson's highly sensitive Personal Data without consent caused Plaintiff Jackson harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Jackson's expense.

151. Because of Defendants' conduct, Plaintiff Jackson has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

152. Defendants' secret collection of Plaintiff Jackson's Personal Data deprived Plaintiff Jackson of control over valuable personal information. Plaintiff Jackson's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Jackson did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Jackson's Personal Data for Defendants' financial benefit. Plaintiff Jackson's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Jackson's knowledge, compensation, or control. Plaintiff Jackson would have expected compensation in exchange for providing Plaintiff Jackson's Personal Data to third parties looking to use it for their own benefit.

153. Plaintiff Jackson had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

154. **Plaintiff Kimberly Kelley** is an adult individual and a natural person, citizen of Georgia, where she resides and intends to stay.

155. In or around 2024, Plaintiff Kelley downloaded and used the GasBuddy, Life360, and Routely apps on her mobile phone. Plaintiff Kelley downloaded the apps for personal use.

Plaintiff Kelley reviewed the prominent information about the nature and function of the apps presented to Plaintiff prior to downloading and using the apps. Plaintiff Kelley was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

156. Plaintiff Kelley is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Kelley's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

157. Plaintiff Kelley was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Kelley's driving behavior, without Plaintiff Kelley's knowledge or consent.

158. Upon information and belief, insurance premiums paid by Plaintiff Kelley was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Kelley rode as a passenger numerous times while carrying Plaintiff Kelley's mobile phone, and any assumption that the movement of Plaintiff Kelley's phone during those trips reflected Plaintiff Kelley's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Kelley paid more for insurance than she otherwise would have.

159. Defendants' interception, collection, and monetization of Plaintiff Kelley's highly sensitive Personal Data without consent caused Plaintiff Kelley harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Kelley's expense.

160. Because of Defendants' conduct, Plaintiff Kelley has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

161. Defendants' secret collection of Plaintiff Kelley's Personal Data deprived Plaintiff of control over valuable personal information. Plaintiff Kelley's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Kelley did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Kelley's Personal Data for Defendants' financial benefit. Plaintiff Kelley's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Kelley's

knowledge, compensation, or control. Plaintiff Kelley would have expected compensation in exchange for providing Plaintiff Kelley's Personal Data to third parties looking to use it for their own benefit.

162. Plaintiff Kelley had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

163. **Plaintiff Daniel Kilgo** is an adult individual and a natural person, citizen of Alabama, where he resides and intends to stay.

164. In or around 2021, Plaintiff Kilgo downloaded and used the Life360 app on his mobile phone. Plaintiff downloaded the app for personal use. Plaintiff Kilgo reviewed the prominent information about the nature and function of the app presented to Plaintiff Kilgo prior to downloading and using the app. Plaintiff Kilgo was not provided meaningful notice that Defendants would use the app to collect and share his Personal Data.

165. Plaintiff Kilgo is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Kilgo's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

166. Plaintiff Kilgo was unaware that Allstate and Arity's SDK had been integrated into the app at the time he installed, and later when he used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Kilgo's driving behavior, without Plaintiff Kilgo's knowledge or consent.

167. Upon information and belief, insurance premiums paid by Plaintiff Kilgo was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Kilgo rode as a passenger numerous times while carrying Plaintiff Kilgo's mobile phone, and any assumption that the movement of Plaintiff Kilgo's phone during those trips reflected Plaintiff Kilgo's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Kilgo paid more for insurance than he otherwise would have.

168. Defendants' interception, collection, and monetization of Plaintiff Kilgo's highly sensitive Personal Data without consent caused Plaintiff Kilgo harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Kilgo's expense.

169. Because of Defendants' conduct, Plaintiff Kilgo has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

170. Defendants' secret collection of Plaintiff Kilgo's Personal Data deprived Plaintiff Kilgo of control over valuable personal information. Plaintiff Kilgo's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Kilgo did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Kilgo's Personal Data for Defendants' financial benefit. Plaintiff Kilgo's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Kilgo's knowledge, compensation, or control. Plaintiff Kilgo would have expected compensation in exchange for providing Plaintiff Kilgo's Personal Data to third parties looking to use it for their own benefit.

171. Plaintiff Kilgo had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

172. **Plaintiff Michael Mahoney** is an adult individual and a natural person, citizen of California, where he resides and intends to stay.

173. In or around 2011, Plaintiff Mahoney downloaded and used GasBuddy on his mobile phone. In addition, in or around 2015, Plaintiff Mahoney downloaded and used the SiriusXM app. Plaintiff Mahoney downloaded the apps for personal use. Plaintiff Mahoney reviewed the prominent information about the nature and function of the apps presented to Plaintiff Mahoney prior to downloading and using the apps. Plaintiff Mahoney was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

174. Plaintiff Mahoney is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Mahoney's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

175. Plaintiff Mahoney was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Mahoney's driving behavior, without Plaintiff Mahoney's knowledge or consent.

176. Upon information and belief, insurance premiums paid by Plaintiff Mahoney was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Mahoney rode as a passenger numerous times while carrying Plaintiff Mahoney's mobile phone, and any assumption that the movement of Plaintiff Mahoney's phone during those trips reflected Plaintiff Mahoney's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be

inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Mahoney paid more for insurance than he otherwise would have.

177. Defendants' interception, collection, and monetization of Plaintiff Mahoney's highly sensitive Personal Data without consent caused Plaintiff Mahoney harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Mahoney's expense.

178. Because of Defendants' conduct, Plaintiff Mahoney has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

179. Defendants' secret collection of Plaintiff Mahoney's Personal Data deprived Plaintiff Mahoney of control over valuable personal information. Plaintiff Mahoney's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Mahoney did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Mahoney's Personal Data for Defendants' financial benefit. Plaintiff Mahoney's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Mahoney's knowledge, compensation, or control. Plaintiff Mahoney would have expected compensation in exchange for providing Plaintiff Mahoney's Personal Data to third parties looking to use it for their own benefit.

180. Plaintiff Mahoney had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

181. **Plaintiff Sofia Malvar** is an adult individual and a natural person, citizen of California, where she resides and intends to stay.

182. In or around 2010, Plaintiff Malvar downloaded and used the GasBuddy app on her mobile phone. In addition, in or around 2014, Plaintiff Malvar also downloaded and used the Fuel Rewards app, and in or around 2020, she downloaded and used the SiriusXM app. Plaintiff Malvar downloaded the apps for personal use. Plaintiff Malvar reviewed the prominent information about the nature and function of the apps presented to Plaintiff Malvar prior to downloading and using the apps. Plaintiff Malvar was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

183. Plaintiff Malvar is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Malvar's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

184. Plaintiff Malvar was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data

listed above, including but not limited to data related to Plaintiff Malvar's driving behavior, without Plaintiff Malvar's knowledge or consent.

185. Upon information and belief, insurance premiums paid by Plaintiff Malvar was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Malvar rode as a passenger numerous times while carrying Plaintiff Malvar's mobile phone, and any assumption that the movement of Plaintiff Malvar's phone during those trips reflected Plaintiff Malvar's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Malvar paid more for insurance than she otherwise would have.

186. Defendants' interception, collection, and monetization of Plaintiff Malvar's highly sensitive Personal Data without consent caused Plaintiff Malvar harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Malvar's expense.

187. Because of Defendants' conduct, Plaintiff Malvar has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

188. Defendants' secret collection of Plaintiff Malvar's Personal Data deprived Plaintiff Malvar of control over valuable personal information. Plaintiff Malvar's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Malvar did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Malvar's Personal Data for Defendants'

financial benefit. Plaintiff Malvar's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Malvar's knowledge, compensation, or control. Plaintiff Malvar would have expected compensation in exchange for providing Plaintiff Malvar's Personal Data to third parties looking to use it for their own benefit.

189. Plaintiff Malvar had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

190. **Plaintiff James McNeill** is an adult individual and a natural person, citizen of Louisiana, where he resides and intends to stay.

191. In or around 2022, Plaintiff McNeill downloaded and used the GasBuddy and Life360 apps on his mobile phone. Plaintiff McNeill downloaded the apps for personal use. Plaintiff McNeill reviewed the prominent information about the nature and function of the apps presented to Plaintiff McNeill prior to downloading and using the apps. Plaintiff McNeill was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

192. Plaintiff McNeill is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff McNeill's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

193. Plaintiff McNeill was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff McNeill's driving behavior, without Plaintiff McNeill's knowledge or consent.

194. In or around 2022, Plaintiff McNeill purchased insurance from Allstate, or one of its subsidiaries. Plaintiff McNeill is an Allstate insurance subscriber, and has been continuously from his initial purchase.

195. Upon information and belief, insurance premiums paid by Plaintiff McNeill was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff McNeill rode as a passenger numerous times while carrying Plaintiff McNeill's mobile phone, and any assumption that the movement of Plaintiff McNeill's phone during those trips reflected Plaintiff McNeill's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff McNeill paid more for insurance than he otherwise would have.

196. Defendants' interception, collection, and monetization of Plaintiff McNeill's highly sensitive Personal Data without consent caused Plaintiff McNeill harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff McNeill's expense.

197. Because of Defendants' conduct, Plaintiff McNeill has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

198. Defendants' secret collection of Plaintiff's McNeill Personal Data deprived Plaintiff McNeill of control over valuable personal information. Plaintiff McNeill's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff McNeill did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff McNeill's Personal Data for Defendants' financial benefit. Plaintiff McNeill's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff McNeill's knowledge, compensation, or control. Plaintiff McNeill would have expected compensation in exchange for providing Plaintiff McNeill's Personal Data to third parties looking to use it for their own benefit.

199. Plaintiff McNeill had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

200. **Plaintiff Jennifer Monilaw** is an adult individual and a natural person, citizen of Illinois, where she resides and intends to stay.

201. In or around 2022, Plaintiff Monilaw downloaded and used the Fuel Rewards and Life360 apps on her mobile phone. In addition, in or around 2024, Plaintiff Monilaw downloaded

and used the GasBuddy app. Plaintiff Monilaw downloaded the apps for personal use. Plaintiff Monilaw reviewed the prominent information about the nature and function of the apps presented to Plaintiff Monilaw prior to downloading and using the apps. Plaintiff Monilaw was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

202. Plaintiff Monilaw is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Monilaw's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

203. Plaintiff Monilaw was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Monilaw's driving behavior, without Plaintiff Monilaw's knowledge or consent.

204. Upon information and belief, insurance premiums paid by Plaintiff Monilaw was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Monilaw rode as a passenger numerous times while carrying Plaintiff Monilaw's mobile phone, and any assumption that the movement of Plaintiff Monilaw's phone during those trips reflected Plaintiff Monilaw's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Monilaw paid more for insurance than she otherwise would have.

205. Defendants' interception, collection, and monetization of Plaintiff Monilaw's highly sensitive Personal Data without consent caused Plaintiff Monilaw harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Monilaw's expense.

206. Because of Defendants' conduct, Plaintiff Monilaw has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

207. Defendants' secret collection of Plaintiff Monilaw's Personal Data deprived Plaintiff Monilaw of control over valuable personal information. Plaintiff Monilaw's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Monilaw did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Monilaw's Personal Data for Defendants' financial benefit. Plaintiff Monilaw's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using

that data without Plaintiff Monilaw's knowledge, compensation, or control. Plaintiff Monilaw would have expected compensation in exchange for providing Plaintiff Monilaw's Personal Data to third parties looking to use it for their own benefit.

208. Plaintiff Monilaw had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use

209. **Plaintiff Amanda Quam** is an adult individual and a natural person, citizen of Illinois, where she resides and intends to stay.

210. In or around 2023, Plaintiff Quam downloaded and used the GasBuddy, Fuel Rewards, Routely apps on her mobile phone. In addition, Plaintiff Quam downloaded the Life360 app. Plaintiff Quam downloaded the apps for personal use. Plaintiff Quam reviewed the prominent information about the nature and function of the apps presented to Plaintiff Quam prior to downloading and using GasBuddy, Fuel Rewards, and Routely. Plaintiff Quam was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

211. Plaintiff Quam is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Quam's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

212. Plaintiff Quam was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used GasBuddy, Fuel Rewards, and Routely. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Quam's driving behavior, without Plaintiff Quam's knowledge or consent.

213. Upon information and belief, insurance premiums paid by Plaintiff Quam was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Quam rode as a passenger numerous times while carrying Plaintiff Quam's mobile phone, and any assumption that the movement of Plaintiff Quam's phone during those trips reflected Plaintiff Quam's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Quam paid more for insurance than she otherwise would have.

214. Defendants' interception, collection, and monetization of Plaintiff Quam's highly sensitive Personal Data without consent caused Plaintiff Quam harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Quam's expense.

215. Because of Defendants' conduct, Plaintiff Quam has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

216. Defendants' secret collection of Plaintiff Quam's Personal Data deprived Plaintiff Quam of control over valuable personal information. Plaintiff Quam's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Quam did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Quam's Personal Data for Defendants' financial benefit. Plaintiff Quam's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Quam's knowledge, compensation, or control. Plaintiff Quam would have expected compensation in exchange for providing Plaintiff Quam's Personal Data to third parties looking to use it for their own benefit.

217. Plaintiff Quam had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

218. **Plaintiff Annette Rastrelli** is an adult individual and a natural person, citizen of Texas, where she resides and intends to stay.

219. More than two years ago, Plaintiff Rastrelli downloaded and used the Gas Buddy and Life360 apps on her mobile phone. Plaintiff Rastrelli downloaded the apps for personal use. Plaintiff Rastrelli reviewed the prominent information about the nature and function of the apps presented to Plaintiff Rastrelli prior to downloading and using the apps. Plaintiff Rastrelli was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

220. Plaintiff Rastrelli is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Rastrelli's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

221. Plaintiff Rastrelli was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Rastrelli's driving behavior, without Plaintiff Rastrelli's knowledge or consent.

222. Upon information and belief, insurance premiums paid by Plaintiff Rastrelli was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Rastrelli rode as a passenger numerous times while carrying Plaintiff Rastrelli's mobile phone, and any assumption that the movement of Plaintiff Rastrelli's phone during those trips reflected Plaintiff Rastrelli's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated.

Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Rastrelli paid more for insurance than she otherwise would have.

223. Defendants' interception, collection, and monetization of Plaintiff Rastrelli's highly sensitive Personal Data without consent caused Plaintiff Rastrelli harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Rastrelli's expense.

224. Because of Defendants' conduct, Plaintiff Rastrelli has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

225. Defendants' secret collection of Plaintiff Rastrelli's Personal Data deprived Plaintiff Rastrelli of control over valuable personal information. Plaintiff Rastrelli's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Rastrelli did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Rastrelli's Personal Data for Defendants' financial benefit. Plaintiff Rastrelli's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Rastrelli's knowledge, compensation, or control. Plaintiff Rastrelli would have expected compensation in exchange for providing Plaintiff Rastrelli's Personal Data to third parties looking to use it for their own benefit.

226. Plaintiff Rastrelli had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

227. **Plaintiff Nicole Rehfuss** is an adult individual and a natural person, citizen of Kentucky, where she resides and intends to stay.

228. In or around 2020, Plaintiff Rehfuss downloaded and used the SiriusXM app on her mobile phone. Plaintiff Rehfuss downloaded the app for personal use. Plaintiff Rehfuss reviewed the prominent information about the nature and function of the app presented to Plaintiff Rehfuss prior to downloading and using the app. Plaintiff Rehfuss was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

229. Plaintiff Rehfuss is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Rehfuss's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

230. Plaintiff Rehfuss was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Rehfuss' driving behavior, without Plaintiff Rehfuss' knowledge or consent.

231. Upon information and belief, insurance premiums paid by Plaintiff Rehfuss was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Rehfuss rode as a passenger numerous times while carrying Plaintiff Rehfuss' mobile phone, and any assumption that the movement of Plaintiff Rehfuss' phone during those trips reflected Plaintiff Rehfuss' driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Rehfuss paid more for insurance than she otherwise would have.

232. Defendants' interception, collection, and monetization of Plaintiff Rehfuss' highly sensitive Personal Data without consent caused Plaintiff Rehfuss harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Rehfuss' expense.

233. Because of Defendants' conduct, Plaintiff Rehfuss has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

234. Defendants' secret collection of Plaintiff Rehfuss' Personal Data deprived Plaintiff Rehfuss of control over valuable personal information. Plaintiff Rehfuss' Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Rehfuss did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Rehfuss' Personal Data for Defendants' financial benefit. Plaintiff Rehfuss' Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data

without Plaintiff Rehfuss' knowledge, compensation, or control. Plaintiff Rehfuss would have expected compensation in exchange for providing Plaintiff Rehfuss' Personal Data to third parties looking to use it for their own benefit.

235. Plaintiff Rehfuss had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

236. **Plaintiff Dorian Rochester** is an adult individual and a natural person, citizen of Pennsylvania, where he resides and intends to stay.

237. In or around 2023, Plaintiff Rochester downloaded and used the Life360 and Routely apps on his mobile phone. Plaintiff Rochester downloaded the apps for personal use. Plaintiff Rochester reviewed the prominent information about the nature and function of the apps presented to Plaintiff Rochester prior to downloading and using the apps. Plaintiff Rochester was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

238. Plaintiff Rochester is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Rochester's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

239. Plaintiff Rochester was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Rochester's driving behavior, without Plaintiff Rochester's knowledge or consent.

240. Upon information and belief, insurance premiums paid by Plaintiff Rochester was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Rochester rode as a passenger numerous times while carrying Plaintiff Rochester's mobile phone, and any assumption that the movement of Plaintiff Rochester's phone during those trips reflected Plaintiff Rochester's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendants' covert collection and use of his Personal Data, Plaintiff Rochester paid more for insurance than he otherwise would have.

241. Defendants' interception, collection, and monetization of Plaintiff Rochester's highly sensitive Personal Data without consent caused Plaintiff Rochester harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Rochester's expense.

242. Because of Defendants' conduct, Plaintiff Rochester has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

243. Defendants' secret collection of Plaintiff Rochester's Personal Data deprived Plaintiff Rochester of control over valuable personal information. Plaintiff Rochester's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Rochester did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff's Personal Data for Defendants' financial benefit. Plaintiff Rochester's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Rochester's knowledge, compensation, or control. Plaintiff Rochester would have expected compensation in exchange for providing Plaintiff Rochester's Personal Data to third parties looking to use it for their own benefit.

244. Plaintiff Rochester had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

245. **Plaintiff Robert Sanginito** is an adult individual and a natural person, citizen of New Jersey, where he resides and intends to stay.

246. In or around 2016, Plaintiff Sanginito downloaded and used the SiriusXM app on his mobile phone. In addition, in or around 2020, Plaintiff Sanginito downloaded and used the Life360 app, and in or around 2021, he downloaded and used the GasBuddy app. Plaintiff Sanginito downloaded the apps for personal use. Plaintiff Sanginito reviewed the prominent information about the nature and function of the apps presented to Plaintiff Sanginito prior to downloading and using the apps. Plaintiff Sanginito was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

247. Plaintiff Sanginito is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Sanginito's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

248. Plaintiff Sanginito was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Sanginito's driving behavior, without Plaintiff Sanginito's knowledge or consent.

249. Upon information and belief, insurance premiums paid by Plaintiff Sanginito was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Sanginito rode as a passenger numerous times while carrying Plaintiff Sanginito's mobile phone, and any assumption that the

movement of Plaintiff Sanginito's phone during those trips reflected Plaintiff Sanginito's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Sanginito paid more for insurance than he otherwise would have.

250. Defendants' interception, collection, and monetization of Plaintiff Sanginito's highly sensitive Personal Data without consent caused Plaintiff Sanginito harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Sanginito's expense.

251. Because of Defendants' conduct, Plaintiff Sanginito has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

252. Defendants' secret collection of Plaintiff Sanginito's Personal Data deprived Plaintiff Sanginito of control over valuable personal information. Plaintiff Sanginito's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Sanginito did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Sanginito's Personal Data for Defendants' financial benefit. Plaintiff Sanginito's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Sanginito's knowledge, compensation, or control. Plaintiff Sanginito would have expected compensation in exchange for providing Plaintiff Sanginito's Personal Data to third parties looking to use it for their own benefit.

253. Plaintiff Sanginito had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

254. **Plaintiff Scott Schultz** is an adult individual and a natural person, citizen of Illinois, where he resides and intends to stay.

255. In or around 2021, Plaintiff Schultz downloaded and used the GasBuddy and Life360 apps on his mobile phone. Plaintiff Schultz downloaded the apps for personal use. Plaintiff Schultz reviewed the prominent information about the nature and function of the apps presented to Plaintiff Schultz prior to downloading and using the apps. Plaintiff Schultz was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

256. Plaintiff Schultz is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Schultz's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

257. Plaintiff Schultz was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data

listed above, including but not limited to data related to Plaintiff Schultz's driving behavior, without Plaintiff Schultz's knowledge or consent.

258. In or around 2024, Plaintiff Schultz purchased insurance from National General, an Allstate subsidiary. Plaintiff Schultz is a National General insurance subscriber, and has been continuously from his initial purchase.

259. Upon information and belief, insurance premiums paid by Plaintiff Schultz was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Schultz rode as a passenger numerous times while carrying Plaintiff Schultz's mobile phone, and any assumption that the movement of Plaintiff Schultz's phone during those trips reflected Plaintiff Schultz's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Schultz paid more for insurance than he otherwise would have.

260. Defendants' interception, collection, and monetization of Plaintiff Schultz's highly sensitive Personal Data without consent caused Plaintiff Schultz harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Schultz's expense.

261. Because of Defendants' conduct, Plaintiff Schultz has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

262. Defendants' secret collection of Plaintiff Schultz's Personal Data deprived Plaintiff Schultz of control over valuable personal information. Plaintiff Schultz's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing

access to such data to insurers, marketers, and other third parties. Plaintiff Schultz did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Schultz's Personal Data for Defendants' financial benefit. Plaintiff Schultz's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Schultz's knowledge, compensation, or control. Plaintiff Schultz would have expected compensation in exchange for providing Plaintiff Schultz's Personal Data to third parties looking to use it for their own benefit.

263. Plaintiff Schultz had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

264. **Plaintiff Chrystie Seay** is an adult individual and a natural person, citizen of South Carolina, where she resides and intends to stay.

265. In or around 2020, Plaintiff Seay downloaded and used the GasBuddy and Life360 apps on her mobile phone. Plaintiff Seay downloaded the apps for personal use. Plaintiff Seay reviewed the prominent information about the nature and function of the apps presented to Plaintiff Seay prior to downloading and using the apps. Plaintiff Seay was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

266. Plaintiff Seay is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Seay's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

267. Plaintiff Seay was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Seay's driving behavior, without Plaintiff Seay's knowledge or consent.

268. In or around 2020, Plaintiff Seay purchased insurance from Allstate, or one of its subsidiaries. Plaintiff Seay is an Allstate insurance subscriber, and has been continuously from her initial purchase.

269. Upon information and belief, insurance premiums paid by Plaintiff Seay was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Seay rode as a passenger numerous times while carrying Plaintiff Seay's mobile phone, and any assumption that the movement of Plaintiff Seay's phone during those trips reflected Plaintiff Seay's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated.

Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Seay paid more for insurance than she otherwise would have.

270. Defendants' interception, collection, and monetization of Plaintiff Seay's highly sensitive Personal Data without consent caused Plaintiff Seay harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Seay's expense.

271. Because of Defendants' conduct, Plaintiff Seay has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

272. Defendants' secret collection of Plaintiff Seay's Personal Data deprived Plaintiff Seay of control over valuable personal information. Plaintiff Seay's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Seay did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Seay's Personal Data for Defendants' financial benefit. Plaintiff Seay's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Seay's knowledge, compensation, or control. Plaintiff Seay would have expected compensation in exchange for providing Plaintiff Seay's Personal Data to third parties looking to use it for their own benefit.

273. Plaintiff Seay had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

274. **Plaintiff Ashika Singh** is an adult individual and a natural person, citizen of North Carolina, where she resides and intends to stay.

275. In or around 2013, Plaintiff Singh downloaded and used the Life 360 app on her mobile phone. In addition, in or around 2020, Plaintiff Singh downloaded and used the Gas Buddy and Sirius XM apps. Plaintiff Singh downloaded the apps for personal use. Plaintiff Singh reviewed the prominent information about the nature and function of the apps presented to Plaintiff Singh prior to downloading and using the apps. Plaintiff Singh was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

276. Plaintiff Singh is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Singh's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

277. Plaintiff Singh was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data

listed above, including but not limited to data related to Plaintiff Singh's driving behavior, without Plaintiff Singh's knowledge or consent.

278. In or around 2010, Plaintiff Singh purchased insurance from Allstate and remained a customer until 2022. In or around 2022, Plaintiff Singh purchased insurance from National General, an Allstate subsidiary. Plaintiff Singh is a National General insurance subscriber, and has been continuously from her initial purchase.

279. Upon information and belief, insurance premiums paid by Plaintiff Singh was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Singh rode as a passenger numerous times while carrying Plaintiff Singh's mobile phone, and any assumption that the movement of Plaintiff Singh's phone during those trips reflected Plaintiff Singh's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Singh paid more for insurance than she otherwise would have.

280. Defendants' interception, collection, and monetization of Plaintiff Singh's highly sensitive Personal Data without consent caused Plaintiff Singh harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Singh's expense.

281. Because of Defendants' conduct, Plaintiff Singh has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

282. Defendants' secret collection of Plaintiff Singh's Personal Data deprived Plaintiff Singh of control over valuable personal information. Plaintiff Singh's Personal Data has intrinsic

and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Singh did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Singh's Personal Data for Defendants' financial benefit. Plaintiff Singh's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Singh's knowledge, compensation, or control. Plaintiff Singh would have expected compensation in exchange for providing Plaintiff Singh's Personal Data to third parties looking to use it for their own benefit.

283. Plaintiff Singh had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

284. **Plaintiff Antonette Slater** is an adult individual and a natural person, citizen of Illinois, where she resides and intends to stay.

285. In or around 2020, Plaintiff Slater downloaded and used Life360 on her mobile phone. As well, in or around 2015, Fuel Rewards (collectively with Life360, the "Apps"). Plaintiff Slater downloaded the Apps for personal use. Plaintiff Slater reviewed the prominent information about the nature and function of the Apps presented to Plaintiff Slater prior to downloading and using the Apps. Plaintiff Slater was not provided meaningful notice that Defendants would use the Apps to collect and share her Personal Data.

286. Plaintiff Slater is informed and believes that the Apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Slater's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

287. Plaintiff Slater was unaware that Allstate and Arity's SDK had been integrated into the Apps at the time she installed, and later when she used the Apps. Through the Apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Slater's driving behavior, without Plaintiff Slater's knowledge or consent.

288. In or around 2006, Plaintiff Slater purchased insurance from Allstate, or one of its subsidiaries. Plaintiff Slater is an Allstate insurance subscriber, and has been continuously from her initial purchase.

289. Upon information and belief, insurance premiums paid by Plaintiff Slater was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Slater rode as a passenger numerous times while carrying Plaintiff Slater's mobile phone, and any assumption that the movement of Plaintiff Slater's phone during those trips reflected Plaintiff Slater's driving was inaccurate.

Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Slater paid more for insurance than she otherwise would have.

290. Defendants' interception, collection, and monetization of Plaintiff Slater's highly sensitive Personal Data without consent caused Plaintiff Slater harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Slater's expense.

291. Because of Defendants' conduct, Plaintiff Slater has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

292. Defendants' secret collection of Plaintiff Slater's Personal Data deprived Plaintiff Slater of control over valuable personal information. Plaintiff Slater's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Slater did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Slater's Personal Data for Defendants' financial benefit. Plaintiff Slater's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Slater's knowledge, compensation, or control. Plaintiff Slater would have expected compensation in exchange for providing Plaintiff Slater's Personal Data to third parties looking to use it for their own benefit.

293. Plaintiff Slater had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

294. **Plaintiff Kayla Smith** is an adult individual and a natural person, citizen of Indiana, where she resides and intends to stay.

295. In or around 2024, Plaintiff Smith downloaded and used the GasBuddy app on her mobile phone. Plaintiff Smith downloaded the app for personal use. Plaintiff Smith reviewed the prominent information about the nature and function of the app presented to Plaintiff Smith prior to downloading and using the app. Plaintiff Smith was not provided meaningful notice that Defendants would use the app to collect and share her Personal Data.

296. Plaintiff Smith is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Smith's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

297. Plaintiff Smith was unaware that Allstate and Arity's SDK had been integrated into the app at the time she installed, and later when she used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Smith's driving behavior, without Plaintiff Smith's knowledge or consent.

298. In or around 2023, Plaintiff Smith purchased insurance from Esurance, an Allstate subsidiary. Plaintiff Smith is an Esurance insurance subscriber, and has been continuously from her initial purchase.

299. Upon information and belief, insurance premiums paid by Plaintiff Smith was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Smith rode as a passenger numerous times while carrying Plaintiff Smith's mobile phone, and any assumption that the movement of Plaintiff Smith's phone during those trips reflected Plaintiff Smith's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Smith paid more for insurance than she otherwise would have.

300. Defendants' interception, collection, and monetization of Plaintiff Smith's highly sensitive Personal Data without consent caused Plaintiff Smith harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Smith's expense.

301. Because of Defendants' conduct, Plaintiff Smith has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

302. Defendants' secret collection of Plaintiff Smith's Personal Data deprived Plaintiff Smith of control over valuable personal information. Plaintiff Smith's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Smith did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the

unauthorized exploitation of Plaintiff Smith's Personal Data for Defendants' financial benefit. Plaintiff Smith's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Smith's knowledge, compensation, or control. Plaintiff Smith would have expected compensation in exchange for providing Plaintiff Smith's Personal Data to third parties looking to use it for their own benefit.

303. Plaintiff Smith had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

304. **Plaintiff Robert Smith** is an adult individual and a natural person, citizen of Ohio, where he resides and intends to stay.

305. In or around 2021, Plaintiff Smith downloaded and used the GasBuddy and Fuel Rewards apps on his mobile phone. Plaintiff Smith downloaded the apps for personal use. Plaintiff Smith reviewed the prominent information about the nature and function of the apps presented to Plaintiff Smith prior to downloading and using the apps. Plaintiff Smith was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

306. Plaintiff Smith is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Smith's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

307. Plaintiff Smith was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Smith's driving behavior, without Plaintiff's knowledge or consent.

308. Upon information and belief, insurance premiums paid by Plaintiff Smith was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Smith rode as a passenger numerous times while carrying Plaintiff Smith's mobile phone, and any assumption that the movement of Plaintiff Smith's phone during those trips reflected Plaintiff Smith's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Smith paid more for insurance than he otherwise would have.

309. Defendants' interception, collection, and monetization of Plaintiff Smith's highly sensitive Personal Data without consent caused Plaintiff Smith harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Smith's expense.

310. Because of Defendants' conduct, Plaintiff Smith has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

311. Defendants' secret collection of Plaintiff Smith's Personal Data deprived Plaintiff Smith of control over valuable personal information. Plaintiff Smith's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Smith did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Smith's Personal Data for Defendants' financial benefit. Plaintiff Smith's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Smith's knowledge, compensation, or control. Plaintiff Smith would have expected compensation in exchange for providing Plaintiff Smith's Personal Data to third parties looking to use it for their own benefit.

312. Plaintiff Smith had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

313. **Plaintiff Rita Streifel** is an adult individual and a natural person, citizen of California, where she resides and intends to stay.

314. In or around 2020, Plaintiff Streifel downloaded and used the GasBuddy and Fuel Rewards apps on her mobile phone. Plaintiff Streifel downloaded the apps for personal use. Plaintiff Streifel reviewed the prominent information about the nature and function of the apps presented to Plaintiff Streifel prior to downloading and using the apps. Plaintiff Streifel was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

315. Plaintiff Streifel is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Streifel's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

316. Plaintiff Streifel was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Streifel's driving behavior, without Plaintiff Streifel's knowledge or consent.

317. Upon information and belief, insurance premiums paid by Plaintiff Streifel was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Streifel rode as a passenger numerous times while carrying Plaintiff Streifel's mobile phone, and any assumption that the movement of

Plaintiff's phone during those trips reflected Plaintiff Streifel's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Streifel paid more for insurance than she otherwise would have.

318. Defendants' interception, collection, and monetization of Plaintiff Streifel's highly sensitive Personal Data without consent caused Plaintiff Streifel harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Streifel's expense.

319. Because of Defendants' conduct, Plaintiff Streifel has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

320. Defendants' secret collection of Plaintiff Streifel's Personal Data deprived Plaintiff Streifel of control over valuable personal information. Plaintiff Streifel's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Streifel did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff's Personal Data for Defendants' financial benefit. Plaintiff Streifel's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Streifel's knowledge, compensation, or control. Plaintiff Streifel would have expected compensation in exchange for providing Plaintiff Streifel's Personal Data to third parties looking to use it for their own benefit.

321. Plaintiff Streifel had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

322. **Plaintiff Kimberly Summersill** is an adult individual and a natural person, citizen of Texas, where she resides and intends to stay.

323. In or around 2017, Plaintiff Summersill downloaded and used Life360 ("Apps") on her mobile phone. Plaintiff Summersill downloaded the Apps for personal use. Plaintiff Summersill reviewed the prominent information about the nature and function of the Apps presented to Plaintiff Summersill prior to downloading and using the Apps. Plaintiff Summersill was not provided meaningful notice that Defendants would use the Apps to collect and share her Personal Data.

324. Plaintiff Summersill is informed and believes that the Apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Summersill's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

325. Plaintiff Summersill was unaware that Allstate and Arity's SDK had been integrated into the Apps at the time she installed, and later when she used the Apps. Through the Apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Summersill's driving behavior, without Plaintiff Summersill's knowledge or consent.

326. Upon information and belief, insurance premiums paid by Plaintiff Summersill was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Summersill rode as a passenger numerous times while carrying Plaintiff Summersill's mobile phone, and any assumption that the movement of Plaintiff Summersill's phone during those trips reflected Plaintiff Summersill's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Summersill paid more for insurance than she otherwise would have.

327. Defendants' interception, collection, and monetization of Plaintiff Summersill's highly sensitive Personal Data without consent caused Plaintiff Summersill harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Summersill's expense.

328. Because of Defendants' conduct, Plaintiff Summersill has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

329. Defendants' secret collection of Plaintiff Summersill's Personal Data deprived Plaintiff Summersill of control over valuable personal information. Plaintiff Summersill's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling

or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Summersill did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Summersill's Personal Data for Defendants' financial benefit. Plaintiff Summersill's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Summersill's knowledge, compensation, or control. Plaintiff Summersill would have expected compensation in exchange for providing Plaintiff Summersill's Personal Data to third parties looking to use it for their own benefit.

330. Plaintiff Summersill had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

331. **Plaintiff Valencia Tucker** is an adult individual and a natural person, citizen of Illinois, where he resides and intends to stay.

332. In or around 2019, Plaintiff Tucker downloaded and used the Fuel Rewards app on his mobile phone. In addition, prior to 2019, Plaintiff Tucker downloaded and used the SiriusXM app. Plaintiff Tucker downloaded the apps for personal use. Plaintiff Tucker reviewed the prominent information about the nature and function of the apps presented to Plaintiff Tucker prior to downloading and using the apps. Plaintiff Tucker was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

333. Plaintiff Tucker is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Tucker's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

334. Plaintiff Tucker was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Tucker's driving behavior, without Plaintiff Tucker's knowledge or consent.

335. Upon information and belief, insurance premiums paid by Plaintiff Tucker was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Tucker rode as a passenger numerous times while carrying Plaintiff Tucker's mobile phone, and any assumption that the movement of Plaintiff Tucker's phone during those trips reflected Plaintiff Tucker's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Tucker paid more for insurance than he otherwise would have.

336. Defendants' interception, collection, and monetization of Plaintiff Tucker's highly sensitive Personal Data without consent caused Plaintiff Tucker harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Tucker's expense.

337. Because of Defendants' conduct, Plaintiff Tucker has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

338. Defendants' secret collection of Plaintiff Tucker's Personal Data deprived Plaintiff Tucker of control over valuable personal information. Plaintiff Tucker's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Tucker did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Tucker's Personal Data for Defendants' financial benefit. Plaintiff Tucker's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Tucker's knowledge, compensation, or control. Plaintiff Tucker would have expected compensation in exchange for providing Plaintiff Tucker's Personal Data to third parties looking to use it for their own benefit.

339. Plaintiff Tucker had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

340. **Plaintiff Tracy Tupper** is an adult individual and a natural person, citizen of New York, where he resides and intends to stay.

341. In or around 2019, Plaintiff Tupper downloaded and used the Drivewise app on his mobile phone. Plaintiff Tupper downloaded the app for personal use. Plaintiff Tupper reviewed

the prominent information about the nature and function of the app presented to Plaintiff Tupper prior to downloading and using the app. Plaintiff Tupper was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

342. Plaintiff Tupper is informed and believes that the app integrates an SDK provided by Defendants, which harvests several types of data from Plaintiff Tupper's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

343. Plaintiff Tupper was unaware that Allstate and Arity's SDK had been integrated into the app at the time he installed, and later when he used the app. Through the app, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Tupper's driving behavior, without Plaintiff Tupper's knowledge or consent.

344. In or around 2019, Plaintiff Tupper purchased insurance from Allstate, or one of its subsidiaries. Plaintiff Tupper is an Allstate insurance subscriber, and has been continuously from his initial purchase.

345. Upon information and belief, insurance premiums paid by Plaintiff Tupper was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Tupper rode as a passenger numerous times while carrying Plaintiff Tupper's mobile phone, and any assumption that the movement of Plaintiff Tupper's phone during those trips reflected Plaintiff Tupper's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Tupper paid more for insurance than he otherwise would have.

346. Defendants' interception, collection, and monetization of Plaintiff Tupper's highly sensitive Personal Data without consent caused Plaintiff Tupper harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Tupper's expense.

347. Because of Defendants' conduct, Plaintiff Tupper has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

348. Defendants' secret collection of Plaintiff Tupper's Personal Data deprived Plaintiff Tupper of control over valuable personal information. Plaintiff Tupper's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Tupper did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct

resulted in the unauthorized exploitation of Plaintiff Tupper's Personal Data for Defendants' financial benefit. Plaintiff Tupper's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Tupper's knowledge, compensation, or control. Plaintiff Tupper would have expected compensation in exchange for providing Plaintiff Tupper's Personal Data to third parties looking to use it for their own benefit.

349. Plaintiff Tupper had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

350. **Plaintiff James Williams** is an adult individual and a natural person, citizen of Washington, where he resides and intends to stay.

351. In or around 2016, Plaintiff Williams downloaded and used the GasBuddy and SiriusXM apps on his mobile phone. In addition, in or around 2018, Plaintiff Williams downloaded and used the Life360 app. Plaintiff Williams downloaded the apps for personal use. Plaintiff Williams reviewed the prominent information about the nature and function of the apps presented to Plaintiff Williams prior to downloading and using the apps. Plaintiff Williams was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

352. Plaintiff Williams is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Williams's phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

353. Plaintiff Williams was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Williams's driving behavior, without Plaintiff Williams's knowledge or consent.

354. Upon information and belief, insurance premiums paid by Plaintiff Williams was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Williams rode as a passenger numerous times while carrying Plaintiff Williams's mobile phone, and any assumption that the movement of Plaintiff's phone during those trips reflected Plaintiff Williams's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Williams paid more for insurance than he otherwise would have.

355. Defendants' interception, collection, and monetization of Plaintiff Williams's highly sensitive Personal Data without consent caused Plaintiff Williams harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Williams's expense.

356. Because of Defendants' conduct, Plaintiff Williams has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

357. Defendants' secret collection of Plaintiff Williams' Personal Data deprived Plaintiff Williams of control over valuable personal information. Plaintiff Williams's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Williams did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Williams's Personal Data for Defendants' financial benefit. Plaintiff Williams's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Williams's knowledge, compensation, or control. Plaintiff Williams would have expected compensation in exchange for providing Plaintiff Williams's Personal Data to third parties looking to use it for their own benefit.

358. Plaintiff Williams had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

359. **Plaintiff Jacob Winkelvoss** is an adult individual and a natural person, citizen of Pennsylvania, where he resides and intends to stay.

360. In or around 2019, Plaintiff Winkelvoss downloaded and used the Life360 on his mobile phone. In addition, in or around 2021, Plaintiff Winkelvoss downloaded and used the

GasBuddy and Fuel Rewards apps, and in or around 2022, he downloaded and used the Sirius XM app. Plaintiff Winkelvoss downloaded the apps for personal use. Plaintiff Winkelvoss reviewed the prominent information about the nature and function of the apps presented to Plaintiff Winkelvoss prior to downloading and using the apps. Plaintiff Winkelvoss was not provided meaningful notice that Defendants would use the apps to collect and share his Personal Data.

361. Plaintiff Winkelvoss is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Winkelvoss' phone without his knowledge or consent, including but not limited to his:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

362. Plaintiff Winkelvoss was unaware that Allstate and Arity's SDK had been integrated into the apps at the time he installed, and later when he used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Winkelvoss' driving behavior, without Plaintiff Winkelvoss's knowledge or consent.

363. Upon information and belief, insurance premiums paid by Plaintiff Winkelvoss was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Winkelvoss rode as a passenger numerous times while carrying Plaintiff Winkelvoss's mobile phone, and any assumption that the movement of Plaintiff Winkelvoss' phone during those trips reflected Plaintiff Winkelvoss's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of his Personal Data, Plaintiff Winkelvoss paid more for insurance than he otherwise would have.

364. Defendants' interception, collection, and monetization of Plaintiff Winkelvoss's highly sensitive Personal Data without consent caused Plaintiff Winkelvoss harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Winkelvoss's expense.

365. Because of Defendants' conduct, Plaintiff Winkelvoss has lost control over the use of his Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

366. Defendants' secret collection of Plaintiff Winkelvoss's Personal Data deprived Plaintiff Winkelvoss of control over valuable personal information. Plaintiff Winkelvoss' Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff Winkelvoss did not authorize the sale, or use of his Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Winkelvoss' Personal Data for Defendants' financial benefit. Plaintiff Winkelvoss' Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using

that data without Plaintiff Winkelvoss' knowledge, compensation, or control. Plaintiff Winkelvoss would have expected compensation in exchange for providing Plaintiff Winkelvoss' Personal Data to third parties looking to use it for their own benefit.

367. Plaintiff Winkelvoss had a reasonable expectation that his location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

368. **Plaintiff Eboni Wright** is an adult individual and a natural person, citizen of Florida, where she resides and intends to stay.

369. In or around 2017, Plaintiff Wright downloaded and used the Life360 app on her mobile phone. In addition, in or around 2022, Plaintiff Wright downloaded and used the Allstate app. Plaintiff Wright downloaded the apps for personal use. Plaintiff Wright reviewed the prominent information about the nature and function of the apps presented to Plaintiff Wright prior to downloading and using the apps. Plaintiff Wright was not provided meaningful notice that Defendants would use the apps to collect and share her Personal Data.

370. Plaintiff Wright is informed and believes that the apps integrate an SDK provided by Defendants, which harvests several types of data from Plaintiff Wright's phone without her knowledge or consent, including but not limited to her:

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

b. how Plaintiff interacted with the phone including when and whether the device was in Plaintiff's hand, how long Plaintiff used the app in which the SDK was integrated, and when and whether the device was locked or unlocked;

c. "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;

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

e. "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

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

371. Plaintiff Wright was unaware that Allstate and Arity's SDK had been integrated into the apps at the time she installed, and later when she used the apps. Through the apps, and the integrated SDKs, Defendants covertly collected, intercepted, and transmitted the types of data listed above, including but not limited to data related to Plaintiff Wright's driving behavior, without Plaintiff Wright's knowledge or consent.

372. Upon information and belief, insurance premiums paid by Plaintiff Wright was, in part, based on Personal Data covertly collected and used by Defendants. The Personal Data was uncontextualized and its accuracy was unverified. Any analysis derived from such Personal Data would be unreliable and misleading. For example, Plaintiff Wright rode as a passenger numerous times while carrying Plaintiff Wright's mobile phone, and any assumption that the movement of Plaintiff Wright's phone during those trips reflected Plaintiff Wright's driving was inaccurate. Furthermore, any insurance premiums based on this analysis would necessarily be inflated. Accordingly, as a result of Defendant's covert collection and use of her Personal Data, Plaintiff Wright paid more for insurance than she otherwise would have.

373. Defendants' interception, collection, and monetization of Plaintiff Wright's highly sensitive Personal Data without consent caused Plaintiff Wright harm, invasion of privacy, and unjust enrichment of Defendants at Plaintiff Wright's expense.

374. Because of Defendants' conduct, Plaintiff Wright has lost control over the use of her Personal Data, which is in the possession of third parties who have used it and will use it for their own financial advantage.

375. Defendants' secret collection of Plaintiff Wright's Personal Data deprived Plaintiff of control over valuable personal information. Plaintiff's Personal Data has intrinsic and economic value, as demonstrated by Defendants' practice of selling or licensing access to such data to insurers, marketers, and other third parties. Plaintiff did not authorize the sale, or use of her Personal Data, and did not receive any compensation. Defendants' conduct resulted in the unauthorized exploitation of Plaintiff Wright's Personal Data for Defendants' financial benefit. Plaintiff Wright's Personal Data is economically and intrinsically valuable, and Defendants profited by commodifying and selling or otherwise using that data without Plaintiff Wright's knowledge, compensation, or control. Plaintiff Wright would have expected compensation in exchange for providing Plaintiff Wright's Personal Data to third parties looking to use it for their own benefit.

376. Plaintiff Wright had a reasonable expectation that her location, driving behaviors, and movement patterns would remain private unless expressly authorized for collection and use.

B. Defendants

377. **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.

378. **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.

379. **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.

380. **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.

381. **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, Arity 875, 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.

382. **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, Arity Services, 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.

383. Upon information and belief, the Allstate and Arity Defendants collaborated among themselves to create a common enterprise for the purpose of collecting Driving Data and Identity Information. Defendants used this Data to support and expand their own insurance business and to sell to third parties for profit. Defendants achieved this common enterprise by relying on coordination between themselves.

384. While Defendant Allstate had developed methods of collecting this data, it formed the Arity subsidiaries in 2016 to further develop and advance its data collection and monetization efforts. Gary Hallgren, the self-purported President of both Arity and Allstate Connected Car,[7] has described the decision by Allstate to form Arity as follows: "[Allstate] faced two choices: they could either keep the technology for themselves or look to the industry. Allstate did the latter and realized we had a strategic asset that could be valuable to the rest of the industry, so Arity formed in 2016."[8]

[7] Gary Hallgren, Linkedin, https://www.linkedin.com/in/garyhallgren/ (last accessed May 22, 2025)

[8] Peter High, *How Allstate Built An Analytics Company Anticipating Major Changes In Transportation*, Forbes (Nov. 11, 2019), https://www.forbes.com/sites/peterhigh/2019/11/11/how-allstate-built-an-analytics-company-anticipating-major-changes-in-transportation/

385. Hallgren has further described the relationship between Allstate Defendants and Arity Defendants, stating:[9]

386. **We think of the Allstate Insurance Company as our customer, and they are in a regulated industry**. Our corporation is not in the regulated part of the Allstate corporate structure, so we must interface with them in the same way that a vendor and a customer would interface for a whole variety of legal and regulatory reasons. **We have a different relationship with the Allstate Corporation. From there, we can leverage a variety of resources, especially around security and cyber.** Having the backing of a [major] financial services company that takes security and cyber so seriously gives us great benefits relative to our competitors of similar size. We try to take the best from the Allstate Corporation, and we are fortunate to have customers that are siblings to us inside of the corporate hierarchy.

387. From 2017 to present, Arity Defendants have marketed and sold Driving Data and Identity Information to Allstate Insurance Defendants as well as to non-Allstate affiliates.[10]

III. JURISDICTION AND VENUE

388. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual class members exceed the sum or value of $5,000,000, exclusive of interests and costs, and this is a class action in which one or more members of the proposed class, including thirty-three (33) Plaintiffs, are citizens of a state different from Defendants. The Court has

[9] *Id.*

[10] The Allstate Corporation, Inc, Form 10-K (Feb. 26, 2018) https://www.allstateinvestors.com/node/14596/html.

supplemental jurisdiction over the alleged state law claims under 28 U.S.C. § 1367 because they form part of the same case or controversy.

389. This Court has personal jurisdiction over the Defendants as Defendants maintain their principal headquarters in this District, do business in this District, directly or through agents, and have sufficient minimum contacts with this District such that they have intentionally availed themselves of the laws of the United States and Illinois.

390. Venue is proper under 28 U.S.C. § 1391(a) through (d) because Defendants' headquarters and principal place of business are located in this District, Defendant resides in this District, and substantial parts of the events or omissions giving rise to the claims occurred in or emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel.

IV. FACTUAL BACKGROUND

391. The car insurance industry collects information about consumers in order to assess an individual's eligibility for insurance, and to set an individual's insurance premium. To calculate premiums, car insurance carriers ("Insurers") collect personal data about drivers, including their driving records, their vehicle, garage, location, and personal characteristics like age and gender.[11] Defendants, however, have taken those efforts further than even the most privacy-conscious consumer could possibly imagine.

392. Using surveillance technology embedded in third-party mobile device applications and in-car sensors to amass vast amounts of highly-sensitive, individual-specific consumer data,

[11] National Association of Insurance Commissioners, "Want Your Auto Insurer to Track Your Driving? Understanding Usage-Based Insurance," NAIC (Sept. 8, 2021) https://content.naic.org/article/consumer-insight-want-your-auto-insurer-track-your-driving-understanding-usage-based-insurance#:~:text=UBI%20or%20usage%2Dbased%20insurance,type%2C%20and%20insurance%20credit%20score.

Defendants have built highly detailed data profiles of at least 45 million Americans, including Plaintiffs,[12] and all without consumers' knowledge or consent.

393. Defendants have monetized this data in a variety of ways, including when underwriting their own automotive insurance policies (in contravention of their own stated privacy policies and insurance agreements), and by selling access to the "world's largest driving behavior database" to third parties, including other Insurers, that likewise use this ill-gotten data to the detriment of consumers.[13]

A. Telemetric Data About Driving

394. In recent years, a new method of collecting individual-specific information has proliferated: telemetry. At a high level, telemetric data provides detailed and time-stamped data about an individual's location, movements, and device usage and is transmitted remotely. Combining telemetric data yields "telematics": data on a driver's speed, phone usage, attention, miles driven, idling time, acceleration and braking, and airbag deployment. This data can be collected through, among other methods, systems installed in vehicles, mobile applications, or SIM cards installed on mobile phones.[14]

395. With the advent of driving telemetric data, the insurance industry touted collection of telematic data in order to provide Usage Based Insurance.[15] Insurers have proposed that

[12] Arity, "Vehicle Miles Traveled," https://arity.com/solutions/vehicle-miles-traveled/, (last accessed May 22, 2025).

[13] Arity, https://arity.com/ (last accessed May 22, 2025).

[14] Carter Cordes, "Driving value from fleet telematics," McKinsey & Company (Dec. 18, 2018), https://www.mckinsey.com/capabilities/operations/our-insights/driving-value-from-fleet-telematics#/; Verizon Connect, "What is Telematics?" Verizon (June 26, 2023) https://www.verizonconnect.com/resources/article/what-is-telematics/.

[15] National Association of Insurance Commissioners, "Want Your Auto Insurer to Track Your Driving? Understanding Usage-Based Insurance," NAIC (Sept. 8, 2021) https://content.naic.org/article/consumer-insight-want-your-auto-insurer-track-your-driving-

analyzing this data allows Insurers to compose a picture of driver behavior, and provide personalized premiums for car insurance.

396. A key feature of Usage Based Insurance is consumer consent.[16] In some states, consent for Usage Based Insurance is a statutory requirement, along with the right to dispute the veracity of the information collected, regulatory reviews of the algorithm collecting and analyzing telemetric data, and a requirement to anonymize any individual consumer data that is transferred or sold.

397. To implement User Based Insurance and collect telematics data, insurance companies have developed smart phone applications ("apps") that allow consumers to access information about their policies, make claims, request roadside assistance, and significantly, enable telemetric data collection.[17]

398. In 2024, 15% of auto-insurance shoppers were offered Usage Based Insurance, and of that 15%, only 17% signed up.[18]

---

understanding-usage-based-insurance#:~:text=UBI%20or%20usage%2Dbased%20insurance,type%2C%20and%20insurance%20credit%20score.

[16] Omri Ben-Shahar, "Privacy Protection, At What Cost? Exploring the Regulatory Resistance to Data Technology in Auto Insurance," Coase-Sandor Working Paper Series in Law and Economics, No. 985 (2023) at 10 f.14, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1114&context=law_and_economics_wp.

[17] Daniel Robinson, "Guide to the Best Car Insurance Apps," MarketWatch (Aug. 9, 2024), https://www.marketwatch.com/insurance-services/auto-insurance/guide-to-the-best-car-insurance-apps/.

[18] J.D. Power, "Get Ready for an Insurance 'Shop-a-Palooza' in 2025" (Dec. 20, 2025) https://www.jdpower.com/business/resources/2025-insurance-outlook

399. Despite the small percentage of auto-insurance shoppers that select Usage Based Insurance products, the market for Usage Based Insurance is estimated to grow from $57 billion in 2023 to $66 billion by 2032.[19]

400. Not satisfied with the amount of data obtained from consumers that opt-in to Usage Based Insurance, Defendants devised a scheme to use other apps to track individuals and obtain significantly more data regarding the millions of consumers that have not opted in to UBI. Most concerning, this tracking was done through third-party apps rather than those developed, published and associated with Defendants, and thus without the knowledge and informed consent of Plaintiffs and class members.

401. Defendants use the voluminous data they intercepted and collected without consumers' consent to enrich themselves at the expense of consumers, including by setting automotive insurance rates for their own customers, and selling the data to third parties.

B. Defendants Developed Software Tools to Covertly Collect Consumers' Data

402. To siphon and amass data concerning consumers, Defendants developed software to embed in third-party apps that require consumers to communicate location data for the app to function as intended.

403. A software development kit ("SDK") is a software-building tool that includes a library of pre-built tools and frameworks, including Application Programming Interfaces ("API"), and code specific to an operating system (such as Android or Apple). SDKs can be downloaded in

[19] Fortune Business Insights, "Automatic Usage Based Insurance Market Size," (Apr. 14, 2025) https://www.fortunebusinessinsights.com/automotive-usage-based-insurance-market-104103.

order to build or integrate into apps in order to reduce the costs, resources, and time required to build apps.[20] Preprogrammed functions in SDKs operate in the background of mobile devices.

404. Developers using SDKs may not know the full extent and functions of the code embedded in their apps. SDKs can be (and, as alleged here, often are) designed to intercept users' location or behavioral data and their personally identifiable information.[21]

405. Defendants' SDK (also referred to herein as the "Arity SDK" and "Defendants' SDK") does all of the above. Defendants made the Arity SDK available to third-party developers to insert as a plug-in for their respective apps. Defendants developed and integrated their SDK not only into their own applications (such as Drivewise), but also into third-party apps unrelated to the provision of automotive insurance, including, but upon information and belief not limited to, Life360 (an app for individuals to share their locations with one another), SiriusXM (a radio and broadcasting app), GasBuddy (an app that identifies gas prices by locations), and the weather apps MyRadar and Weather Bug, the functionality of which relies on location data.[22] Defendants did so to ensure that when an individual downloaded any of these apps they also, unwittingly, downloaded Defendants' software.

406. The Arity SDK siphons, collects, and diverts in real time substantial amounts of data concerning users, including the user's geolocation and movements, as well as the individual's use of the smartphone.

---

[20] Arity, "Powering safer driving with DriveDown," (Sept. 2023) https://arity.com/wp-content/uploads/2023/09/Arity_Case-Study_insol_southern-farm-bureau.pdf.

[21] IBM, "SDK v. API: What's the difference?" https://www.ibm.com/think/topics/api-vs-sdk (last accessed May 3, 2025).

[22] Kathleen Sampey, "Arity's Driver Data Reaches 200 Million Connections," Street Fight Magazine (Mar. 24, 2023) https://streetfightmag.com/2023/03/24/aritys-driver-data-reaches-200-million-connections/.

407. "Smartphones come equipped with an array of microelectromechanical sensors (MEMS) capable of gathering information about the world around them, such as location-based and motion sensors, environmental sensors, biometric sensors and activity and health sensors."[23] Specifically, "Smartphone sensors are specific technologies able to sense a physical quantity and translate it into electric signals, so that the particular quantity can be interpreted by the smartphone computing system."

408. A smartphone's accelerometer, magnetometer, and gyroscope are such sensors that collect and send signals that, when processed through the internal computing system, enable the device to perform useful functions for the user's benefit including measuring steps taken and determining the device's position for screen orientation and game functions. They "permit capturing data directly from hardware sensors, embedded into the device, and derived sensors which provide processed and fused data from a few raw sensors all at once, providing users of the system with different information." A user can grant access to this data to software developers "to create novel sensing applications of increasing functionality and complexity."[24]

409. Unbeknownst to consumers, Defendants' apps and the SDK embedded in third-party apps siphon consumers' phone and location data, including precise geolocation data. The Arity SDK can even track users' locations through public Bluetooth beacons, which enable fine-grained tracking indoors.[25]

---

[23] George Grouios et al., "Accelerometers in Our Pocket: Does Smartphone Accelerometer Technology Provide Accurate Data?" (Dec. 24, 2022) https://pmc.ncbi.nlm.nih.gov/articles/PMC9824767/.

[24] *Id.*

[25] Devin McLaughlin, "OEM and mobile telematics data: Unlock a more complete driver profile," Arity (Sept. 9, 2024), https://arity.com/move/oem-and-mobile-telematics-data-unlock-a-more-complete-driver-profile/.

410. Once downloaded onto a consumer's device, the Arity SDK can intercept and read massive amounts of consumer data.[26] The Arity SDK collects telemetric information about trip distance, trip duration, phone usage, driver attention, acceleration, hard braking, and GPS coordinates, including longitude and latitude, that is collected in "real-time."[27] The movement-tracking portion of this collection is accomplished through GPS, accelerometer, and gyroscope sensors on mobile phones that can track a vehicle's speed, direction, and lane changes.[28]

411. The Arity SDK also collects additional data that includes but is not limited to:

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

b. how a user interacts with their device including whether the user locks and unlocks their phone;

c. whether the phone is in the user's hand;

d. the amount of time the user spends using the app in which it is embedded;

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

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

[26] Arity, "How can insurers drive profitable growth using telematics?" https://arity.com/auto-insurance-drive-profitability-growth-telematics/ (last accessed May 4, 2025).

[27] Arity, "Arity Platform," https://apidocs.arity.com/ (last accessed May 4, 2025).

[28] Satoru Inoue, "Analytics in action: What driving data can we collect from accelerometers?," Arity (Oct. 28, 2024), https://arity.com/move/analytics-in-action-what-driving-data-can-we-collect-from-accelerometers/.

g. "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

h. Metadata, such as ad ID, country code, iOS vs. Android indicator, User ID, Mobile Advertising ID ("MAID"), device type, app version, and OS version.[29]

412. In addition to the foregoing data, the Arity SDK also collects information about the mobile device on which the app is installed, like IP addresses, browser and device information, user IDs, geolocation data, and other data. Defendants use this data (as well as personally identifiable information such as names and email addresses licensed from their partner apps) to "fingerprint" individuals, which allows them to generate revenue from the use of this data and the later sale thereof to third parties.[30]

413. Additionally, the Arity SDK collects and transmits encrypted data to Defendants concerning the devices, user, and user's actions. Due to the nature of the encryptions, Plaintiffs cannot determine the full extent of the data that the Arity SDK intercepts and transmits to Defendants.

414. The Arity SDK runs in the background of the device, even if the user is not currently using an app that includes the Arity SDK.

415. The Driving Data collected by Defendants, even without Identity Information, can be personally identifying. For example, the data collected just from the accelerometer of a mobile

[29] Allstate, "Allstate online Privacy Statement," (Sept. 6, 2024), https://delivery.contenthub.allstate.com/api/public/content/3140e554e53b44dfa00a40f15fddca39?v=a9270b36.

[30] Allstate, "Allstate online Privacy Statement," (Sept. 6, 2024), https://delivery.contenthub.allstate.com/api/public/content/3140e554e53b44dfa00a40f15fddca39?v=a9270b36.

device can create an "accelerometer fingerprint" that be used by the receiver of that data to "track [a user] over space and time."[31] One study found that, once created, such a "fingerprint" is "hard to erase, unless the accelerometer wears out to the degree that its fingerprint becomes inconsistent"—which was not observed even once during 9 months of testing 107 different accelerometers.[32]

416. In addition to the telemetric information, the Arity SDK collects usage data from mobile phones, including "scrolling, tapping, locking and unlocking, and hands-free phone calls."[33] This data goes far beyond where a consumer is at any given moment and directly communicates the user's decisions, actions, choices, and activities, and can and is used to understand consumers' behaviors and actions.

417. The Arity SDK is little more than a method for Defendants to scrape user data from unrelated third-party apps under the pretext of providing a necessary function, and all alongside various identifiers unique to the consumers from whose data has been misappropriated, allowing Defendants to build incredibly detailed profiles concerning the movements, actions, behaviors and choices of specific individuals and others close to them.

418. Meanwhile, consumers who had chosen to download and use a third-party app with the Arity SDK embedded had no knowledge that the app they were using contained the Arity SDK, which was harvesting their data for these purposes. Defendants never notified nor otherwise

[31] Dey at al., "AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable" at 2, *available at* https://www.ndss-symposium.org/wp-content/uploads/2017/09/03_2_1.pdf.

[32] *Id.*

[33] Arity, "Device data is good. Mobility data is better," (Mar. 12, 2020), https://arity.com/move/shift-location-device-data-mobility-data/.

informed consumers that they were collecting consumer data via the Arity SDK and third-party apps.

C. Defendants Paid App Developers to Integrate the Arity SDK Into Mobile Apps

419. Since at least 2017, Defendants have paid third-party app developers millions of dollars to integrate the Arity SDK into their respective mobile apps. Defendants successfully integrated Arity SDK into several popular apps, such as Routely, Life360, GasBuddy, Sirius XM, Fuel Rewards, Streetwise, GPS Driving Route, Fuelzee, and Ago. These apps had a key feature that made them appealing to Defendants as a vehicle for their data collection efforts: all these apps required location information to function properly. Location information is central to the development of the Personal Data Defendants sought to capture, since it factors into many components of driver data, including geolocation, "trip attributes," "GPS points," and "derived events."

420. Once an app integrated the Arity SDK, a consumer who downloaded and used that app unknowingly enabled Defendants to collect their location data without their consent.

421. In addition, Personal Data collected from users by the third-party apps was licensed to and shared with Defendants. The personal data that mobile apps licensed to Defendants generally included first and last name, phone number, address, zip code, mobile ad-ID ("MAID"), and device ID. Together with the Driving Data, the Personal Data could be used by Defendants to more reliably identify the specific person being monitored by the Arity SDK.

422. Defendants would similarly share some of the driving data they collected with the third-party apps with which they contracted to support those apps' features. Thus even the third-party apps that consumers chose to download and use for a specific purpose profited from Defendants' surreptitious and nonconsensual collection of consumers' personal information.

D. Defendants Offer Drivewise

423. As well, in 2010, Defendants began offering Drivewise to Allstate customers, which monitored driving behavior through a small telematics device provided by the company to customers at their request. Defendants offered that if customers installed Drivewise devices in their cars they could be rewarded for low mileage and safe driving by, for example, receiving lower rates or other discounts [34] In 2014, Defendants introduced Drivewise Mobile for Allstate customers, the industry's first mobile telematics app.

424. The current iteration of the Drivewise program uses a mobile app that includes a "dashboard" providing driving feedback in real time, "driving insights" that provide personalized feedback on how users can make driving improvements, and a "trip summary" that includes trip histories, parking locations, and family driving insights.[35]

425. Drivewise identifies safe driving by automatically detecting when trips occur and collecting driving information such as speed, braking behaviors, and the time of day you're on the road.[36]

426. Nevertheless, Defendants acknowledge that "Drivewise follows the person, not the vehicle," so the app will detect trips when you are a passenger in a vehicle.[37] Trips are assigned a predicted vehicle, i.e., automobile, train, bus, plane or boat, but can be wrong. The Drivewise user could also be identified as the driver when he or she is in fact the passenger. For this reason, and

[34] *Our History*, Allstate, https://www.allstatecorporation.com/about/our-history.aspx (last accessed May 22, 2025).

[35] *Drivewise from Allstate*, Allstate, https://www.allstate.com/drivewise (last accessed May 22, 2025).

[36] *Id*.

[37] *Drivewise FAQs,* Allstate, https://www.allstate.com/drivewise/drivewise-faq-asc (last accessed May 22, 2025).

in clear recognition of the imperfect method that collecting driver trip data through a mobile phone represents, the Drivewise program allows users to edit recorded to trips to correct mistakes before they are considered for any rate or discount decision.

427. Defendants include in the Drivewise app the Arity SDK, and through it share all data they collect through the app. Defendants clearly understand that no consumer would permit submission of driving data to their auto insurer without the opportunity to review and correct it. Defendants offer this opportunity with their own Drivewise app. Nevertheless, there is no such ability for any consumers to correct the data collected by the Defendants through the Arity SDK, or control how that information is further relayed to insurers.

E. Defendants' Products and Services Monetized Class Members' Personal Information

428. Defendants further profited off of the Personal Data they collected by using it to create and sell additional products and services. These products and services included:

a. **Drivesight**. Drivesight is a product created and sold by the Arity Defendants to third parties to generate a driving score for potential insureds by analyzing data and using that information to score that individual's driving risk.[38]

b. **ArityIQ**. This product is directed at insurers, enabling them to access the driving data collected by Defendants and to use that data to assign more accurate (and therefore "to price more profitably") insurance rate quotes to individual consumers."[39]

[38] Arity, "Drivesight®," https://arity.com/solutions/drivesight/ (last accessed on May 22, 2025).
[39] Arity, "ArityIQ SM," https://arity.com/solutions/arity-iq/ (last accessed on May 22, 2025).

c. **Arity Marketing Platform**. Defendants' marketing platform enables third-party advertisers to target drivers "based on driving behavior data" and publishers to "monetize their inventory by displaying relevant ads to high-intent US drivers at scale."[40]

d. **Arity Audiences**. Defendants let companies, including third-party insurers, target drivers with marketing "based on their actual driving history." As part of this product, Defendants displayed ads to the users of apps that agreed to integrate the Arity SDK.[41]

e. **Real Time Insights**. This product collects and distributes transportation-related data derived from the personal and driving data collected by Defendants.

f. **Routely**. This product is offered to consumers as a "free" application providing "helpful insights" into the consumers' driving habits to encourage safer driving. By contrast, Defendants sell this product to insurers as "a better way to effectively measure and quantify risky driving behaviors" and "provide personalized pricing while lowering loss ratios."[42]

429. Defendants also partnered with Google, starting in October 2023. Defendants provided their data to "Google Cloud's insurance customers," including unnamed third parties.[43]

[40] Arity, "Arity Marketing Platform," https://arity.com/solutions/arity-marketing-platform/ (last assessed on May 22, 2025).

[41] Arity, "Arity Audiences," https://arity.com/solutions/arity-audiences/ (last accessed on May 22, 2025).

[42] Arity, "Routely®," https://arity.com/solutions/routely/ (last accessed on May 22, 2025).

[43] Arity, "Arity launches Arity IQ℠ on Google Cloud's Analytics Hub," (Oct. 19, 2023), https://arity.com/move/arity-launches-arity-iq-on-google-clouds-analytics-hub.

430. Defendants track and associate the data collected with specific individuals using various smartphone device identifiers. One of the above-referenced unique smartphone identifiers collected by the Arity SDK, in addition to consumers' names and email addresses, is a Mobile Advertising ID ("MAID"). A MAID is a unique identifier assigned to a consumer's mobile device to assist marketers in advertising to the consumer. MAIDs thus can be used to fingerprint consumers across the internet, and associate and aggregate data collected about them in one place with data generated elsewhere. For example, on iPhones, the MAID is referred to as an identifier for advertisers ("IDFA"), is used for tracking and identifying a user and is assigned at the device level.[44]

431. Although a MAID may be changed by a consumer, doing so requires the consumer to proactively reset the MAID on the consumer's mobile device. Some consumers attempt to block developers from accessing their device's MAID in order to prevent the association of a phone's location data and other unique identifiers with a specific individual.

432. In addition to the IDFA, app developers also create unique identifiers for users of their apps, referred to as the "Identifier for Vendors," or IDFV.[45] An IDFV is a code created by an app developer and assigned to all of their apps. This code is also shared between all of the apps created by the same developer. The IDFV value is the same for apps from the same developer running on the same device. IDFVs thus provide a way to run cross-promotional iOS campaigns,

[44] The Android equivalent of the IDFA is called GAID, for Google Advertising ID. Play Console Help, "Advertising ID," GOOGLE, https://support.google.com/googleplay/android-developer/answer/6048248?hl=en (last accessed May 4, 2025).

[45] Apple Developer, "IdentifierforVendor," Apple, https://developer.apple.com/documentation/uikit/uidevice/identifierforvendor (last accessed May 4, 2025).

compatible with iPhones. So long as an IDFV is passed in the tracker URLs and apps, the IDFV can provide app developers with more accurate attribution data for iOS campaigns.[46]

433. In other words, even when consumers try to protect their privacy by disabling device tracking for advertising purposes, app developers can overcome those efforts by doing an end-run around those consumer protections by gathering IDFV and other unique identifying information in order to continue to track consumers without their knowledge or consent, thus further invading their privacy.

434. Privacy experts note that mobile advertising IDs like MAIDs can be more valuable as a tracker and a "better identifier than a name because "[t]his code can be used to track and follow you across many life situations."[47]

435. 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, or which particular person was driving.

436. For example, if a person was a passenger in a bus, a taxi, or a friend's car, and that vehicle's driver sped, braked hard, 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.

[46] Apple Developer, "IdentifierforVendor," Apple, https://developer.apple.com/documentation/uikit/uidevice/identifierforvendor (last accessed May 4, 2025).

[47] Jon Keegan and Alfred Ng, "The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users," The Markup (Dec. 6, 2021), https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user.

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.

437. In a further example of the obvious flaws in Defendants' abusive practices using Driving Data, a person's driving score was lowered because the "driving" behavior data collected from his phone by that insurance company assumed he was driving, when he was actually riding a roller coaster.[48]

438. The Driving Data further would not reflect contextual information necessary to determine whether certain driving events recorded reflected risky driving. A "hard braking event," for example, could be the result of a sudden hazard such as a child or animal running into the roadway. But the Driving Data would record only a "hard braking event," negatively impacting the risk score assigned by Defendants.

439. These flaws are and should have been obvious to all of the Defendants, yet they continued to collect, disclose, and profit from flawed Driving Data without regard to inaccuracy of the information.

440. Nevertheless, the data Defendants collect through the Arity SDK is incredibly valuable. Geolocation data alone is part of an estimated $12 billion market.[49]

441. An investigation by the Public Interest Research Group found that the data Defendants collect just on consumer geolocation is sold to advertisers so that they can target

[48] 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-cutsdriving-score-man-riding-the-beast-kings-island/75554987007/.

[49] Jon Keegan and Alfred Ng, "There's a Multibillion-Dollar Market for Your Phone's Location Data," The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

consumers based on location and driving habits, allowing advertisers to target consumers "on when and where they drive."[50]

442. Defendants' monetization efforts have proven successful and profitable, stating "[t]elematics data available at time of quote through the Arity IQ℠ network was exactly what many of our partners needed to return to a stable, profitable state."

443. Defendants further attribute the industry's swing to a $9.3 billion underwriting gain in Q1 of 2024, compared to the $8.5 billion loss in Q1 of 2023, because of Insurers' more widespread use of their telematics information.[51] And between 2024 and 2025, Allstate's "revenue increased 50.6% or $43 million" which Allstate credited, "primarily due to higher lead generation revenue at Arity."[52]

F. Defendants' Failure to Disclose the Collection, Sharing, and Use of Plaintiffs' Driving Data

444. 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. Defendants do not verify whether the third-party apps that incorporate Arity SDK obtain informed consumer consent prior to collecting, recording, using, and disseminating consumers' data.

445. In fact, Defendants and the apps running Defendants' SDK either failed to inform Plaintiffs and Class Members that Defendants were collecting Personal Data and Driving Data, or

[50] R.J. Cross and Nico Vacca, "How Allstate's data broker Arity sells driver Data," Public Interest Research Group (Jan. 22, 2025), https://pirg.org/resources/allstate-arity-selling-data/.

[51] Jen Gold, *How Telematics is Revolutionizing Auto Insurance Marketing Strategies*, ARITY (Oct. 21, 2024) https://arity.com/move/how-telematics-is-revolutionizing-auto-insurance-marketing-strategies.

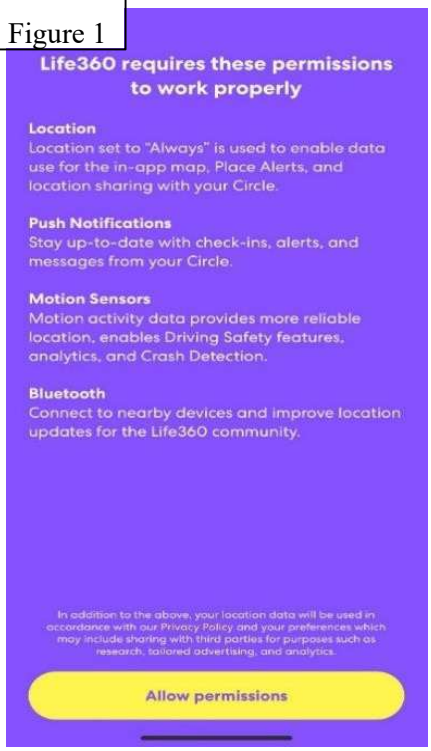
[52] The Allstate Corporation, Inc, "Form 10-K for Fiscal Quarter Ended May 31, 2025," https://www.allstateinvestors.com/static-files/cd69f838-5d9b-4b01-b4c4-237b935afd1c.

purported to do so in a manner so misleading, confusing, deceptive, and opaque that no reasonable consumer would have understood the extent of the Personal Data and Driving Data collection. Vague disclosures offered by third party apps stating that they are "powered by Arity" or that "certain information" is shared with Defendants did not hint at the scope, sensitive nature, detail, and volume of data sharing, nor that Defendants were using them to build profiles to used and sold for profit.

446. Thus, neither Defendants nor the apps on Defendants' behalf, informed Plaintiffs and Class Members of the various ways that Defendants would collect, use, and ultimately monetize the Personal Data collected by Defendants.

447. For example, Life360 told app users that it needed location sharing turned on "to enable data use for the in-app map, Place Alerts, and location sharing with [a user's] Circle." Nowhere on that screen – even in the fine print – did Life360 mention Defendants' existence, let alone the breadth of Defendants' data collection and use and sale of that data.

Figure 1



448. Similarly, Fuel Rewards requests permission to track location to "Allow Fuel Rewards to use your location to help find the best gas prices near you and to send you personalized offers and location based alerts." Nowhere is it disclosed that users' mobile phone location and other data is being used to infer driving behavior for purposes of auto insurance underwriting, nor would any reasonable consumer infer that. The reference to additional disclosure of "location" to "third parties" and "business partners" is not just vague but affirmatively misleading given the breadth of data actually shared and because the data is being used for much more than "provid[ing] you with personalized offers."

Figure 2

Location Services

Allow Fuel Rewards ® to use your location to help find the best gas prices near you and to send you personalized offers and location-based alerts. This information may be collected while you are using the app and in the background. We will also share or disclose your location with third parties, including our business partners as described in our privacy policy, to provide you with personalized offers.

Allow Location

449. Because Defendants did not disclose their unlawful practices, Plaintiffs and Class Members were wholly unaware that Defendants were collecting the Personal Data and Driving

Data from their phones. Plaintiffs and Class Members were likewise wholly unaware (and had no way of knowing) that Defendants would use the Personal Data and Driving Data to create and sell several different products and services to third parties, including other insurers.

450. Defendants did not provide Plaintiffs 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.

451. Even if a Class Member took the extra step to investigate Defendants outside of the app by navigating to Defendants' website and locating their privacy disclosures, Class Members would still not understand the breadth of the data collected or 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.

452. For example, Arity's Privacy Policy states that it "do[es] not sell personal information for monetary value,"[53] which is false – and Defendants know it is false. Defendants sold a number of data-based products and services for monetary value that linked a specific app user to their alleged driving behavior, which is personal information. Further, Defendants do not provide Class Members with the ability to request that Defendants stop selling their data.

453. Defendants likewise obscured how they used Plaintiffs' 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

[53] Arity, "Privacy Statement," *supra* n.1.

fail to explain that they combine the Driving Data and Personal Data to create a database of driving profiles for more than 45 million Americans and sell access to that database as a for-profit product. 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.[54]

454. 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. The privacy statement did not provide a method for a consumer to request that such data not be used to profile them.

G. Defendants' Practices Cause Substantial Injury to Consumers

455. Since Defendants' SDK records location and other data regardless of whether the device is active or idle, and this information is transmitted to Defendants in real time, Defendants are able to collect highly sensitive information about consumers. Even with just location data, Defendants could determine where someone lived, where they worked, where their children go to school, where they go for medical treatment, where they worship, whether and which rallies, demonstrations or protests they attend, and any and all information that can be determined by tracking a person's location and movement. Defendants collected this highly sensitive information,

[54] *Id.*

and integrated it with unique PII and demographic data, and additional data regarding their device usage.

456. Such data is valuable for marketing and advertising purposes, and is therefore regularly bought and sold in the "data broker" market. The data broker market is a booming industry market analysts estimate generates nothing less than hundreds of billions of dollars annually. The general market for location data alone is estimated to be over $12 billion.[55] Thus, Plaintiffs were economically harmed because the information taken from them without consent has an economic value that can be measured by the very markets for that data the Defendants participate in.

457. In addition, Defendants' actions caused economic harm to Plaintiffs who faced adverse insurance outcomes, such as denied coverage, increased rates, dropped coverage, and excessively high quotes, as a result of the information Defendants collected about them and packaged for use and sale in the insurance market.

458. Defendants' actions also caused significant privacy harms. Defendants' extensive surveillance of Plaintiffs' activities while using their phones and within their vehicles—a private space where individuals spend a considerable amount of time speaking with others and engaging in intimate actions beyond simply driving—is an unlawful intrusion in and of itself. Collection and sale of such data is an intrusion into the most private areas of a consumer's life. The scope, quality, and character of the data collected must also be considered as part of that harm. Consumers do not expect that their every movement and details of their device usage, including both in their own

[55] There's a Multibillion-Dollar Market for Your Phone's Location Data, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

vehicles in additional to any other vehicle in which they travel will be tracked in excruciating detail, recorded, and disseminated to unknown third parties.

H. Plaintiffs' Injuries

459. As described more fully above, the data that Defendants extracted, manipulated, and monetized may be used to identify consumers' sensitive locations and to infer "driving behavior" including driver attention and details regarding their device usage. The collection and sale of this data is an unwarranted and unauthorized intrusion into the most private areas of a consumer's life and has caused, or is likely to cause, substantial injury to the consumers and their privacy interests.

460. Each Plaintiff's cell phone contains one or more mobile applications that have embedded Defendants' SDK.

461. On information and belief, the SDK harvested several types of data from each Plaintiff's phone without their knowledge or consent, and exfiltrated this data to Defendants, including but not limited to:

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

b. how a user interacts with their device including whether the user locks and unlocks their phone;

c. whether the phone is in the user's hand;

d. the amount of time the user spends using the app in which it is embedded;

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

f. "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;

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

h. Metadata, such as ad ID, country code, IOS vs Android, User ID, device type, app version, and OS version.

462. Each Plaintiff was unaware that Defendants' SDK was covertly installed on his or her phone. Each Plaintiff was similarly unaware that this SDK was secretly collecting her or his highly granular location, driving, and other data -- and exfiltrating it to Defendants.

463. None of the Plaintiffs consented to Defendants' conduct. None of the Plaintiffs have any agreement with the Defendants concerning the collection of private information from their mobile devices.

464. Plaintiffs have had insurers drop them from coverage, have been denied coverage, have experienced a substantial increase in insurance premiums compared to the steady and regular increases they would otherwise expect, and have been quoted excessively high premiums. These Plaintiffs have not had any accidents, speeding tickets, or other moving violations that could reasonably be attributed to their loss of coverage or these otherwise unreasonable rate increases.

465. The "driving behavior" and other data described above that was extracted from Plaintiffs without knowledge or consent has substantial integrity issues causing it to be misleading and unreliable as a way of profiling driving behavior. Defendants were aware of these obvious flaws, but marketed and sold the data to insurers to be used to infer driving habits anyway.

466. Plaintiffs' data has tangible value. Defendants' conduct has caused Plaintiffs and Class Members to lose control over the data that Defendants have secretly taken from them and sold for profit. This data is now in the possession of third parties, including insurers, that have used it for their own financial benefit, and will continue to use it to their advantage.

467. Plaintiffs and Class Members have a reasonable expectation of privacy in their vehicles, in taxis, on public transit, while going about their daily lives, and at their doctors' offices. Plaintiffs and Class Members reasonably expect that their location, driving behavior, routes, and schedule would not be collected, transmitted to third parties, or sold without express consent or authorization. This unceasing, detailed, comprehensive, and silent collection of data – including data not perceptible to the naked eye – for profile-building purposes far exceeds what any Plaintiff or Class Member reasonably understood another motorist or passerby might notice about Class Members' driving behavior by virtue of driving on the road with other people. By covertly harvesting, exfiltrating, manipulating, and selling their personal information, Defendants have invaded Plaintiffs and Class Members' privacy rights.

V. TOLLING OF THE STATUTE OF LIMITATIONS

468. All applicable statute(s) of limitations have been tolled by Defendants' knowing and active concealment and denial of the facts alleged herein. Plaintiffs and Class Members could not have reasonably discovered Defendants' practice of surreptitiously acquiring and compiling their Driving Data and Personal Data, including sensitive location data, without their consent, selling it to third parties, and/or compiling it in a manner that impacts their insurance premiums—including when the data gathered does not accurately reflect Plaintiffs or Class Members' driving habits.

469. Defendants were and remain under a continuing duty to disclose to Plaintiffs and Class Members their practice of acquiring Driving Data and Personal Data, including sensitive location data, for use in determining insurance premiums. As a result of the active concealment by Defendants, any and all applicable statutes of limitations otherwise applicable to the allegations herein have been tolled.

VI. CLASS ACTION ALLEGATIONS

470. Plaintiffs seek certification of the class set forth herein under Federal Rule of Civil Procedure 23. Specifically, Plaintiffs seek class certification of all claims for relief herein of a class and subclass defined as follows:

> **Class:** All persons residing in the United States and its territories whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Class").
>
> **FCRA Subclass:** All persons residing in the United States and its territories whose vehicle Driving Data and/or Identity Information was collected, stored, distributed, and/or sold by Defendants, and for which a report was created, which was then disclosed to a third party.
>
> **Alabama Subclass:** All person residing in Alabama whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Alabama Subclass").
>
> **Arizona Subclass:** All person residing in Arizona whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Arizona Subclass").
>
> **California Subclass:** All person residing in California whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "California Subclass").
>
> **Florida Subclass:** All person residing in Florida whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Florida Subclass").
>
> **Georgia Subclass:** All person residing in Georgia whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Georgia Subclass").
>
> **Illinois Subclass:** All person residing in Illinois whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Illinois Subclass").
>
> **Indiana Subclass:** All person residing in Indiana whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Indiana Subclass").
>
> **Kentucky Subclass:** All person residing in Kentucky whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Kentucky Subclass").

Michigan Subclass: All person residing in Michigan whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Michigan Subclass").

Mississippi Subclass: All person residing in Mississippi whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Mississippi Subclass").

New Jersey Subclass: All person residing in New Jersey whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "New Jersey Subclass").

New York Subclass: All person residing in New York whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "New York Subclass").

North Carolina Subclass: All person residing in North Carolina whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "North Carolina Subclass").

Ohio Subclass: All person residing in Ohio whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Ohio Subclass").

Oregon Subclass: All person residing in Oregon whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Oregon Subclass").

Pennsylvania Subclass: All person residing in Pennsylvania whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Pennsylvania Subclass").

South Carolina Subclass: All person residing in South Carolina whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "South Carolina Subclass").

Texas Subclass: All person residing in Texas whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Texas Subclass").

Utah Subclass: All person residing in Utah whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Utah Subclass").

Washington Subclass: All person residing in Washington whose Personal Data was collected, distributed, stored, and/or sold by Defendants (the "Washington Subclass").

471. Excluded from the proposed Class are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

472. Plaintiffs reserve the right to re-define the Class definition after conducting discovery.

473. **Numerosity (Fed. R. Civ. P. 23(a)(1)).** The Class Members are so numerous that joinder of all members is impracticable. Based on information and belief, the Class includes millions of people who were harmed as a result of Defendants' unlawful conduct. The parties will be able to identify the exact size of the Class through discovery and Defendants' records.

474. **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2); 23(b)(3)).** Common questions of law and fact exist for each of the claims and predominate over questions affecting only individual members of the Class. Questions common to the Class include, but are not limited to the following:

a. Whether Defendants engaged in the activities and practices referenced above, including whether Defendants collected and shared Plaintiffs' and Class Members' Driving Data;

b. Whether Defendants used this information to determine insurance premiums and/or insurance coverage;

c. Whether Plaintiffs and Class Members consented to such collection and sharing;

d. Whether Defendants were unjustly enriched;

e. Whether Defendants' conduct constitutes an invasion of privacy and/or an intrusion upon seclusion;

f. Whether Defendants' conduct violated federal and state wiretap laws;

g. Whether Defendants acted knowingly and/or willfully;

h. Whether Plaintiffs and Class Members sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

i. Whether Defendants should be enjoined from such conduct in the future; and

j. Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount.

475. 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.

476. **Typicality (Fed. R. Civ. P. 23(a)(3)).** Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs' claims are typical of the claims of the members of the Class because all Class Members' highly personal data was captured by Defendants in the same or substantially similar way, and thus Class Members were similarly harmed as a result.

477. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)).** Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class Members. Plaintiffs have retained counsel experienced in prosecuting class actions and data privacy cases.

478. **Superiority (Fed. R. Civ. P. 23(b)(3)).** Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual Class Members because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield

inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

479. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

a. the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual Class Members which would establish incompatible standards of conduct for Defendants;

b. the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to individual Class Members which would, as a practical matter, be dispositive of the interests of other Class Members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

c. Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

480. **Issue Certification (Fed. R. Civ. P. 23(c)(4)).** In the alternative, the common questions of fact and law, set forth in Paragraph 79, are appropriate for issue certification on behalf of the proposed Class.

VII. CAUSES OF ACTION

COUNT ONE
Violation of the Federal Wiretap Act,
18 U.S.C. §§ 2510, *et seq.*
(On Behalf of Plaintiffs and the Class Against All Defendants)

481. Plaintiffs repeat and fully incorporate all preceding paragraphs as if fully set forth herein.

482. 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.

483. 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).

484. 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).

485. 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).

486. 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).

487. 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).

488. 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).

489. 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).

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

491. Defendants are each a person as defined in 18 U.S.C. §2510(6).

492. The data and transmissions within and from Plaintiffs' 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. As the sensors in Plaintiffs' devices generated data to be analyzed by and stored within their devices (for Plaintiffs' benefit) or to be sent to the servers of the application developer, the Arity SDK intercepted and siphoned that data and diverted it to Defendants.

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

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

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

496. 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.

497. 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).

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

499. As a result, Plaintiffs 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.

500. Pursuant to 18 U.S.C. § 2520, Plaintiffs 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 TWO
Violation of the Computer Fraud and Abuse Act,
18 U.S.C. §§ 1030, *et seq.*
(On Behalf of Plaintiffs and the Class Against All Defendants)

501. Plaintiffs repeat and fully incorporate all preceding factual allegations as if fully set forth herein.

502. 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).

503. 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).

504. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality and privacy of information within their computers.

505. 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).

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

507. 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).

508. "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).

509. Plaintiffs and Class Members' mobile devices 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).

510. 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). Plaintiffs' and Class Members' mobile devices 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).

511. Through their SDK embedded in third party apps, Defendants intentionally accessed the Plaintiffs' and Class Members' mobile devices 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). Plaintiffs and Class Members did not authorize Defendants to access any information at all on their cell phones.

512. Plaintiffs and Class Members have suffered harm and injury due to Defendants' unauthorized access to the communications containing their private and personal information.

513. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I) from the unauthorized access and collection of Driving Data to Plaintiffs and Class Members and excessive

insurance costs. 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 THREE
Willful Violation of the Fair Credit Reporting Act,
15 U.S.C. §§ 1681, *et seq.*
(On Behalf of Plaintiffs and the FCRA Subclass Against the Arity Defendants)

514. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

515. Plaintiffs bring this claim on their own behalf and on behalf of each member of the FCRA Subclass described above against the Arity Defendants.

516. Plaintiffs and FCRA Subclass Members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

517. Under the FCRA, a "consumer reporting agency" includes any person which, for monetary fees or on a cooperative nonprofit basis, regularly engages, in whole or in part, in the practice of assembling or evaluating consumer credit information or other consumer information for the purpose of furnishing "consumer reports" to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. At all relevant times, the Arity Defendants were consumer reporting agencies. 15 U.S.C. § 1681a(f).

518. Under the FCRA, a "consumer report" is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used, expected to be used, or collected, in whole or in part, for the purpose of

serving as a factor in establishing the consumer's eligibility for (i) credit or insurance to be used primarily for personal, family, or household purposes, (ii) employment purposes, or (iii) any other purpose authorized by 15 U.S.C. § 1681b. At all relevant times, the Arity Defendants had compiled and maintained "consumer reports" on Plaintiffs and FCRA Subclass Members. 15 U.S.C. § 1681a(d)(1).

519. As consumer reporting agencies, the Arity Defendants are and were required to identify, implement, maintain, and monitor systems to ensure the accuracy of consumer information in its possession, custody, and control, including Plaintiffs' and FCRA Subclass Members' Driving Data.

520. The Arity Defendants obtain driver behavior data from Defendants and furnish it to third parties, including automobile insurers, for many purposes outside of insurance such as marketing and analytics, without Plaintiffs' and other FCRA Subclass Members' full knowledge and consent. For example, the Arity Defendants describe their own "Arity Audiences" and "Arity Marketing Platform" products and services as tailored to providing data useful for targeted advertising – not for insurance underwriting. The Arity Defendants at all times knew that Plaintiffs and the FCRA Subclass Members did not provide consent for collection, use, and sale of their Driving Data, including for marketing and analytics purposes.

521. The Arity Defendants' provision of credit information that includes driver behavior data to third parties, including automobile insurance companies, constitutes the furnishing of consumer reports under the FCRA and an impermissible purpose and use of data under the FCRA.

522. The FCRA requires credit reporting agencies to adopt reasonable procedures to ensure the "maximum possible accuracy" of the consumer credit information it furnishes. 15 U.S.C. § 1681e(b).

523. The Arity Defendants act as consumer reporting agencies, as defined by 15 U.S.C. § 1681(c)(1), but have failed to implement procedures to maintain "maximum possible accuracy" regarding Plaintiffs' and FCRA Subclass Members' Driving Data.

524. The Arity Defendants have knowingly and willfully engaged in the collection and production of inaccurate data metrics regarding Plaintiffs' and FCRA Subclass Members' driving abilities. Those actions have included, among other things as alleged herein:

a. Adopting and implementing systems which misreport Driver Data and as being associated with one individual, when that information should be associated with other individuals;

b. Continuing to misreport Driver Data and Identity Information even when the Arity Defendants know that the systems they developed to collect and report such information is prone to errors, does not correctly report Driver Data, provides no context for certain Driver Data, and is not subject to review to ensure that the Driver Data is correct;

c. Preparing reports which the Arity Defendants knew, or were reckless in not knowing, that the Driver Data included therein was inaccurate.

525. As a result of the Arity Defendants' conduct, insurance carriers and other third parties who view these consumer reports receive and in turn rely on an inaccurate representation of Plaintiffs' and FCRA Subclass Members' driving abilities.

526. The foregoing deceptive acts and practices constitute reckless and/or negligent violations of the FCRA, including, but not limited to, 15 U.S.C. § 1681e(b).

527. As a result of each and every willful violation of the FCRA, Plaintiffs are entitled to actual damages as the Court may allow pursuant to 15 U.S.C. § 1681n(a)(1); statutory damages

pursuant to 15 U.S.C. § 1681n(a)(1); punitive damages as the Court may allow pursuant to 15 U.S.C. § 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681n(a)(3) from the Arity Defendants.

528. As a result of each and every negligent noncompliance of the FCRA, Plaintiffs and FCRA Subclass Members are entitled to actual damages as the Court may allow pursuant to 15 U.S.C. § 1681o(a)(1); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. § 1681o(a)(2) from the Arity Defendants.

COUNT FOUR
Violations of Common Law Right to Privacy
(On Behalf of Each Plaintiff for the State They Reside In and the Members of the Respective State Subclass Against All Defendants)

529. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

530. Common law prohibits Defendants from intentional intrusion into the personal matters of Plaintiffs and Class Members, including their PII, driver behavior information, and location.

531. Plaintiffs and Class Members hold, and at all relevant times held, a legally protected privacy interest in their PII and other personal data and are entitled to the protection of private property, matters, and information therein from intentional intrusions and unauthorized access.

532. As Plaintiffs and Class Members used and carried their phones, visiting family and going about their days, they have unknowingly created troves of highly sensitive data mapping of their respective personal lives which is then collected, captured, transmitted, accessed, compiled, stored, analyzed, and sold—all without their knowledge or informed consent.

533. The private Information of Plaintiffs and Class Members consists of PII and other personal data that were never intended to be shared to third parties.

534. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy regarding their PII and other personal data and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

535. Defendants intentionally invaded Plaintiffs' and Class Members' privacy interests by deliberately designing devices and programs that surreptitiously obtain, improperly gain knowledge of, review, retain, package, and sell their PII and other data.

536. Defendants' unauthorized acquisition and collection of Plaintiffs' and Class Members' PII and other personal data, is highly offensive to a reasonable person. 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. It is not simply an intentional intrusion but a profound and egregious infringement upon the most personal and sacred aspects of one's life. Plaintiffs have unknowingly been subjected to constant observation while they go about their days, which destabilizes the very essence of personal liberty. This unceasing, detailed, comprehensive, and silent collection of data – including data not perceptible to the naked eye – for profile-building purposes far exceeds what any Plaintiff or Class Member reasonably understood another motorist or passerby might notice about Class Members' behavior by virtue of being on the road or out in public.

537. Defendants' conduct exploited Plaintiffs' phone in order to record and transmit Plaintiffs' highly sensitive and personally identifiable data and behavior.

538. Defendants' willful and intentional use of Plaintiffs' and Class Members' PII and other personal data constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns of a kind that would be highly offensive to a reasonable person.

539. Defendants intentionally and willfully acquired Plaintiffs' data, Defendants had notice and knew that its practices would cause injury to Plaintiffs and Class Members.

540. Defendants' conduct constitutes and, at all relevant times, constituted serious and highly offensive invasions of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would record, collect, capture, sell, take and make use of—and allow third-party companies to take and make use of Plaintiffs' and Class Members' PII and other personal data.

541. Defendants profited from Plaintiffs' and Class Members' data without compensating them, and often inaccurately reporting on Plaintiffs' and Class Members' driving abilities and history to third parties. Plaintiffs and Class Members did not receive any compensation in return for the improper use of their personal data. Defendants deprived Plaintiffs and Class Members of the right to control how their personal information is collected, used, or disseminated and by whom.

542. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, loss of time, money, and opportunity costs, plus prejudgment interest, and costs.

543. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information is still maintained by Defendants.

544. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their PII and other personal data. A judgment for monetary damages will not undo Defendants' disclosure of the information to third parties, who on information and belief, continue to possess and utilize that information.

545. Plaintiffs, on behalf of themselves and Class Members, further seek injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiffs' and Class members' PII and other data and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT FIVE
Intrusion Upon Seclusion
(On Behalf of Plaintiffs and the Class Against All Defendants)

546. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

547. Plaintiffs and Class Members have reasonable expectations of privacy in their mobile phones, vehicles, and with their movements, generally. Plaintiffs' and Class Members' private affairs include their locations.

548. The reasonableness of such expectations of privacy is supported by Defendants' unique position to monitor Plaintiffs' and Class Members' behavior through their access to Plaintiffs' and Class Members' mobile phone location data through the inclusion of their SDK in certain apps unbeknownst to Plaintiffs. It is further supported by the surreptitious and non-intuitive nature of Defendants' tracking practices. The unceasing, detailed, comprehensive, and silent collection of data – including data not perceptible to the naked eye – for profile-building purposes far exceeds what any Plaintiff or Class Member reasonably understood another motorist or passerby might notice about Class Members' driving behavior by virtue of driving on the road with other people.

549. Defendants intentionally intruded on and into Plaintiffs' and Class Members' solitude, seclusion, or private affairs by intentionally collecting and transmitting information via the SDK installed in their mobile phones.

550. These intrusions are highly offensive to a reasonable person.

551. Plaintiffs and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

552. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiffs and Class Members.

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

COUNT SIX
Unjust Enrichment (Quasi-Contract Claim for Restitution and Disgorgement) or, Alternatively, Breach of Contract
(On Behalf of Plaintiffs and the Class Against All Defendants)

554. Plaintiffs hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

555. Plaintiffs bring this claim on their own behalf and on behalf of Class Members.

556. Plaintiffs and Class Members unwittingly conferred a benefit upon Defendants.

557. Defendants collected and sold Plaintiffs' and Class Members' Personal Data, without Plaintiffs' and Class Members' consent to insurance companies and to other third parties and also used it to build products and services to further sell. Defendants also used this data to evaluate insurance premiums and coverage.

558. Defendants were enriched when they utilized Plaintiffs' and Class Members' location information, gathered without consent, for their own financial advantage to sell in raw

form, or use to create reports or other analyses for sale, including, but not limited to, reports of Plaintiffs' and Class Members' driving behaviors for automobile insurers.

559. In exchange for Plaintiffs' and Class Members' loss of privacy and the financial benefits Defendants enjoyed as a result thereof, including, but not limited to, profits from the sale of the location data, and reports based on that location data, Plaintiffs and Class Members received nothing.

560. Plaintiffs and Class Members received no benefit from this use and sale of their Personal Data. Plaintiffs and Class Members would have expected to receive compensation for providing this data to a data broker who uses such data for profit. But, because Plaintiffs and Class Members did not consent to Defendants' collection and sale of Plaintiffs' and Class Members' Personal 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 Plaintiffs and Class Members for the value of their Personal Data.

561. Alternatively, to the extent Defendants successfully assert that any terms of service from a binding contract that sufficiently defines the parties' rights regarding Defendants' use of Plaintiffs' and Class Members' location information, thereby rendering a claim for unjust enrichment unavailable (which Plaintiffs deny in the first instance), then Plaintiffs allege that Defendants' conduct constitutes a breach of any such binding contract, including, but not limited to, the covenant of good faith and fair dealing implied into every contract. Defendants did not adequately disclose prior to collecting or selling Plaintiffs' and Class Members' mobile phone location and driving behavior data that it would or could be sold to automobile insurance companies with whom Plaintiffs and Class Members had an ongoing, or prospective relationship. By virtue of Defendants' conduct as alleged herein, including the sale of Plaintiffs' and Class

Members' location information without adequate disclosure beforehand, Defendants breached the covenant of good faith and fair dealing implied into every contract, including any applicable terms of service.

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

COUNT SEVEN
Violation of the Alabama Deceptive Trade Practices Act,
Ala. Code §§ 8-19-1, *et seq.*
(On Behalf of the Alabama Plaintiff and the Alabama Subclass Against All Defendants)

563. Plaintiff Kilgo (for the purposes of this count, the "Alabama Plaintiff"), individually and on behalf of the Alabama Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

564. Alabama Plaintiff brings this claim on his own behalf and on behalf of each member of the Alabama Subclass described above.

565. Alabama Plaintiff and the Alabama Subclass Members are each a "consumer" as defined in Ala. Code § 8-19-3.

566. Defendants are each a "person" as defined by Ala. Code § 8-19-3.

567. Alabama Plaintiff sent pre-suit notice pursuant to Ala. Code § 8-19-10(e).

568. Defendants are each engaged in "trade or commerce" affecting the people of Alabama by advertising, offering for sale, selling, or distributing goods and services in the State of Alabama. *See* Ala. Code § 8-19-3.

569. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Ala. Code § 8-19-3.

570. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Ala. Code § 8-19-5, including:

a. Intercepting, collecting, using, and selling Alabama Plaintiff's and Alabama Subclass Members' data, including driving data, without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Alabama Plaintiff's and Alabama Subclass Members' data, including driving data, to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that other third parties collected, manipulated, used, and sold Alabama Plaintiff's and Alabama Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and the associated mobile applications with respect to the privacy of consumers;

e. Misrepresenting the purpose of the SDK and that it would protect the privacy of Alabama Plaintiff's and the Alabama Subclass Members' data, including that it would not intercept, collect, use or sell such data; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Alabama Plaintiff's and Alabama Subclass Members' data, including driving data.

571. These statements, misrepresentations, omissions, and concealments constitute violations of Ala. Code § 8-19-5 (5), (7), (9) and (27).

572. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Alabama Plaintiff's and Alabama Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Alabama Plaintiff's and Subclass Members' data without obtaining their consent.

573. The fact that Defendants intercepted, collected, used, and sold Alabama Plaintiff's and Alabama Subclass Members' data was material to Alabama Plaintiff and Alabama Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

574. Alabama Plaintiff and Alabama Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of the SDK and associated applications, the security and privacy of their data, and their privacy, to their detriment.

575. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging the conduct alleged herein, including by harvesting, selling, and disseminating Alabama Plaintiff and Alabama Subclass Members' data without Plaintiff's and Subclass Members' consent.

576. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Alabama Plaintiff and Alabama Subclass Members have suffered and

will continue to suffer injury, including, but not limited to, the loss of privacy, the unauthorized dissemination of their valuable data, and economic harm stemming from Defendants' exploitation of their data.

577. Defendants' unconscionable and unfair acts and practices caused substantial injury to Alabama Plaintiff and Alabama Subclass Members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

578. Alabama Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

COUNT EIGHT
Violation of the Arizona Consumer Fraud Act,
Ariz. Rev. Stat. §§ 44-1521, *et seq.*
(On Behalf of the Arizona Plaintiff and the Arizona Subclass Against All Defendants)

579. Plaintiff Gable (for the purposes of this count, the "Arizona Plaintiff"), individually and on behalf of the Arizona Subclass, hereby repeats and incorporates by reference each preceding paragraph as if fully stated herein.

580. Arizona Plaintiff brings this claim on her own behalf and on behalf of each member of the Arizona Subclass described above.

581. Arizona Plaintiff and members of the Arizona Subclass are each a "person" as defined by Ariz. Rev. Stat. § 44-1521.

582. Defendants are each a "person" as defined by Ariz. Rev. Stat. § 44-1521.

583. Defendants are each engaged in trade directly or indirectly affecting the people of Arizona by advertising, offering for sale, selling or distributing goods and services in the State of Arizona. *See* Ariz. Rev. Stat. § 44-1521.

584. Defendants are engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of Arizona Revised Statute § 44-1522(A), including:

a. Intercepting, collecting, using, and selling Arizona Plaintiff's and Arizona Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Arizona Plaintiff's and Arizona Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants collected, manipulated, used, and sold Arizona Plaintiff's and Arizona Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of the SDK and associate applications with respect to the privacy of consumers;

e. Misrepresenting the purpose of their SDK and associated applications, and that it would protect the privacy of Arizona Plaintiff's and the Arizona Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Arizona Plaintiff's and Subclass Members' data.

585. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Arizona Plaintiff's and Arizona Subclass Members' rights, because

Defendants intentionally intercepted, collected, used, and sold Arizona Plaintiff's and Arizona Subclass Members' Driving data without obtaining their consent.

586. The fact the Defendants intercepted, collected, used and sold Arizona Plaintiff's and Arizona Subclass Members' data was material to Arizona Plaintiff and Arizona Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download, or use an application.

587. Arizona Plaintiff and Arizona Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of their SDK and associated mobile applications, the security and privacy of their data, and their privacy while going about their day, to their detriment.

588. Arizona Plaintiff's and the Arizona Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Arizona Plaintiff's and Arizona Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

589. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Arizona Plaintiff and Arizona Subclass Members have suffered and will continue to suffer injury, including, but not limited to, the loss of privacy, the unauthorized dissemination of their valuable data, and economic harm stemming from Defendants' exploitation of their data.

590. Arizona Plaintiff and Arizona Subclass Members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

COUNT NINE
Violation of the California Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502
(On Behalf of the California Plaintiffs and the California Subclass Against All Defendants)

591. Plaintiffs Azar, Bare, Duffield, Hernandez, Jackson, Mahoney, Malvar, and Streifel (for the purposes of this count, the "California Plaintiffs"), individually and on behalf of the California Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

592. California Plaintiffs bring this claim on their own behalf and on behalf of each member of the California Subclass described.

593. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The enactment of CDAFA was motivated by the finding that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . unauthorized access to computers, computer systems, and computer data." *Id.*

594. The CDAFA provides a private right of action to the "owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subsection (c)." Cal. Penal Code § 502(a).

595. California Plaintiffs' and California Subclass Members' smartphones constitute "computers" within the scope of the CDAFA.

596. Defendants violated the following sections of the CDAFA:

a. Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network

in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

b. Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; and

c. Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

597. Defendants knowingly accessed California Plaintiffs' and California Subclass Members' smartphones without their permission by including within the SDK that Defendants provide to app developers software that intercepts and transmits data, communications, and personal information concerning California Plaintiffs and California Subclass Members.

598. Defendants took, copied, intercepted, and made use of data, communications, and personal information from California Plaintiffs' and California Subclass Members' smartphones.

599. Defendants used data, communications, and personal information that they intercepted and took from California Plaintiffs' and California Subclass Members' smartphones to wrongfully and unjustly enrich themselves at the expense of California Plaintiffs and California Subclass Members.

600. Defendants knowingly and without California Plaintiffs' and California Subclass Members' permission accessed, or caused to be accessed, their smartphones by installing, without

California Plaintiffs' and California Subclass Members' consent, software that intercepts and/or takes data, communications, and personal information concerning the California Plaintiffs and California Subclass Members. California Plaintiffs and California Subclass Members never authorized Defendants to access any information at all on their smartphones.

601. California Plaintiffs and California Subclass Members are residents of California and used their smartphones in California. Defendants accessed or caused to be accessed California Plaintiffs' and California Subclass Members' Personal Driving Data and personal information from California. On information and belief, Defendants uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning California Plaintiffs and California Subclass Members.

602. Defendants were unjustly enriched by intercepting, acquiring, taking, or using California Plaintiffs' and California Subclass Members' data, communications, and personal information without their permission, and using it for Defendants' own financial benefit. Defendants have been unjustly enriched in an amount to be determined at trial.

603. As a direct and proximate result of Defendants' violations of the CDAFA, California Plaintiffs and California Subclass Members suffered damages.

604. Pursuant to CDAFA Section 502(e)(1), California Plaintiffs and California Subclass Members seek compensatory, injunctive, and equitable relief in an amount to be determined at trial.

605. Pursuant to CDAFA Section 502(e)(2), California Plaintiffs and California Subclass Members seek an award of reasonable attorneys' fees and costs.

606. Pursuant to CDAFA Section 502(e)(4), California Plaintiffs and California Subclass Members seek punitive or exemplary damages for Defendants' willful violations of the CDAFA.

COUNT TEN
California Constitutional Invasion of Privacy
(On Behalf of the California Plaintiffs and the California Subclass Against All Defendants)

607. Plaintiffs Azar, Bare, Duffield, Hernandez, Jackson, Mahoney, Malvar, and Streifel (for the purposes of this count, the "California Plaintiffs"), individually and on behalf of the California Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

608. California Plaintiffs bring this claim on their own behalf and on behalf of each member of the California Subclass described above.

609. 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.

610. California Plaintiffs and California Subclass Members have an interest in precluding the dissemination and misuse of their driving data by Defendants, and using their personal property without observation, intrusion, or interference by Defendants.

611. California Plaintiffs and California Subclass Members had no knowledge and did not consent or authorize Defendants to obtain their driving data or to share it with third parties and with each other, let alone to use that data in determining insurance coverage and pricing.

612. California Plaintiffs and California Subclass Members enjoyed objectively reasonable expectations of privacy surrounding their driving telematics data. The unceasing, detailed, comprehensive, and silent collection of such data – including data not perceptible to the

naked eye – for profile-building purposes far exceeds what any California Plaintiff and California Subclass Member reasonably understood another motorist or passerby might notice about Class Members' driving behavior by virtue of being on a public highway.

613. Defendants' intrusion upon seclusion occurred the moment Defendants began tracking California Plaintiffs and California Subclass Members' driving data.

614. Defendants' conduct was intentional and intruded on California Plaintiffs' and California Subclass Members' use of their personal property.

615. Defendants' conduct was highly offensive to a reasonable person because they shared and/or sold the data to auto insurance companies to influence California Plaintiffs' and California Subclass Members' insurance rates without their prior knowledge or consent.

616. As a direct and proximate result of Defendants' invasions of privacy, California Plaintiffs and California Subclass Members have suffered and will continue to suffer injury and damages, as alleged herein, including but not limited to overpayment for auto insurance services and decreased value of their driving telematics data.

617. California Plaintiff and California Subclass Members seek all relief available for invasion of privacy claims under the California Constitution, including nominal damages and general privacy damages.

COUNT ELEVEN
Violation of the California Invasion of Privacy Act – Wiretapping Act,
Cal. Penal Code §§ 630, *et seq.*
(On Behalf of the California Plaintiffs and the California Subclass Against All Defendants)

618. Plaintiffs Azar, Bare, Duffield, Hernandez, Jackson, Mahoney, Malvar, and Streifel (for the purposes of this count, the "California Plaintiffs"), individually and on behalf of the California Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

619. California Plaintiffs bring this claim on their own behalf and on behalf of each member of the California Subclass described.

620. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

621. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

622. The California legislature was motivated to enact CIPA by a concern that the "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." *Id.*

623. Cal. Penal Code § 632 prohibits eavesdropping upon or recording of any confidential communication, including those occurring among the parties in the presence of one another or by means of a telephone, telegraph, or other device, through the use of an electronic amplifying or recording device without the consent of all parties to the communication.

624. Cal. Penal Code § 631(a) prohibits:

> any person [from using] any machine, instrument, [] contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or 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.

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

626. California Plaintiffs' and California Subclass Members' specific user input events and choices on their mobile devices that are tracked by Defendants' SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the California Wiretapping Act.

627. The transmissions of information from California Plaintiffs' and California Subclass Members' mobile device sensors within California Plaintiffs' and California Subclass Members' mobile devices, and to the servers of third-party app developers, constitute communications within the meaning of the California Wiretapping Act.

628. California Plaintiffs' and California Subclass Members are residents of California and used their smartphones within California. As such, Defendants intercept, read, or attempt to read California Plaintiffs' and California Subclass Members' data, communications, and personal information in California.

629. On information and belief, Defendants use servers in California to intercept, track, process, or otherwise use California Plaintiffs' and California Subclass Members' data, communications, and personal information within California.

630. Defendants intercept California Plaintiffs' and California Subclass Members' communications while they are in transit within and from California Plaintiffs' and California Subclass Members' smartphones and the apps, app developers, and cellphone towers; Defendants transmit a copy of California Plaintiffs' and California Subclass Members' communications to themselves. As the sensors in California Plaintiffs' and California Subclass Members' devices generated data to be analyzed by and stored within their devices (for plaintiffs' benefit) or to be sent to the servers of the application developer, the Arity SDK intercepted and siphoned that data

and diverted it to Defendants. Defendants use the contents of the communications to sell to third parties and in other methods for their own pecuniary gain.

631. Neither Defendants nor any other person informed California Plaintiffs and California Subclass Members that Defendants were intercepting and transmitting California Plaintiff's and California Subclass Members' private communications. California Plaintiffs and California Subclass Members did not know Defendants were intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendants and thereafter transmitted to others.

632. Defendants' SDK constitutes a machine, instrument, contrivance, or other manner to track and intercept California Plaintiffs' and California Subclass Members' communications while they are using their smartphones.

633. Defendants use and attempt to use or communicate the meaning of California Plaintiffs' and California Subclass Members' communications by ascertaining their personal information, including their Personal Driving Data and places that they have visited, in order to sell California Plaintiffs' and California Subclass Members' personal information to third parties.

634. Specifically, Defendants have used the information derived from the communications described above to create products they market, license, and sell, including driving scores, risk ratings, and access to databases containing Plaintiffs' and California Subclass Members' data.

635. Further, Defendants have used the information derived from the communications described above for their own financial and commercial benefit, obtaining substantial profit.

636. Specifically, Defendants knew or should have known that the detailed information they used and sold was captured in secret in violation of the Act for the following reasons, among others that will become known through discovery:

a. The opaque disclosures in Defendants' various terms and polices, which did not operate as a reasonable basis for inferring consumer consent to share the information with third parties;

b. The lack of public knowledge about Defendants' collection and sharing practices until at least January 2025;

c. The fact that Defendants continue to collect after it was publicized that collection was secret/happening without consent or knowledge; and

d. The nature of the data as such that it had to be obtained via a wiretap.

637. At all relevant times to this complaint, Defendants intercepted and recorded components of California Plaintiffs' and California Subclass Members' private telephone communications and transmissions when California Plaintiffs and California Subclass Members accessed Defendants' software via their cellular mobile access devices within the State of California.

638. At all relevant times to this complaint, California Plaintiffs and the California Subclass Members did not know Defendants were engaging in such interception and recording and therefore could not provide consent to have their Personal Data intercepted and recorded by Defendants and thereafter transmitted to others.

639. At the inception of Defendants' illegally intercepting and storing the Personal Driving Data, Defendants never advised California Plaintiffs or the other California Subclass

Members that any part of this sensitive Personal Data would be intercepted, recorded, and transmitted to third parties.

640. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5–6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

641. Defendants' use of MAIDs and its SDK are both a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

642. At all relevant times, by using Defendants' MAID software and SDK as well as tracking California Plaintiffs' and California Subclass Members' geolocation and Personal Driving Data, Defendants intentionally tapped, electrically or otherwise, the lines of internet communication between California Plaintiffs and California Subclass Members on the one hand, and the specific sites and locations California Plaintiffs and California Subclass Members visited on the other.

643. At all relevant times, by using Defendants' geolocation tracking software technology, Defendants willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of California Plaintiffs and putative California Subclass Members,

while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

644. California Plaintiffs and California Subclass Members did not consent to any of Defendants' actions in implementing these wiretaps. Nor have California Plaintiffs or California Subclass Members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of California Plaintiffs' and California Subclass Members' electronic communications.

645. Defendants violated Cal. Penal Code §§ 631 and 632 by knowingly accessing and without permission accessing California Plaintiffs' and California Subclass Members' devices in order to obtain their personal information, including their Personal Driving Data and location data, and in order for Defendants to share that data with third parties, in violation of California Plaintiffs' and California Subclass Members' reasonable expectations of privacy in their devices and data.

646. Defendants violated Cal. Penal Code §§ 631 and 632 by knowingly and without permission intercepting, wiretapping, accessing, taking, and using California Plaintiffs' and California Subclass Members' personally identifiable information and personal communications with others.

647. As a direct and proximate result of Defendants' violation of the Wiretapping Act, California 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.

648. Defendants were unjustly enriched by their violation of the Wiretapping Act. Pursuant to California Penal Code § 637.2, California Plaintiffs and California Subclass Members

have been injured by Defendants' violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT TWELVE
Use of a Pen Register or Trap and Trace Device,
Cal. Penal Code § 638.51
(On Behalf of the California Plaintiffs and the California Subclass Against All Defendants)

649. Plaintiffs Azar, Bare, Duffield, Hernandez, Jackson, Mahoney, Malvar, and Streifel (for the purposes of this count, the "California Plaintiffs"), individually and on behalf of the California Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

650. California Plaintiffs bring this claim on their own behalf and on behalf of each member of the California Subclass described above.

651. California Penal Code § 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

652. California Penal Code § 638.51 prohibits any person from using a pen register without a court order.

653. Defendants' SDK constitutes a "pen register" because it is a device or process that records addressing or signaling information—California Plaintiffs' and Class Members' location data and personal information—from the electronic communications transmitted by their smartphones.

654. Defendants were not authorized by any court order to use a pen register to track California Plaintiffs' and Class Members' location data and personal information.

655. As a direct and proximate result of Defendants' conduct, California Plaintiffs and Class Members suffered losses and were damaged in an amount to be determined at trial.

COUNT THIRTEEN
Violation of the California Unfair Competition Law ("UCL"),
Cal. Bus. & Prof. Code §§ 17200, *et seq.*
(On Behalf of the California Plaintiffs and the California Subclass Against All Defendants)

656. Plaintiffs Azar, Bare, Duffield, Hernandez, Jackson, Mahoney, Malvar, and Streifel (for the purposes of this count, the "California Plaintiffs"), individually and on behalf of the California Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

657. California Plaintiffs bring this claim on their own behalf and on behalf of each member of the California Subclass described above.

658. Defendants are "persons" as defined by Cal. Bus. & Prof. Code § 17201.

659. Defendants violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

660. Defendants have engaged in "unlawful" business practices by violating California common law and California constitutional right to privacy.

661. Defendants violated, and continue to violate, the "unfair" prong of the UCL because they took California Plaintiffs' and the California Subclass Members' Personal Data and used this data for undisclosed purposes, including sharing this information with undisclosed third parties. Defendants' statements to consumers were so hidden, misleading, confusing, deceptive, and opaque that no reasonable consumer would have understood the extent of the Personal Data collection if the consumer understood Defendants were collecting it at all. Plaintiffs' Personal Data is property under the laws of California and common law. The Defendants' use of this Data also caused Plaintiffs to overpay for auto insurance services. Defendants' unlawful taking and use of

this property was immoral, unethical, oppressive, unscrupulous and substantially injurious to California Plaintiffs and the California Subclass. Defendants' unauthorized collection and disclosure of Plaintiffs' Personal Data was made for their own gain and at the expense of California Plaintiffs and the California Subclass.

662. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because they failed to inform California Plaintiffs and the California Subclass that Defendants were collecting their Personal Data, or purported to do so in a manner so misleading, confusing, deceptive, and opaque that no reasonable consumer would have understood the extent of the Personal Data collection. Defendants failed to disclose or did not meaningfully disclose that its SDK and associated applications, intercepted, collected, used, and disseminated Plaintiffs' and California Subclass Members' data, or that Defendants profited from the dissemination, sale, and use of such data. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the true function and purposes of Defendants' products and services. Reasonable consumers lack the means to verify Defendants' representations and omissions concerning the SDK's, and associated mobile applications, data collection practices, or to understand the fact or significance of Defendants' practices concerning the collection, dissemination and use of Plaintiffs' and California Subclass Members' data.

663. As a direct and proximate result of Defendants' unfair, unlawful, and fraudulent acts and practices, California Plaintiffs and California Subclass Members were injured and suffered damages, as alleged herein, including but not limited to invasion of privacy; overpayment for auto insurance services; and decreased value of their driving telematics data.

664. Defendants acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded California Plaintiffs' and California Subclass Members' rights.

665. California Plaintiffs and California Subclass Members seek all monetary relief allowed by law, including restitution of all profits stemming from Defendants' unfair, unlawful, and fraudulent business practices and reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5. California Plaintiffs and the California Subclass are entitled to restitution as the available damages remedies are inadequate to return to California Plaintiffs and the California Subclass the value of the information taken by Defendants. California Plaintiffs and the California Subclass are entitled to restitution for Defendants' unjust enrichment in a quanta that is not identical to the legal damages suffered.

666. Further, California Plaintiffs and the California Subclass lack an adequate remedy at law and are thus entitled to seek equitable relief. Unless restrained and enjoined, Defendants will continue to misrepresent their data practices and will not recall and destroy all wrongfully collected data. Due to the ongoing nature of the harm, damages will be insufficient to address it. Thus, injunctive relief is appropriate.

COUNT FOURTEEN
Violation of the Florida Security of Communications Act ("FSCA"),
Fla. Stat. §§ 934.01, *et seq.*
(On Behalf of the Florida Plaintiff and the Florida Subclass Against All Defendants)

667. Plaintiff Wright (for the purposes of this count, the "Florida Plaintiff"), individually and on behalf of the Florida Subclass, repeat and reallege the preceding paragraphs as if fully alleged herein.

668. Florida Plaintiff brings this claim on her own behalf and on behalf of each member of the Florida Subclass described above.

669. The Florida Security of Communications Act ("FSCA"), Fla. Stat. §§ 934.01, *et seq.*, states that any person who"[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication" is subject to liability. Fla. Stat. § 934.03(1)(a).

670. Florida Plaintiff, members of the Florida Subclass, and Defendants each constitute a "person" as defined in Fla. Stat. § 934.02.

671. The data and transmissions within, to, and from Florida Plaintiff's and Class Members' vehicles constitute "electronic communications," as defined by Fla. Stat. § 934.02, as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic or photooptical systems that affect intrastate, interstate or foreign commerce.

672. The FSCA prohibits any person from intentionally disclosing, or endeavoring to disclose, to any other person "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the FSCA]." Fla. Stat. Ann. § 934.03(c).

673. The FSCA prohibits any person from intentionally using, or endeavoring to use, "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the FSCA.]" Fla. Stat. Ann. § 934.03(d).

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

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

Florida Subclass Members have a reasonable expectation of privacy within their vehicles, and Florida Plaintiff and Florida Subclass Members reasonably expected privacy while driving their vehicles, in their homes, and in their doctor's office. Further, there is a reasonable expectation that the interactions between a driver and their phone, including their personal data, are private.

676. Defendants intercepted these electronic communications in real time separately from and in addition to accessing data stored in Florida Plaintiff's and Florida Subclass Members' MAIDs.

677. Defendants intercepted these data transmissions by diverting them, during flight, to their own servers, unbeknownst to Florida Plaintiff and Florida Subclass Members.

678. As detailed herein, the electronic communications detailed above that Defendants intercepted are tied to individuals and vehicles, and are not anonymized.

679. In further violation of the FSCA, Defendants have disclosed or attempted to disclose to third parties the contents of the communications described above while knowing or having reason to know that the information was obtained through interception in violation of the FSCA.

680. In further violation of the FSCA, Defendants have used or attempted to use the contents of the communications described above while knowing or having reason to know that the information was obtained through interception in violation of the FSCA.

681. In further violation of the FSCA, Defendants have used the information derived from the communications described above to create products they market, license, and sell, including so-called driving scores, risk ratings, and access to databases containing Florida Plaintiff's and the Florida Subclass Members' data.

682. Upon information and belief, Defendants continue to disclose and use unlawfully obtained data, including driving data, for their own financial gain.

683. Florida Plaintiff and Florida Subclass Members did not consent or otherwise authorize Defendants to intercept, disclose, or use their communications.

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

685. Defendants' violations of the FSCA have directly and proximately caused Florida Plaintiff and the Florida Subclass to suffer harm and injury due to the interception, disclosure, and/or use of their private and personal information in an amount to be ascertained at trial.

686. Pursuant to Fla. Stat. § 934.10(1), Florida Plaintiff and Florida Subclass Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the FSCA and are entitled to: (1) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Florida Plaintiff and the Florida Subclass or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT FIFTEEN
Violation of the Florida Unfair and Deceptive Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et seq.*
(On Behalf of the Florida Plaintiff and the Florida Subclass Against All Defendants)

687. Plaintiff Wright (for the purposes of this count, the "Florida Plaintiff"), individually and on behalf of the Florida Subclass, repeat and reallege the preceding paragraphs as if fully alleged herein.

688. Florida Plaintiff brings this claim on her own behalf and on behalf of each member of the Florida Subclass described above.

689. The Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. §§ 501.201, *et seq.*, prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce[.]" Fla. Stat. § 501.204.

690. Florida Plaintiff and the members of the Florida Subclass are each a "consumer" as defined in Fla. Stat. Ann. § 501.203.

691. Defendants are each a "person" as defined in Fla. Stat. Ann. § 504.203.

692. Defendants each engaged in "trade or commerce" affecting the people of Florida by advertising, offering for sale, selling or distributing goods and services in the State of Florida. Fla. Stat. Ann. § 501.203.

693. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of the FDUTPA by:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding;

e. Failing to comply with common law and/or statutory duties pertaining to the privacy of Florida Plaintiff's and Florida Subclass Members' data.

694. These deceptive statements, misrepresentations, omissions, concealments and acts constitute violations of Fla. Stat. 7 501.204(1).

695. Defendants acted intentionally, knowingly, and maliciously to violate FDUTPA, and recklessly disregarded Florida Plaintiff's and Florida Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Florida Plaintiff's and Florida Subclass Members' data without obtaining their consent.

696. The fact that Defendants intercepted, collected, used, and sold Florida Plaintiff's and Florida Subclass Members' data was material to Florida Plaintiff and Florida Subclass Members. This is a fact that reasonable consumers would consider important when choosing download, use, or purchase an application.

697. Florida Plaintiff and Florida Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of their SDK, the security and privacy of their data, and their privacy in their own vehicles to their detriment.

698. Florida Plaintiff's and the Florida Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Florida Plaintiff's and Florida Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

699. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Florida Plaintiff and Florida Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal

information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

700. Florida Plaintiff and Florida Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT SIXTEEN
Violation of the Georgia Uniform Deceptive Trade Practices Act,
Ga. Code Ann. §§ 10-1-370, *et seq.*
(On Behalf of the Georgia Plaintiff and the Georgia Subclass Against All Defendants)

701. Plaintiff Kelley (for the purposes of this count, the "Georgia Plaintiff"), individually and on behalf of the Georgia Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

702. Georgia Plaintiff bring this claim on her own behalf and on behalf of each member of the Georgia Subclass described above.

703. Defendants, Georgia Plaintiff, and Georgia Subclass Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

704. Defendants engaged in deceptive trade practices in the conduct of its business in violation of Ga. Code § 10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

705. Defendants engaged in unfair, unconscionable, unlawful, and/or deceptive acts and practices in conducting trade and commerce in violation of the Georgia UDTPA by:

a. Intercepting, collecting, using, and selling Georgia Plaintiff's and Georgia Subclass Members' data, including driving data, without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Georgia Plaintiff's and Georgia Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and third parties collected, manipulated, used, and sold Georgia Plaintiff's and Georgia Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, particularly Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, particularly Routely, and that it would protect the privacy of Georgia Plaintiff's and the Georgia Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Georgia Plaintiff's and Georgia Subclass Members' data.

706. Defendants acted intentionally, knowingly, and maliciously to violate the Georgia UDTPA, and recklessly disregarded Georgia Plaintiff's and Georgia Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Georgia Plaintiff's and Georgia Subclass Members' data without obtaining their consent.

707. The fact that Defendants intercepted, collected, used, and sold Georgia Plaintiff's and Georgia Subclass Members' data was material to Georgia Plaintiff and Georgia Subclass Members. This is a fact that reasonable consumers would consider important when choosing which applications to download.

708. Georgia Plaintiff and Georgia Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, and the security and privacy of their and data.

709. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants' spent millions of dollars to influence application developers to integrate their SDK that covertly harvested user data demonstrates that Defendants were aware that consumers would not consent to the collection and disclosure of their Data, thus necessitating Defendants' omissions and misrepresentations regarding their actions.

710. Georgia Plaintiff's and the Georgia Subclass' Data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Georgia Plaintiff's and Georgia Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

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

712. Georgia Plaintiff and Georgia Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs under O.C.G.A. § 10-1-373.

COUNT SEVENTEEN
Recovery of Expenses of Litigation,
O.C.G.A. §§ 13-6-11, *et seq.*
(On Behalf of the Georgia Plaintiff and the Georgia Subclass Against All Defendants)

713. Plaintiff Kelley (for the purposes of this count, the "Georgia Plaintiff"), individually and on behalf of the Georgia Subclass, hereby repeat and incorporate by reference each preceding paragraph as if fully stated herein.

714. Georgia Plaintiff bring this claim on their own behalf and on behalf of each member of the Georgia Subclass described above.

715. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

716. Defendants, through its actions alleged and described herein, acted in bad faith, was stubbornly litigious, or caused the Georgia Subclass unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

717. The Georgia Subclass therefore requests that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

COUNT EIGHTEEN
Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§ 505, *et seq.*
(On Behalf of the Illinois Plaintiffs and the Illinois Subclass Against All Defendants)

718. Plaintiffs Monilaw, Quam, Schultz, Slater, and Tucker (for the purposes of this count, the "Illinois Plaintiffs"), individually and on behalf of the Illinois Subclass, repeat and reallege the preceding paragraphs as if fully alleged herein.

719. Illinois Plaintiffs bring this claim on their own behalf and on behalf of each member of the Illinois Subclass described above.

720. Defendants are each a "person" as defined by 815 Ill. Comp. Stat. § 505/1(c).

721. Illinois Plaintiffs and Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. § 505/1(e).

722. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

723. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Intercepting, collecting, using, and selling Illinois Plaintiffs' and Illinois Subclass Members' Driving Data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Illinois Plaintiffs' and Illinois Subclass Members' Driving Data to other third parties for their own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that Defendants and other parties collected, manipulated, used, and sold Illinois Plaintiffs' and Illinois Subclass Members' Driving Data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of the Arity SDK with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of the Arity SDK and that it would protect the privacy of Illinois Plaintiffs' and the Illinois Subclass Members' Driving Data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Illinois Plaintiffs' and Illinois Subclass Members' Driving Data.

724. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Illinois Plaintiffs' and Illinois Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Illinois Plaintiffs' and Illinois Subclass Members' Driving Data without obtaining their consent. The fact that Defendants intercepted, collected, used, and sold Illinois Plaintiffs' and Illinois Subclass Members' Driving Data was material to Illinois Plaintiffs and Illinois Subclass Members. This is a fact that reasonable consumers would consider important when choosing to use a mobile app or in-vehicle app.

725. Illinois Plaintiffs and Illinois Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants misrepresentations and omissions regarding the functionality of the Arity SDK, the security and privacy of their Driving Data, and their privacy in their own vehicles to their detriment.

726. Defendants intended to mislead Illinois Plaintiffs and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

727. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive.

728. Illinois Plaintiffs and the Illinois Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

729. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by inducing Illinois Plaintiffs and Illinois Subclass Members to provide their Driving Data with knowledge that such data was obtained without Illinois Plaintiffs' and Illinois Subclass Members' consent, and further using, selling, and disseminating Illinois Plaintiffs' and Illinois Subclass Members' Driving Data without their consent.

730. Defendants also violated the Act by knowingly taking advantage of Illinois Plaintiffs' and Illinois Subclass Members' inability to reasonably protect their interests, due to their lack of knowledge regarding Defendants' practices, of which Defendants were aware.

731. Illinois Plaintiffs' and the Illinois Subclass Members' Driving Data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Illinois Plaintiffs' and Illinois Subclass Members' Driving Data is in the possession of third parties—who have used and will use such data for their commercial benefit.

732. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Illinois Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, including, but not limited to: loss of privacy; 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.

733. Illinois Plaintiffs and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT NINETEEN
Violation of the Illinois Wiretapping, Electronic Surveillance, and Interception of Communications Law, 720 ILCS 5/14-1, *et seq.*
(On Behalf of the Illinois Plaintiffs and the Illinois Subclass Against All Defendants)

734. Plaintiffs Monilaw, Quam, Schultz, Slater, and Tucker (for the purposes of this count, the "Illinois Plaintiffs"), individually and on behalf of the Illinois Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

735. Illinois Plaintiffs brings this claim on their own behalf and on behalf of each member of the Illinois Subclass described above.

736. The Illinois Eavesdropping Law, 720 ILCS 5/14-1, *et seq.*, prohibits, *inter alia*, any person from knowingly or intentionally "intercept[ing], record[ing], or transcrib[ing], in a surreptitious manner, any private electronic communication" without the consent of all parties. 720 ILCS 5/14-2(a)(3).

737. The Illinois Eavesdropping Law also prohibits any person from using or disclosing "any information which he or she knows or reasonably should know was obtained" in violation of the Act, unless such use or disclosure is done "with the consent of all of the parties." 720 ILCS 5/14-2(a)(5).

738. Defendants are each a "person" within the scope of the Illinois Eavesdropping Law.

739. The data and transmissions within, to, and from Illinois Plaintiffs' and Illinois Subclass Members' vehicles constitute "private electronic communications" as defined by 720

ILCS 5/14-1(e), as they are transfers of signals, data, and intelligence transmitted by electromagnetic, photoelectronic, or photooptical systems.

740. Illinois Plaintiffs and Illinois Subclass Members have a reasonable expectation of privacy within their vehicles, and Illinois Plaintiffs and Illinois Subclass Members reasonably expected privacy while driving their vehicles. Further, there is a reasonable expectation that the interactions between a driver and their vehicle, *i.e.*, their personal Driving Data, are private.

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

742. Defendants intercepted these data transmissions by diverting them to their own servers, unbeknownst to Illinois Plaintiffs and Illinois Subclass Members.

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

744. In further violation of the Illinois Eavesdropping law, Defendants intentionally disclosed or endeavored to disclose to third parties the contents of the private electronic communications described above while knowing or having reason to know that the information was obtained through the interception of the private electronic communications.

745. In further violation of the Illinois Eavesdropping law, Defendants 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 interception in violation of the Act.

746. Defendants have disclosed and used the contents of the communications described above by selling consumers' personal Driving Data to the third parties, for its own financial and commercial benefit, obtaining substantial profit.

747. In violation of the Illinois Eavesdropping Law, Defendants intentionally disclosed, used, or endeavored to use disclose to third parties the contents of Illinois Plaintiffs and Illinois Subclass Members' private electronic communications intercepted by Defendants while knowing or having reason to know that the information was obtained through the interception of the communications in violation of the Illinois Eavesdropping law.

748. Specifically, Defendants intentionally disclosed or endeavored to disclose Illinois Plaintiffs and Illinois Subclass Members' detailed Driving Data to various auto insurance companies.

749. Defendants further used the information derived from Illinois Plaintiffs' and Illinois Subclass Members' private electronic communications to create products they market, license, and sell, including so-called driving scores, risk ratings, and access to databases containing Illinois Plaintiffs' and Illinois Subclass Members' Driving Data. Defendants also used the information derived from the communications described above in aggregate fashion to create their telematics exchange, develop risk models, and other products they market and sell.

750. Defendants knew or should have known that the detailed driving information they used and sold was captured in violation of the Illinois Eavesdropping Law for the following reasons, among others that will become known through discovery:

a. the numerous, obvious consent and privacy challenges to the collection of Driving Data that Defendants acknowledged in writing and in presentations;

b. the opaque disclosures in Defendants various terms and policies, which did not operate as a reasonable basis for inferring consumer consent to share the information with Defendants;

c. the sheer volume of data Defendants were receiving versus from other

manufacturers;

d. the lack of public knowledge about Defendants' collection and sharing practices until at least 2024;

e. that fact that Defendants continued to collect after it was publicized that collection was secret/happening without consent or knowledge; and

f. the nature of the data as such that it had to be obtained via a wiretap.

751. Illinois Plaintiffs and Illinois Subclass Members did not consent or otherwise authorize Defendants to intercept, disclose, or use their communications.

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

753. Pursuant to 720 ILCS 14-6, Illinois Plaintiffs and Illinois Subclass Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the Eavesdropping law and are entitled to: (1) damages, in an amount to be determined at trial; (2) punitive damages; (3) injunctive relief prohibiting Defendants from further eavesdropping; and (4) reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT TWENTY
Violation of the Indiana Deceptive Consumer Sales Act,
Ind. Code §§ 24-5-035-1, *et seq.*
(On Behalf of the Indiana Plaintiff and the Indiana Subclass Against All Defendants)

754. Plaintiff Kayla Smith (for the purposes of this count, the "Indiana Plaintiff"), individually and on behalf of the Indiana Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

755. Indiana Plaintiff brings this claim on her own behalf and on behalf of each member of the Indiana Subclass described above.

756. Defendants are each a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

757. Defendants are each a "supplier" as defined by § 24-5-0.5-2(a)(1), because they regularly engage in or solicit "consumer transactions," within the meaning of Ind. Code § 24-5-0.5-2(a)(3)(A).

758. Defendants engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions by advertising, offering for sale, selling, or distributing goods and services in the State of Indiana. Ind. Code § 24-5-0.5-3(a).

759. Defendants' representations and omissions include both implicit and explicit representations.

760. Defendant engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade or commerce in violation of Ind. Code § 24-5-0.5- 3 by:

a. Intercepting, collecting, using, and selling Indiana Plaintiff's and Indiana Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Indiana Plaintiff's and Indiana Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Indiana Plaintiff's and Indiana Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated application, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated mobile application, and that it would protect the privacy of Indiana Plaintiff's and Indiana Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Indiana Plaintiff's and Indiana Subclass Members' data.

761. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Indiana Plaintiff's and Indiana Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Indiana Plaintiff's and Indiana Subclass Members' data, including driving data, without obtaining their consent.

762. The fact that Defendant intercepted, collected, used, and sold Indiana Plaintiff's and Indiana Subclass Members' data was material to Indiana Plaintiff and Indiana Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

763. Indiana Plaintiff and Indiana Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, the security and privacy of their data, and their privacy in their own vehicles and while going about their day, to their detriment.

764. Defendants intended to mislead Indiana Plaintiff and Indiana Subclass Members and induce them to rely on their misrepresentations and omissions.

765. In the course of their business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants paid mobile developers millions to integrate their SDK, which

covertly harvested user data, demonstrating that consumers would not consent to the collection and disclosure of data, thus necessitating Defendants' omissions and misrepresentations regarding their programs.

766. Had Defendants disclosed to Indiana Plaintiff and Indiana Subclass Members that they were collecting and disclosing their data, they would have been unable to enroll so many individuals in their programs or disseminate Defendants' SDK. Instead, in order to drastically increase the numbers of consumers enrolled in its programs, Defendants did not disclose material terms or obtain actual, written consent for them. Instead, Defendants omitted material facts from consumers, and misrepresented the actual purpose of its programs. Accordingly, Indiana Plaintiff and the Indiana Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

767. Defendants engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by selling and disseminating Indiana Plaintiff's and Indiana Subclass Members' data with knowledge that such data was obtained without Indiana Plaintiff's and Indiana Subclass Members' consent.

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

769. Indiana Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5. Defendants have not cured their unfair, abusive, and deceptive acts and

practices, or their violations of Indiana Deceptive Consumer Sales Act were incurable. Defendants' conduct was incurable because Indiana Plaintiff's and Indiana Subclass Members' data has already been used and shared with third parties.

770. Defendants' violations present a continuing risk to Indiana Plaintiff and Indiana Subclass Members as well as to the general public if injunctive relief does not prevent them from continuing their deceptive acts and practices in the future.

771. Indiana Plaintiff and Indiana Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

COUNT TWENTY-ONE
Violation of the Kentucky Consumer Protections Act,
Ky. Rev. Stat. §§ 367.110, *et seq.*
(On Behalf of the Kentucky Plaintiff and the Kentucky Subclass Against All Defendants)

772. Plaintiff Rehfuss (for the purposes of this count, the "Kentucky Plaintiff"), individually and on behalf of the Kentucky Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

773. Kentucky Plaintiff brings this claim on her own behalf and on behalf of each member of the Kentucky Subclass described above.

774. Defendants are each a "person" as defined by Ky. Rev. Stat. § 367.110(1).

775. Defendants advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

776. Defendants engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Intercepting, collecting, using, and selling Kentucky Plaintiff's and Kentucky Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Kentucky Plaintiff's and Kentucky Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Kentucky Plaintiff's and Kentucky Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Kentucky Plaintiff's and the Kentucky Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Kentucky Plaintiff's and Kentucky Subclass Members' data.

777. Defendants' representations and omissions include both implicit and explicit representations.

778. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Kentucky Plaintiff's and Kentucky Subclass Members' rights, because

Defendants intentionally intercepted, collected, used, and sold Kentucky Plaintiff's and Kentucky Subclass Members' data without obtaining their consent.

779. The fact that Defendants intercepted, collected, used, and sold Kentucky Plaintiff's and Kentucky Subclass Members' data was material to Kentucky Plaintiff and Kentucky Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

780. Kentucky Plaintiff and Kentucky Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data to their detriment.

781. In the course of their business, Defendants engaged in activities with a tendency or capacity to deceive. Defendants paid mobile developers millions of dollars to integrate their SDK, which covertly harvested user Data, demonstrating that Defendants knew consumers would not consent to the collection and disclosure of data, thus necessitating Defendants' omissions and misrepresentations regarding their programs.

782. Had Defendants disclosed to Kentucky Plaintiff and Kentucky Subclass Members that they were collecting and disclosing data, they would have been unable to enroll so many individuals in their programs. Instead, in order to drastically increase the numbers of consumers enrolled in its programs and third-party applications, Defendants did not disclose material terms or obtain actual, written consent for them. Instead, Defendants omitted material facts from consumers and misrepresented the actual purpose of its programs. Accordingly, Kentucky Plaintiff and the Kentucky Subclass Members acted reasonably in relying on Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

783. Defendants are engaged in unfair and unconscionable conduct in violation of the Act by engaging in the conduct alleged herein, including by selling and disseminating Kentucky Plaintiff's and Kentucky Subclass Members' data without their consent.

784. The above unfair, deceptive, and unconscionable practices and acts by Defendants a were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Kentucky Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

785. Defendants acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Kentucky Plaintiff's and Kentucky Subclass Members' rights.

786. Kentucky Plaintiff's and the Kentucky Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Kentucky Plaintiff's and Kentucky Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefits.

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

788. Kentucky Plaintiff and Kentucky Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs. Defendants' violations present a continuing risk to Kentucky Plaintiff

and Kentucky Subclass Members as well as to the general public if injunctive relief does not prevent them from continuing their deceptive acts and practices in the future.

COUNT TWENTY-TWO
Violation of the Mississippi Consumer Protection Act,
Miss. Code. §§ 75-24-1, *et seq.*
(On Behalf of the Mississippi Plaintiff and the Mississippi Subclass Against All Defendants)

789. Plaintiff Carroll (for the purposes of this count, the "Mississippi Plaintiff"), individually and on behalf of the Mississippi Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

790. Mississippi Plaintiff brings this claim on his own behalf and on behalf of each member of the Mississippi Subclass described above.

791. Mississippi Plaintiff and Defendants are each "persons" as defined by Miss. Code. § 75-24-1(a).

792. Defendants engaged in "trade" and "commerce" as defined by Miss. Code. § 75-24-1(b)

793. Defendants engaged in trade and commerce in Mississippi and/or directly or indirectly affecting the people of Mississippi.

794. Defendants engaged in unfair or deceptive trade practices in or affecting commerce, in violation of Miss. Code. § 75-24-5, including by:

a. Intercepting, collecting, using, and selling Mississippi Plaintiff's and Kentucky Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Mississippi Plaintiff's and Kentucky Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Mississippi Plaintiff's and Kentucky Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Mississippi Plaintiff's and the Kentucky Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Mississippi Plaintiff's and Kentucky Subclass Members' data.

795. Defendants intended to mislead Mississippi Plaintiff and induce Mississippi Subclass Members to rely on their misrepresentations and omissions.

796. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Mississippi Plaintiff's and Mississippi Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Mississippi Plaintiff's and Mississippi Subclass Members' data without obtaining their consent.

797. The fact that Defendants intercepted, collected, used, and sold Mississippi Plaintiff's and Mississippi Subclass Members' data was material to Mississippi Plaintiff and

Mississippi Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or sue an application.

798. Mississippi Plaintiff and Mississippi Subclass Members were deceived, and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of the SDK, the security and privacy of their data, and their privacy in their own vehicles and while going about their day, to their detriment.

799. Defendants engaged in unfair and deceptive trade practices in or affecting commerce, in violation of Miss. Code. § 75-24-5, by engaging in the conduct alleged herein, including by using, selling and disseminating Mississippi Plaintiff's and Mississippi Subclass Members' data without their consent.

800. Defendants acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Mississippi Plaintiff's and the Mississippi Subclass' rights.

801. Mississippi Plaintiff's and the Mississippi Subclass' data, including driving data, has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, Mississippi Plaintiff's and Mississippi Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

802. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive acts and practices, Mississippi Plaintiff and Mississippi Subclass Members have suffered and will continue to suffer injury ascertainable losses of money or property, and monetary and nonmonetary damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the

likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

803. Mississippi Plaintiff's and the Mississippi Subclass' data was exploited without informed consent. Accordingly, Mississippi Plaintiff and the Mississippi Subclass are entitled to part of Defendants' profits that were generated by their data without informed consent.

804. Mississippi Plaintiff and the Mississippi Subclass seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, attorneys' fees and costs, and any other relief that is just and proper. Miss. Code. § 75-24-15.

COUNT TWENTY-THREE
Violation of the Michigan Consumer Protection Act,
Mich. Comp. Laws Ann. §§ 445.901, *et seq.*
(On Behalf of the Michigan Plaintiff and the Michigan Subclass Against All Defendants)

805. Plaintiff Anderson (for the purposes of this count, the "Michigan Plaintiff"), individually and on behalf of the Michigan Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

806. Defendants and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

807. Defendants advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

808. Defendants engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that their goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

809. Defendants' unfair, unconscionable, and deceptive practices included the following conduct:

a. Intercepting, collecting, using, and selling Michigan Plaintiff's and Michigan Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Michigan Plaintiff's and Michigan Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Michigan Plaintiff's and Michigan Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Michigan Plaintiff's and the Michigan Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Michigan Plaintiff's and Michigan Subclass Members' data.

810. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers.

811. Defendants intended to mislead Michigan Plaintiff and Michigan Subclass members and induce them to rely on its misrepresentations and omissions.

812. The fact that Defendants intercepted, collected, used, and sold Michigan Plaintiffs' and Michigan Subclass Members' Driving Data was material to Michigan Plaintiff and Michigan Subclass Members. This is a fact that reasonable consumers would consider important when choosing to use applications associated with Defendants' SDK.

813. Defendants acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Michigan Plaintiff and Michigan Subclass members' rights because Defendants intentionally intercepted, collected, used, and sold Michigan Plaintiff's and Michigan Subclass Members' data without obtaining their consent.

814. Defendants' unfair, unconscionable, and deceptive practices in the conduct of trade and commerce included entering into a consumer transaction in which the consumer waives or purports to waive a right, benefit, or immunity provided by law, where the waiver was not clearly stated and the consumer did not specifically consent to it. Mich. Comp. Laws Ann. § 445.903(1)(t).

815. As a direct and proximate result of Defendants' unfair, unconscionable, and deceptive practices, Michigan Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

816. Michigan Plaintiff's and the Michigan Subclass' data was exploited without informed consent. Accordingly, Michigan Plaintiff and the Michigan Subclass are entitled to part of Defendants' profits that were generated by their data without informed consent.

817. Michigan Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, disgorgement, injunctive relief, attorneys' fees and costs, and any other relief that is just and proper.

COUNT TWENTY-FOUR
Violation of the New Jersey Consumer Fraud Act,
N.J. Stat. Ann. §§ 56:8-1, *et seq.*
(On Behalf of the New Jersey Plaintiff and the New Jersey Subclass Against All Defendants)

818. Plaintiff Sanginito (for the purposes of this count, the "New Jersey Plaintiff"), individually and on behalf of the New Jersey Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

819. New Jersey Plaintiff brings this claim on his own behalf and on behalf of each member of the New Jersey Subclass described above.

820. Defendants are "person(s)" as defined by N.J. Stat. Ann. § 56:8-1(d).

821. Defendants sell "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) and (e).

822. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

823. Defendants' unconscionable and deceptive practices include:

a. Intercepting, collecting, using, and selling New Jersey Plaintiff's and New Jersey Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling New Jersey Plaintiff's and New Jersey Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold New Jersey Plaintiff's and New Jersey Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of New Jersey Plaintiff's and the New Jersey Subclass Members' data,

including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of New Jersey Plaintiff's and New Jersey Subclass Members' data.

824. Defendants intended to mislead New Jersey Plaintiff and New Jersey Subclass members and induce reliance on their misrepresentations and omissions.

825. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded New Jersey Plaintiff's and New Jersey Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold New Jersey Plaintiff's and New Jersey Subclass Members' data without obtaining their consent.

826. The fact that Defendants intercepted, collected, used, and sold New Jersey Plaintiff's and New Jersey Subclass Members' data was material to New Jersey Plaintiff and New Jersey Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, download or use an application.

827. New Jersey Plaintiff and New Jersey Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

828. New Jersey Plaintiff's and the New Jersey Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, New Jersey Plaintiff's and New Jersey Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

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

830. New Jersey Plaintiff and New Jersey Subclass Members have suffered injuries in fact and ascertainable losses of money or property as a result of Defendants' deceptive acts and practices. New Jersey Plaintiff's data has tangible economic value, which was wrongfully appropriated by Defendants for financial gain.

831. New Jersey Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, treble damages under N.J. Stat. Ann. § 56:8-19, attorneys' fees, filing fees, and costs.

COUNT TWENTY-FIVE
Violation of the New York General Business Law,
N.Y. Gen. Bus. Law § 349
(On Behalf of the New York Plaintiff and the New York Subclass Against All Defendants)

832. Plaintiff Tupper (for the purposes of this count, the "New York Plaintiff"), individually and on behalf of the New York Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

833. New York Plaintiff brings this claim on his own behalf and on behalf of each member of the New York Subclass described above.

834. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce, in violation of N.Y. Gen. Bus. Law § 349. Defendants engaged in deceptive acts and practices by:

a. Intercepting, collecting, using, and selling New York Plaintiff's and New York Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling New York Plaintiff's and New York Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold New York Plaintiff's and New York Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of New York Plaintiff's and the New York Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of New York Plaintiff's and New York Subclass Members' data.

835. Defendants' omissions and misrepresentations were material because they were likely to deceive reasonable consumers into believing that their data would not be sold or used for financial gain without their knowledge or consent.

836. Defendants acted intentionally, knowingly, and maliciously to violate N.Y. Gen. Bus. Law § 349, or acted with reckless disregard for the rights of New York Plaintiff and New York Subclass Members.

837. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, New York Plaintiff and New York Subclass Members have suffered and will continue to suffer injury, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

838. New York Plaintiff and New York Subclass Members have suffered injuries in fact and ascertainable losses of money or property as a result of Defendants' deceptive acts and practices. New York Plaintiff's and New York Subclass Members' data has tangible economic value, which was wrongfully appropriated by Defendants for financial gain.

839. The public interest and consumers at large were harmed by Defendants' deceptive and unlawful acts, which affected thousands of New York residents.

840. New York Plaintiff and New York Subclass Members seek all monetary and non-monetary relief available under N.Y. Gen. Bus. Law § 349, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, attorneys' fees, and costs.

COUNT TWENTY-SIX
Violation of the New York General Business Law,
N.Y. Gen. Bus. Law § 350
(On Behalf of the New York Plaintiff and the New York Subclass Against All Defendants)

841. Plaintiff Tupper (for the purposes of this count, the "New York Plaintiff"), individually and on behalf of the New York Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

842. New York Plaintiff brings this claim on her own behalf and on behalf of each member of the New York Subclass described above.

843. Defendants engaged in advertising, including labeling, of goods and services that was misleading in a material respect in violation of New York General Business Law § 350-a(1).

844. Defendants' advertising was misleading in a material respect because it falsely implied that their goods and services included privacy protections for consumers' data and failed to disclose material facts regarding the collection and sale of such data. Specifically, Defendants failed to disclose that it was surreptitiously collecting New York Plaintiff's and New York Subclass Members' data and subsequently selling that data to third parties for profit.

845. The omission of these material facts rendered Defendants' representations misleading in light of the advertised nature of their goods and services. New York Plaintiff and New York Subclass Members reasonably believed, based on Defendants' advertising, that their data would not be collected or sold without their knowledge and consent.

846. Defendants knowingly and intentionally engaged in false advertising with the intent to induce New York Plaintiff and New York Subclass Members to use their goods and services, and the goods and services of applications using Defendants' SDK, relying on the misleading representations and omissions regarding privacy protections for data.

847. As a direct and proximate result of Defendants' false advertising, New York Plaintiff and New York Subclass Members were injured in that they purchased or downloaded goods and services under false pretenses and suffered a loss of privacy and control over their data, which has tangible value. New York Plaintiff and New York Subclass Members would not have purchased or downloaded Defendants' goods and services, or the goods and services of mobile

applications utilizing Defendants' SDK, or would have paid less for them, had the true facts been disclosed.

848. New York Plaintiff seeks all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of five hundred dollars per violation, whichever is greater, treble damages for willful or knowing violations, injunctive relief, reasonable attorneys' fees, costs, pre-judgment interest, and any other relief the Court deems just and proper.

COUNT TWENTY-SEVEN
Violation of the New York General Business Law – SHIELD Act,
N.Y. Gen. Bus. Law §§ 899-aa, 899-bb
(On Behalf of the New York Plaintiff and the New York Subclass Against All Defendants)

849. Plaintiff Tupper (for the purposes of this count, the "New York Plaintiff"), individually and on behalf of the New York Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

850. New York Plaintiff brings this claim on her own behalf and on behalf of each member of the New York Subclass described above.

851. Defendants are businesses that own, license, or maintain computerized data that includes private information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Accordingly, Defendants are subject to the requirements of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

852. New York Plaintiff's and Class Members' data includes private information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b), as it contains sensitive, identifiable information, including records of their driving events.

853. Defendants collected and maintained data from New York Plaintiff and New York Subclass Members without informing them of the scope of the data collection or obtaining their consent for its subsequent use and sale to third parties.

854. Pursuant to N.Y. Gen. Bus. Law § 899-bb(2), Defendants were required to implement and maintain reasonable administrative, technical, and physical safeguards to protect New York Plaintiff's and New York Subclass Members' data, including driving data, against unauthorized access, acquisition, or misuse.

855. Defendants failed to implement such reasonable safeguards, as they failed to disclose the sale of New York Plaintiff's and New York Subclass Members' data and enabled unauthorized access and transfer of this private information.

856. Defendants violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3) by failing to provide timely, accurate, and sufficient notice to New York Plaintiff and New York Subclass Members of the unauthorized collection, use, and sale of their data.

857. Defendants' failure to adhere to the administrative and security requirements of the SHIELD Act (N.Y. Gen. Bus. Law § 899-bb(2)) further compromised the security and confidentiality of New York Plaintiff's and New York Subclass Members' private information.

858. As a direct and proximate result of Defendants' violations of N.Y. Gen. Bus. Law §§ 899-aa and 899-bb, New York Plaintiff and New York Subclass Members suffered damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

859. New York Plaintiff and New York Subclass Members seek all remedies available under N.Y. Gen. Bus. Law §§ 899-aa(6)(b) and 899-bb(2), including actual damages, injunctive relief, and any other relief deemed just and proper by the Court.

COUNT TWENTY-EIGHT
Violation of the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen. Stat. §§ 75-1.1, *et seq.*
(On Behalf of the North Carolina Plaintiff and the North Carolina Subclass Against All Defendants)

860. Plaintiff Singh (for the purposes of this count, the "North Carolina Plaintiff"), individually and on behalf of the North Carolina Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

861. North Carolina Plaintiff brings this claim on her own behalf and on behalf of each member of the North Carolina Subclass described above.

862. Defendants and North Carolina Plaintiff are "persons" as defined by N.C. Gen. Stat. § 75-1.1(d).

863. Defendants advertised, offered, or sold goods and services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. § 75-1.1(b).

864. Defendants engaged in unfair, unconscionable, and deceptive practices in violation of N.C. Gen. Stat. § 75-1.1(a). These practices include:

a. Intercepting, collecting, using, and selling North Carolina Plaintiff's and North Carolina Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling North Carolina Plaintiff's and North Carolina Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold North Carolina Plaintiff's and North Carolina Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of North Carolina Plaintiff's and the North Carolina Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of North Carolina Plaintiff's and North Carolina Subclass Members' data.

865. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded North Carolina Plaintiff's and North Carolina Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold North Carolina Plaintiff's and North Carolina Subclass Members' data, including driving data, without obtaining their consent. Defendants intended to mislead North Carolina Plaintiff and North Carolina Subclass members and induce them to rely on the omissions to their detriment.

866. The fact that Defendants intercepted, collected, used, and sold North Carolina Plaintiff's and North Carolina Subclass Members' data was material to North Carolina Plaintiff and North Carolina Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

867. North Carolina Plaintiff and North Carolina Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations

and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

868. North Carolina Plaintiff's and the North Carolina Subclass' data has tangible value. As a direct and proximate result of Defendants' unfair and deceptive acts and practices, North Carolina Plaintiff's and North Carolina Subclass Members' data is in the possession of third parties who have used and will use such data for their commercial benefit.

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

870. North Carolina Plaintiff and the North Carolina Subclass seek all monetary and non- monetary relief allowed by law, including actual damages or statutory damages of $500 per violation, whichever is greater, treble damages pursuant to N.C. Gen. Stat. § 75-16, injunctive relief, attorneys' fees under N.C. Gen. Stat. § 75-16.1, pre-judgment interest, costs, and any other relief the Court deems just and proper.

COUNT TWENTY-NINE
Violation of the Ohio Consumer Sales Practices Act,
Ohio Rev. Code §§ 1345.01, *et seq.*
(On Behalf of the Ohio Plaintiff and the Ohio Subclass Against All Defendants)

871. Plaintiff Robert Smith (for the purposes of this count, the "Ohio Plaintiff"), individually and on behalf of the Ohio Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

872. Ohio Plaintiff brings this claim on his own behalf and on behalf of each member of the Ohio Subclass described above.

873. Ohio Plaintiff and Ohio Subclass Members are "persons" as defined by Ohio Rev. Code § 1345.01(B).

874. Defendants are a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) and (C), by offering goods and services to consumers in Ohio.

875. Defendants engaged in unfair and deceptive acts and practices in connection with consumer transactions, in violation of Ohio Rev. Code §§ 1345.02 and 1345.03.

876. Defendants violated Ohio Rev. Code § 1345.02(B)(1) by representing that its goods and services had characteristics, uses, and benefits that they did not have, including misleading Ohio Plaintiff and Ohio Subclass Members into believing their data would remain private and secure, while surreptitiously collecting and selling such data to third parties.

877. Defendants further violated Ohio Rev. Code § 1345.02(B)(2) by representing that its goods and services were of a particular standard or quality when they were not, misleading Ohio Plaintiff and Ohio Subclass Members into believing that their data, including driving data, would not be misused for Defendants' profit.

878. Defendants engaged in unconscionable acts in connection with consumer transactions, in violation of Ohio Rev. Code § 1345.03, by surreptitiously collecting and monetizing Ohio Plaintiff's and Ohio Subclass Members' data without their knowledge or consent and by exploiting the inability of consumers to reasonably protect their interests in the face of Defendants' concealed practices.

879. Defendants failed to disclose material facts about its data collection and monetization practices, despite a duty to do so, and concealed its sale of data to third parties, in violation of Ohio Rev. Code §§ 1345.02 and 1345.03.

880. Defendants acted knowingly, intentionally, and maliciously to violate the Ohio Consumer Sales Practices Act by surreptitiously monetizing Ohio Plaintiff's and Ohio Subclass Members' data without consent and in reckless disregard of Ohio Plaintiff's and Ohio Subclass Members' rights.

881. As a direct and proximate result of Defendants' unfair, deceptive, and unconscionable acts and practices, Ohio Plaintiff and Ohio Subclass Members have suffered ascertainable losses of money or property, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

882. Ohio Plaintiff and Ohio Subclass Members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or statutory damages, treble damages, injunctive relief, attorneys' fees and costs, and any other relief the Court deems just and proper.

COUNT THIRTY
Violation of the Oregon Unlawful Trade Practices Act,
ORS §§ 646.605, *et seq.*
(On Behalf of the Oregon Plaintiff and the Oregon Subclass Against All Defendants)

883. Plaintiff Hartline (for the purposes of this count, the "Oregon Plaintiff"), individually and on behalf of the Oregon Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

884. Oregon Plaintiff brings this claim on her own behalf and on behalf of each member of the Oregon Subclass described above.

885. Defendants are "person(s)" within the meaning of ORS § 646.605(4).

886. Defendants have sold "goods or services" within the meaning of the Act, which mean "those that are or may be obtained primarily for personal, family or household purposes[.]" ORS § 646.605(6)(a).

887. Defendants violated the Unlawful Trade Practices Act ("UTPA") by representing that its goods and services had characteristics, uses, and benefits that they did not have, including misleading Oregon Plaintiff and Oregon Subclass Members into believing their data would remain private and secure, while surreptitiously collecting and selling such data to third parties.

888. Defendants' conduct violated ORS § 646.607(1) by employing unconscionable tactics in connection with its sale by surreptitiously monetizing Oregon Plaintiff's and Oregon Subclass Members' data without consent and in reckless disregard of Oregon Plaintiff's and Oregon Subclass Members' rights.

889. Defendant's conduct also violated ORS § 646.608(1)(e) by representing at the time of sale that goods or services have characteristics, uses, benefits, or qualities that Defendant now claims they do not have.

890. Defendant's conduct also violated ORS § 646.608(1)(g) by representing at the time of sale that goods or services were of a particular standard or quality that Defendant now claims they are not.

891. Defendant's conduct also violated ORS § 646.608(1)(i) by advertising goods or services with the intent not to provide them as advertised.

892. Defendant's conduct also violated ORS § 646.608(1)(u) by, *inter alia*, by surreptitiously monetizing Oregon Plaintiff's and Oregon Subclass Members' data without consent and in reckless disregard of Oregon Plaintiff's and Oregon Subclass Members' rights, including but not limited to the rights provided by the Oregon Consumer Privacy Act, § ORS 646A.570, *et seq*.

893. Defendant's conduct also violated ORS § 646.607(2) by failing to deliver Oregon Plaintiff's and Class Members' goods or services as promised.

894. A violative representation "may be made by any assertion by words or conduct, including, but not limited to, a failure to disclose a fact." ORS § 646.608(2). Defendants engaged in unlawful trade practices by:

a. Intercepting, collecting, using, and selling Oregon Plaintiff's and Oregon Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Oregon Plaintiff's and Oregon Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Oregon Plaintiff's and Oregon Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Oregon Plaintiff's and the Oregon Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Oregon Plaintiff's and Oregon Subclass Members' data.

895. These misrepresentations and omissions concern the characteristics, uses, benefits, qualities and standards of Defendants' goods and services, in violation of ORS § 646.605(1)(e) and (1)(g).

896. By misrepresenting and omitting crucial information regarding the functionality of the apps with respect to the privacy of drivers in their own vehicles, Defendants advertised its goods and services with intent not to provide them as advertised, in violation of ORS § 646.605(1)(i).

897. Defendants' conduct caused substantial injury to Oregon Plaintiff and Class Members, is not outweighed by any countervailing benefits to consumers or competitors, and was not reasonably avoidable by consumers.

898. Defendant's conduct is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

899. Had Oregon Plaintiff and Class Members known about Defendants unlawful trade practices, they would not have purchased the goods or services or would have paid much less for them.

900. As a direct and proximate result of Defendants' unlawful practices, Oregon Plaintiff and Oregon Subclass Members have suffered and will continue to suffer injury, losses, and

damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

901. In violating Oregon Plaintiff's and Oregon Subclass Members' rights under the UPTA as described herein, Defendants acted intentionally, knowingly, and/or with reckless disregard of the rights of Oregon Plaintiff and Oregon Subclass Members.

902. Oregon Plaintiff, individually and on behalf of the Class, seeks all remedies available under the UTPA, including equitable relief, actual damages and statutory damages, including under ORS § 646.638(1).

903. Oregon Plaintiff, individually and on behalf of the Class, also seeks reasonable attorneys' fees and costs under ORS § 646.638(3).

COUNT THIRTY-ONE
Pennsylvania Invasion of Privacy
(On Behalf of the Pennsylvania Plaintiffs and the Pennsylvania Subclass Against All Defendants)

904. Plaintiffs DeValkeneer, Eppley, Rochester, and Winkelvoss (for the purposes of this count, the "Pennsylvania Plaintiffs"), individually and on behalf of the Pennsylvania Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

905. Pennsylvania Plaintiffs bring this claim on their own behalf and on behalf of each member of the Pennsylvania Subclass described above.

906. Pennsylvania recognizes an inherent right to privacy.

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

908. Pennsylvania Plaintiffs and Pennsylvania Subclass Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

909. Pennsylvania Plaintiffs and Pennsylvania Subclass Members had no knowledge and did not consent or authorize Defendants to obtain their driving telematics data or to share it with third parties, let alone the specific third parties to whom Defendants shared it with and/or sold Pennsylvania Plaintiffs' and Subclass Members' data.

910. Pennsylvania Plaintiffs and Pennsylvania Subclass Members enjoyed objectively reasonable expectations of privacy surrounding their data, including their precise location and other PII and personal data. Defendants' intrusion upon seclusion occurred the moment Defendants began tracking Pennsylvania Plaintiffs and Pennsylvania Subclass Members' personal data, including their locations and other PII and other data.

911. Defendants' conduct was intentional and intruded on Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' use of their personal property.

912. Defendants' conduct was highly offensive to a reasonable person because they shared and/or sold the data for reports for auto insurance companies to influence Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' insurance rates without their prior knowledge or consent.

913. As a direct and proximate result of Defendants' invasions of privacy, Pennsylvania Plaintiffs and Pennsylvania Subclass Members have suffered and will continue to suffer injury and damages, as alleged herein, including but not limited to overpayment for auto insurance services and decreased value of their driving telematics data.

914. Pennsylvania Plaintiffs and Pennsylvania Subclass Members week all relief available for invasion of privacy claims, including nominal damages and general privacy damages.

915. Pennsylvania Plaintiffs, on behalf of themselves and Pennsylvania Subclass Members, further seeks injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' Private Information and to adhere to its common law, contractual, statutory, and regulatory duties.

COUNT THIRTY-TWO
Pennsylvania Unlawful Use of Computer
(On Behalf of the Pennsylvania Plaintiffs and the Pennsylvania Subclass Against All Defendants)

916. Plaintiffs DeValkeneer, Eppley, Rochester, and Winkelvoss (for the purposes of this count, the "Pennsylvania Plaintiffs"), individually and on behalf of the Pennsylvania Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

917. Pennsylvania Plaintiffs bring this claim on their own behalf and on behalf of each member of the Pennsylvania Subclass described above.

918. Pennsylvania criminal code prohibits parties to "intentionally and without authorization accesses or exceeds authorization to access, alters, interferes with the operation of, damages or destroys any computer, computer system, computer network, computer software, computer program, computer database, World Wide Web site or telecommunication device or any part thereof," and to "intentionally or knowingly and without authorization gives or publishes a password, identifying code, personal identification number or other confidential information about a computer, computer system, computer network, computer database, World Wide Web site or telecommunication device." 73 Pa. Stat. § 7611(a).

919. Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' smartphones constitute "computers" within the scope of Pennsylvania law.

920. Defendants knowingly accessed Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' smartphones without their permission by including within the SDK (that Defendants provide to developers) software that intercepts and transmits data, communications, and personal and confidential information concerning Pennsylvania Plaintiffs and Pennsylvania Subclass Members.

921. Defendants used data, communications, and personal information that it intercepted and took from Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' smart phones to wrongfully and unjustly enrich itself at the expense of Pennsylvania Plaintiffs and Subclass Members.

922. Defendants knowingly and without Pennsylvania Plaintiffs' and Subclass Members' permission accessed or caused to be their smartphones by installing without Pennsylvania Plaintiffs' and Subclass Members' informed consent software that intercepts and/or takes data, communications, and personal information concerning Pennsylvania Plaintiffs and Subclass Members.

923. Pennsylvania Plaintiffs and Pennsylvania Subclass Members are residents of Pennsylvania, and used their smartphones in Pennsylvania. Defendants accessed or caused to be accessed Pennsylvania Plaintiffs' and Pennsylvania Class Members' data, communications, and personal information from Pennsylvania.

924. As a direct and proximate result of Defendants' violations of the Pennsylvania unlawful computer use statute, Pennsylvania Plaintiffs and Pennsylvania Subclass Members suffered damages.

925. Pennsylvania Plaintiffs and Subclass Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial, including an award of reasonable attorneys' fees and costs and punitive or exemplary damages for Defendants' willful violations.

COUNT THIRTY-THREE
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTP"), 73 Pa. Stat. §§ 201, *et seq.*
(On Behalf of the Pennsylvania Plaintiffs and the Pennsylvania Subclass Against All Defendants)

926. Plaintiffs DeValkeneer, Eppley, Rochester, and Winkelvoss (for the purposes of this count, the "Pennsylvania Plaintiffs"), individually and on behalf of the Pennsylvania Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

927. Pennsylvania Plaintiffs bring this claim on their own behalf and on behalf of each member of the Pennsylvania Subclass described above.

928. Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTP") defines "unfair or deceptive acts or practices" to include any "fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding." 73 Pa. Stat. § 201, et seq.

929. Pennsylvania courts have invariably interpreted the UTP using the kind of liberal construction afforded to state consumer protection statutes intended to prevent fraud.

930. Pennsylvania Plaintiffs and the Pennsylvania Subclass Members, as "person[s]," are consumers within the protection of the UTP. See 73 Penn. Stat. § 201-2(2).

931. Defendants engaged in unfair, unconscionable, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of 73 Penn. Stat. § 201-2(4), including but not limited to the following: (a) knowingly and improperly storing, possessing, using, and/or procuring the interception of, Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' Personal; (b) using that PII and other personal data to impose increased insurance rates; and (c) selling and/or

transmitting Pennsylvania Plaintiffs' and Pennsylvania Subclass Members' data to third parties without their consent.

932. The unfair, unconscionable, and unlawful acts and practices of Defendants alleged herein, emanated and arose within the Commonwealth of Pennsylvania, within the scope of the UTP.

933. Pennsylvania Plaintiffs and Pennsylvania Subclass Members are entitled to injunctive relief to protect them from the substantial and imminent risk of future loss of Private Information, including, but not limited to: (a) ordering that Defendants immediately purge, delete, and destroy PII and other personal data not necessary for its provisions of services; and (b) remove tracking technology that causes the disclosure of PII and other personal data without consent.

934. Pennsylvania Plaintiffs bring this action on behalf of themselves and Pennsylvania Subclass Members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed decisions with their PII and other personal data and to protect Pennsylvania Plaintiffs, Pennsylvania Subclass Members, and the public from Defendants' unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Class Action Complaint has had widespread impact on the public at large.

935. Defendants' actions and inactions in engaging in the unfair, unconscionable, and unlawful practices described herein were negligent, knowing and willful, and/or wanton and reckless.

936. Pennsylvania Plaintiffs and Pennsylvania Subclass Members seek relief under the UTP, 73 P.S. §§ 201-1, *et seq.*, including, but not limited to, a declaratory judgment that Defendants' actions and/or practices violate the UTP; and injunctive relief enjoining Defendants,

their employees, parents, subsidiaries, affiliates, executives, and agents from continuing to violate the UTP as described above.

937. Pennsylvania Plaintiffs and Pennsylvania Subclass Members therefore seek restitution, an injunction, and all other appropriate relief in equity, including reasonable attorneys' fees and costs of suit.

COUNT THIRTY-FOUR
Violation of the Pennsylvania Wiretapping and Electronic Surveillance Act ("WECMA"), 18 Pa. Stat. §§ 5703, *et seq.*
(On Behalf of the Pennsylvania Plaintiffs and the Pennsylvania Subclass Against All Defendants)

938. Plaintiffs DeValkeneer, Eppley, Rochester, and Winkelvoss (for the purposes of this count, the "Pennsylvania Plaintiffs"), individually and on behalf of the Pennsylvania Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

939. Pennsylvania Plaintiffs bring this claim on their own behalf and on behalf of each member of the Pennsylvania Subclass described above.

940. To establish liability under the Pennsylvania Wiretapping and Electronic Surveillance Control Act ("WECMA"), Pennsylvania Plaintiffs need only to establish that Defendant "procure[d] any other person to intercept [electronic] communication." 18 Pa. C.S. § 5725.

941. At all relevant times, there was in full force and effect WECMA, which prohibits parties that

> (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
>
> (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
>
> (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know,

> that the information was obtained through the interception of a wire, electronic or oral communication.

18 Pa. Stat. § 5703.

942. Pennsylvania Plaintiffs' and Subclass Members' specific user input events and choices on their mobile devices that are tracked by Defendants' SDK constitute communications within the scope of Pennsylvania's prohibition upon Wiretapping.

943. Pennsylvania Plaintiffs and Subclass Members are residents of Pennsylvania, and used their smartphones within Pennsylvania. As such, Defendants intercept, collected, read or attempt to read, and/or used or attempted to use Pennsylvania Plaintiffs' and Subclass Members' data, communications, and personal information in Pennsylvania.

944. Defendants intercept Pennsylvania Plaintiffs' and Subclass Members' communications and data while they are in transit to and from Plaintiff's and Subclass Members' smartphones and the apps, app developers, and cellphone towers; Defendants transmit a copy of Pennsylvania Plaintiffs' and Subclass Members' communications to itself and/or third parties. Defendants use the contents of the communications to sell to third parties and in other methods for their own pecuniary gain.

945. Neither Defendants nor any other person informed Pennsylvania Plaintiffs and Subclass Members that Defendants were intercepting and transmitting Pennsylvania Plaintiffs' private communications and data.

946. Pennsylvania Plaintiffs and Subclass Members did not know Defendants were intercepting and recording their communications and data, as such they could not and did not consent for their communications and data to be intercepted by Defendants and thereafter transmitted to others.

947. Defendants' SDK constitutes a machine, instrument, contrivance or other manner to track and intercept Pennsylvania Plaintiffs' and Subclass Members' communications while they are using their smartphones.

948. Defendants use and attempt to use or communicate the meaning of Pennsylvania Plaintiffs' and Subclass Members' communications and data by ascertaining their personal information, including their geolocation and places that they have visited and other PII and personal data, in order to sell Pennsylvania Plaintiffs' and Subclass Members' personal information to third parties and to use for Defendants' own gain.

949. At all relevant times to this complaint, Defendants intercepted and recorded components of Plaintiff's and the putative Subclass members' private phone communications and transmissions when Plaintiff and other Subclass Members accessed Defendants' software via their cellular mobile access devices within the State of Pennsylvania.

950. At all relevant times to this complaint, Pennsylvania Plaintiffs and the other Subclass Members did not know Defendants were engaging in such interception and recording and therefore could not provide consent to have any part of their PII and other personal data and communications intercepted and recorded by Defendants and thereafter transmitted to others.

951. Defendants never advised Pennsylvania Plaintiffs or the other Subclass Members that any part of their PII and other personal data and communications would be intercepted, recorded and transmitted to third parties.

952. Defendants' use of MAIDs, IDFAs, IDFVs and its SDK are both a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

953. At all relevant times, by using Defendants' MAID software and SDK as well as tracking Pennsylvania Plaintiffs' and Subclass Members' geolocation, Defendants intentionally tapped, electrically or otherwise, the lines of internet communication between Pennsylvania Plaintiffs and Subclass Members on the one hand, and the specific sites, apps, and locations Pennsylvania Plaintiffs and Subclass Members visited on the other.

954. At all relevant times, by using Defendants' geolocation tracking software technology, Defendants willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Pennsylvania Plaintiffs and putative Subclass Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within Pennsylvania.

955. Pennsylvania Plaintiffs and Subclass Members did not consent to any of Defendants' actions in implementing these wiretaps within its geolocation tracking software. Nor have Pennsylvania Plaintiffs or Subclass Members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Pennsylvania Plaintiffs and Subclass Members' electronic communications.

956. Pennsylvania Plaintiffs' and the Subclass Members devices of which Defendants accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

957. Defendants violated WECMA by knowingly accessing and without permission accessing Pennsylvania Plaintiffs' and Subclass Members' devices in order to obtain their personal information, including their communications and device and location data, and in order for

Defendants to share that data with third parties, in violation of Pennsylvania Plaintiffs' and Subclass Members' reasonable expectations of privacy in their devices and data.

958. Defendants violated WECMA by knowingly and without permission intercepting, wiretapping, accessing, taking and using Pennsylvania Plaintiffs' and the Subclass Members' personally identifiable information and personal communications with others.

959. As a direct and proximate result of Defendants' violation of WECMA, Pennsylvania Plaintiffs and 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.

960. Defendants were unjustly enriched by its violation of WECMA.

961. Pursuant to 18 Pa. Stat. § 5703, Pennsylvania Plaintiffs and Subclass Members have been injured by Defendants' violation, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT THIRTY-FIVE
Violation of the South Carolina Unfair Trade Practices Act ("South Carolina UTPA"), S.C. Code §§ 39-5-10, *et seq.*
(On Behalf of the South Carolina Plaintiff and the South Carolina Subclass Against All Defendants)

962. Plaintiff Baumgartner and Seay (for the purposes of this count, the "South Carolina Plaintiffs"), individually and on behalf of the South Carolina Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

963. South Carolina Plaintiffs bring this claim on their own behalf and on behalf of each member of the South Carolina Subclass described above.

964. The South Carolina Unfair Trade Practices Act ("South Carolina UTPA") makes unlawful unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. S.C. Code § 39-5-10(a).

965. Defendants are each a "person" as defined by S.C. Code § 39-5-10(a), which includes corporations, trusts, partnerships, incorporated or unincorporated associations and any other legal entity.

966. Defendants are each engaged in "trade" or "commerce" as defined by S.C. Code § 39-5-10(b), which includes the advertising, offering for sale, sale or distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of South Carolina.

967. The South Carolina UTPA is guided by the interpretations given by the Federal Trade Commission and the Federal Courts to Section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. § 45(a)(1)).

968. Pursuant to 15 U.S.C. 45(n), an act or practice is "unfair" if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n).

969. By surreptitiously collecting South Carolina Plaintiffs' and South Carolina Subclass Members' data, including driving data, and exploiting that data for their own commercial gain, Defendants have engaged in unfair practices.

970. South Carolina Plaintiffs and South Carolina Subclass Members could not have reasonably avoided Defendants' practices as described herein because Defendants concealed their practices.

971. South Carolina Plaintiffs and South Carolina Subclass Members have derived no benefit from Defendants' surreptitious collection and exploitation of their private information, and

there are no countervailing benefits to consumers or to competition in engaging in the unauthorized tracking and sale of consumer data.

972. South Carolina Plaintiffs and South Carolina Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because they have experienced economic loss.

973. As a direct and proximate result of Defendants' unfair practices, South Carolina Plaintiffs and South Carolina Subclass Members have suffered and will continue to suffer injury, losses, and damages, including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

974. In violating South Carolina Plaintiffs' and South Carolina Subclass Members' rights under the South Carolina UTPA as described herein, Defendants acted intentionally, knowingly, and/or with reckless disregard of the rights of South Carolina Plaintiffs and South Carolina Subclass Members.

975. South Carolina Plaintiffs and South Carolina Subclass Members seek all monetary and nonmonetary relief allowed by law, including equitable relief, actual damages, treble damages, punitive damages, and reasonable attorneys' fees and costs.

COUNT THIRTY-SIX
Violation of the Texas Deceptive Trade Practices-Consumer Protection Act ("Texas TPCPA"), Tex. Bus. & Com. Code §§ 17.41, *et seq.*
(On Behalf of the Texas Plaintiffs and the Texas Subclass Against All Defendants)

976. Plaintiffs Freel, Rastrelli, and Summersill (for the purposes of this count, the "Texas Plaintiffs"), individually and on behalf of the Texas Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

977. Texas Plaintiffs bring this claim on their own behalf and on behalf of each member of the Texas Subclass described above.

978. The Texas Trade Practices-Consumer Protection Act ("Texas TPCPA") "shall be liberally construed and applied to promote its underlying purposes, which are to protect consumers against false, misleading, and deceptive business practices, unconscionable actions, and breaches of warranty and to provide efficient and economical procedures to secure such protection." Tex. Bus. & Com. Code § 17.44(a).

979. Defendants are each a "person" as defined by Tex. Bus. & Com. Code § 17.45(3), which includes partnership, corporation, association, or other group, however organized.

980. Defendants engage in "trade" or "commerce" as defined by Tex. Bus. & Com. Code § 17.45(6), which includes advertising, offering for sale, sale or distribution of any services and any property, tangible or intangible, real, personal or mixed, and any other article, commodity, or thing of value wherever situate, and includes any trade or commerce directly or indirectly affecting the people of Texas.

981. Defendants engaged in unfair and deceptive trade practices by representing to Texas Plaintiffs and Texas Subclass Members, as well as third party applications, that their data would be kept secure and that data would not be shared, when in fact Defendants regularly collected detailed consumer data.

982. Defendants further engaged in deceptive and unfair trade practices by failing to disclose to and concealing from Texas Plaintiffs and Texas Subclass Members that their detailed data was being collected and sold to third parties, who then used the data to make products and profit.

983. These deceptive statements, misrepresentations, and omissions, and concealments constitute violations of Tex. Bus. & Com. Code § 17.46(b).

984. Defendants violated Tex. Bus. & Com. Code § 17.46(b)(5), (9), and (20) and (24) by:

a. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Texas Plaintiffs' and Texas Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

b. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Texas Plaintiffs' and Texas Subclass Members' data for their own financial and commercial benefit;

c. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles; and

d. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Texas Plaintiffs' and the Texas Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent.

985. Texas Plaintiffs and Texas Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely,

the security and privacy of their data, including driving data, and their privacy in their own vehicles to their detriment.

986. Further, Defendants violated Tex. Bus. & Com. Code § 17.46(b)(2) and (3) by causing likelihood of confusion or misunderstanding as to the source, sponsorship, approval, certification, affiliation, connection, or association with Texas Plaintiffs' and Texas Subclass Members' data, namely that the collection and sale of such data was not authorized or consented-to by them, and therefore unlawfully obtained.

987. In engaging in the above-described practices, Defendants acted intentionally and with flagrant disregard of prudent and fair business practices to the extent that Defendant should be treated as having acted intentionally. Tex. Bus. & Com. Code § 17.45(13).

988. Texas Plaintiffs and Texas Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because substantial numbers of them have experienced economic loss.

989. As a direct and proximate result of Defendants' deceptive practices, Texas Plaintiffs and Texas Subclass Members have suffered and will continue to suffer injury, losses, and damages, including but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

990. Texas Plaintiffs and Texas Subclass Members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages, punitive damages, and reasonable attorneys' fees and costs.

COUNT THIRTY-SEVEN
Violation of the Utah Truth in Advertising Act,
Utah Code Ann. §§ 13.11a-1, *et seq.*
(On Behalf of the Utah Plaintiff and the Utah Subclass Against All Defendants)

991. Plaintiff Arellano (for the purposes of this count, the "Utah Plaintiff"), individually and on behalf of the Utah Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

992. Utah Plaintiff brings this claim on her own behalf and on behalf of each member of the Utah Subclass described above.

993. The Utah Truth in Advertising Act prohibits "deceptive, misleading, and false advertising practices and forms in Utah." Utah Code Ann. § 13.11a-1.

994. Defendants are each a "person" as defined by Utah Code Ann. § 13.11a-2(7).

995. Defendants engaged in the complained-of conduct in connection with "sales transaction[s]," as defined by Utah Code Ann. § 13.11a-2(15).

996. Defendants engaged in deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Utah Plaintiff and the Utah Subclass Members in violation of Utah Code Ann. § 13.11a-2(e), (g), and (i), including by:

a. Intercepting, collecting, using, and selling Utah Plaintiff's and Utah Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Utah Plaintiff's and Utah Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Utah Plaintiffs' and Utah Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of Utah Plaintiff's and the Utah Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Utah Plaintiff's and Utah Subclass Members' data.

997. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Utah Plaintiff's and Utah Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Utah Plaintiff's and Utah Subclass Members' data, including driving data, without obtaining their consent.

998. The fact that Defendants intercepted, collected, used, and sold Utah Plaintiff's and Utah Subclass Members' data was material to Utah Plaintiff and Utah Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

999. Utah Plaintiff and Utah Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding

the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

1000. Defendants intended to mislead Utah Plaintiff and Utah Subclass Members and induce them to rely on their misrepresentations and omissions.

1001. Defendants benefited from misleading Utah Plaintiff and Utah Subclass Members as it obtained a profit from the collection of data, including driving data.

1002. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

1003. Defendants' deceptive acts directly and proximately caused Utah Plaintiff and Utah Subclass Members to suffer damages including, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

1004. Utah Plaintiff and Utah Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages sustained or $2,000, whichever is greater, restitution, injunctive relief, and attorneys' fees and costs.

COUNT THIRTY-EIGHT
Violation of the Washington Consumer Protection Act ("Washington CPA"), Wash. Rev. Code §§ 19.86.010, *et seq.*
(On Behalf of the Washington Plaintiff and the Washington Subclass Against All Defendants)

1005. Plaintiff Williams (for the purposes of this count, the "Washington Plaintiff"), individually and on behalf of the Washington Subclass, repeat and reallege all preceding paragraphs, as if fully alleged herein.

1006. Washington Plaintiff brings this claim on his own behalf and on behalf of each member of the Washington Subclass described above.

1007. The Washington Consumer Protection Act ("Washington CPA") declares that unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful. Wash. Rev. Code § 19.86.020.

1008. Defendants are each a "person" as defined by Wash. Rev. Code § 19.86.010(1), which includes corporations, trusts, unincorporated associations and partnerships.

1009. Defendants engage in "trade" or "commerce" as defined by Wash. Rev. Code § 19.86.010(2), which includes the sale of assets or services, and any commerce directly or indirectly affecting the people of the state of Washington. Defendants have engaged in unfair practices by:

a. Intercepting, collecting, using, and selling Washington Plaintiff's and Washington Subclass Members' data without obtaining their consent;

b. Omitting, suppressing, and concealing the material fact that Defendants were intercepting, collecting, using, and selling Washington Plaintiff's and Washington Subclass Members' data to third parties for Defendants' own financial and commercial benefit;

c. Omitting, suppressing, and concealing the material fact that third parties collected, manipulated, used, and sold Washington Plaintiff's and Washington Subclass Members' data for their own financial and commercial benefit;

d. Omitting, suppressing, and concealing material facts regarding the functionality of Defendants' SDK and associated applications, including Routely, with respect to the privacy of consumers in their own vehicles;

e. Misrepresenting the purpose of Defendants' SDK and associated applications, including Routely, and that it would protect the privacy of

Washington Plaintiff's and the Washington Subclass Members' data, including that it would not intercept, collect, use, or sell such data without consumers' express consent; and

f. Failing to comply with common law and/or statutory duties pertaining to the privacy of Washington Plaintiff's and Washington Subclass Members' data.

1010. Defendants acted intentionally, knowingly, and maliciously to violate the Act, and recklessly disregarded Washington Plaintiff's and Washington Subclass Members' rights, because Defendants intentionally intercepted, collected, used, and sold Washington Plaintiff's and Washington Subclass Members' data, including driving data, without obtaining their consent.

1011. The fact that Defendants intercepted, collected, used, and sold Washington Plaintiff's and Washington Subclass Members' data was material to Plaintiff and Washington Subclass Members. This is a fact that reasonable consumers would consider important when choosing to purchase, use or download an application.

1012. Washington Plaintiff and Washington Subclass Members were deceived and/or could reasonably be expected to be deceived by Defendants' material misrepresentations and omissions regarding the functionality of Defendants' SDK and associated applications, including Routely, the security and privacy of their data, and their privacy to their detriment.

1013. Washington Plaintiff and Washington Subclass Members could not have reasonably avoided Defendants' practices as described herein because Defendants concealed their practices.

1014. Washington Plaintiff and Washington Subclass Members have derived no benefit from Defendants' surreptitious collection and exploitation of their private information, and there

are no countervailing benefits to them or to competition in engaging in the unauthorized tracking and sale of consumer data.

1015. Washington Plaintiff and Washington Subclass Members have been substantially injured by the practices described herein because their rights to privacy have been violated, and because substantial numbers of them have experienced economic loss. As such, Defendants' deceptive and unfair acts and practices affect the public interest as they have had the capacity to injure and have injured other persons.

1016. As a direct and proximate result of Defendants' unfair practices, Washington Plaintiff and Washington Subclass Members have suffered and will continue to suffer injury, losses, and damages, but not limited to: loss of privacy; unauthorized dissemination of their valuable data; damage to and diminution of the value of their personal information; the likelihood of future misuse of their data; and economic harm stemming from the exploitation of their data.

VIII. REQUEST FOR RELIEF

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

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

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.

IX. JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: May 27, 2025

Respectfully submitted,

/s/ Robert A. Clifford
Robert A. Clifford
rac@cliffordlaw.com
CLIFFORD LAW OFFICES, P.C.
120 North LaSalle Street, 36th Floor
Chicago, Illinois 60602
Tel.: (312) 899-9090

Liaison Counsel

/s/ Gary M. Klinger
Gary M. Klinger
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Tel.: (866) 252-0878

/s/ John A. Yanchunis
John A. Yanchunis
jyanchunis@forthepeople.com
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505

Interim Co-Lead Counsel

/s/ Tina Wolfson
Tina Wolfson
twolfson@ahdootwolfson.com
AHDOOT & WOLFSON PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel.: (310) 474-9111

/s/ Lesley E. Weaver
Lesley E. Weaver (SBN 191305)
lweaver@bfalaw.com
BLEICHMAR FONTI & AULD LLP
1330 Broadway, Suite 630
Oakland, California 94612
Tel.: (415) 445-4003

/s/ Julian C. Diamond
Julian C. Diamond
jdiamond@bursor.com
BURSOR & FISHER PA
1330 Avenue of the Americas, 32nd Floor
New York, New York 10019
Tel.: (646) 837-7150

/s/ Thomas E. Loeser
Thomas E. Loeser
tloeser@cpmlegal.com
COTCHETT, PITRE & MCCARTHY LLP
1809 7th Avenue, Suite 1610
Seattle, Washington 98101
Tel.: (206) 970-8181

/s/ Adele Daniel
Adele Daniel
adaniel@kellerrohrback.com
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3400
Seattle, Washington 98101
Tel.: (206) 623-1900

/s/ Sabita J. Soneji
Sabita J. Soneji (SBN 224262)
ssoneji@tzlegal.com
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Tel.: (510) 254-6808

/s/ Daniel O. Herrera
Daniel O. Herrera
dherrera@caffertyclobes.com
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Tel.: (312) 782-4880

/s/ Adam E. Polk
Adam E. Polk
apolk@girardsharp.com
GIRARD SHARP LLP
601 California Street, Suite 1400
San Francisco, CA 94108
Tel.: (415) 981-4800

/s/ Jeff Ostrow
Jeff Ostrow
ostrow@kolawyers.com
KOPELOWITZ OSTROW P.A.
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 332-4200

/s/ Rebecca Solomon
Rebecca Solomon
rsolomon@tousley.com
TOUSLEY BRAIN STEPHENS PLLC
1200 5th Avenue, Suite 1700
Seattle, Washington 98101
Tel.: (206) 667-0249

Plaintiffs' Executive Committee

/s/ Charles E. Schaffer
Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com