Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com
Jared Lucky (SBN 354413)
jlucky@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Schuyler Ufkes*
sufkes@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

**Pro hac vice admission to be sought*

Counsel for Plaintiff and the Putative Classes

IN THE UNITED STATES DISTRICT COURT

FOR NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

KYLE ATKINS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AMPLITUDE, INC., a Delaware corporation,

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR

(1) Violation of 18 U.S.C. § 2510, *et seq.*;
(2) Violation of Cal. Penal Code § 638.51;
(3) Violation of Cal. Penal Code § 502; and
(4) Violation of Cal. Penal Code § 631.

AND DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Kyle Atkins ("Plaintiff" or "Atkins") brings this Class Action Complaint and Demand for Jury Trial against Amplitude, Inc. ("Amplitude" or "Defendant") for surreptitiously tracking consumers' sensitive locations and capturing their in-app activities. Plaintiff alleges as follows upon personal knowledge as to himself and his own acts and experiences, and, as to all other matters, upon information and belief.

NATURE OF THE ACTION

1. Amplitude is a data analytics company that surreptitiously collects sensitive information about consumers and their mobile devices.

2. Amplitude developed and disseminated a software development kit (or "SDK") that enables backdoor access to consumers' devices and opens a data collection pipeline directly from consumers to Amplitude. Thousands of developers have embedded Amplitude's SDK into their mobile apps allowing them to siphon data from millions of consumers.

3. The data Amplitude collects from unsuspecting consumers is incredibly sensitive. Amplitude collects in-app consumer activity such as the pages they view and, in the case of shopping apps, the items they place in their shopping carts and the search terms they input. Even worse, Amplitude collects consumers' names and email addresses together with their geolocation data that reveals where a consumer lives, works, and the locations they frequent.

4. The collected location data reveals sensitive information about a consumer, for instance, their religious affiliation, sexual orientation, and medical condition allowing Amplitude to build a comprehensive profile on the consumer and their whereabouts.

5. Plaintiff and the Class are consumers whose sensitive location data and search terms (among other in-app activities and usage) have been obtained from their devices while using ordinary mobile apps with Amplitude's SDK embedded. Plaintiff and the Class do not know—nor could they—that the apps they regularly use have embedded Amplitude's SDK and, as such, did not (and could not) consent to Amplitude's data collection practices.

PARTIES

6. Plaintiff Kyle Atkins is a natural person and citizen of the State of California.

7. Defendant Amplitude, Inc is a corporation organized and existing under the laws of Delaware with its principal place of business located at 201 3rd Street, Suite 200, San Francisco, California 94103.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (i) at least one member of the Class is a citizen of a different state than any Defendant, (ii) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to this action.

9. This Court has personal jurisdiction over Defendant because Defendant conducts business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

10. Venue is proper pursuant to 28 U.S.C. § 1391(b) because defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in the District.

DIVISIONAL ASSIGNMENT

11. Pursuant to Civil Local Rule 3-2(c)–(d), this case should be assigned to the San Francisco Division because a substantial part of the events or omission giving rise to the claim occurred within the county of San Francisco.

COMMON FACTUAL ALLEGATIONS

Amplitude Surreptitiously Collects Precise Location Information and In-App Activity from Millions of Mobile Devices

12. Amplitude is a data analytics company. Their entire business model depends on collecting sensitive information from consumers' devices and sharing it with data partners such as advertising networks and data warehouses, among others. Amplitude collects sensitive timestamped geolocation data and consumer in-app activity.

13. The secret to Amplitude's data pipeline is the collection of what the advertising industry calls "first-party data," or data collected directly from consumers. Amplitude accomplishes this task by developing a SDK.

14. SDKs are a collection of reusable and packaged pieces of computer code that perform specific functions and processes. Software developers can integrate SDKs into their applications to save time and execute specific tasks.

15. On information and belief, over 40,000 mobile app developers integrated Amplitude's SDK. These apps include, among others, shopping, productivity, dating, and gaming apps.

16. Amplitude surreptitiously collects sensitive data from consumers through its SDK in real time. Amplitude collects identity information such as the consumer's name and email address, mobile advertisings IDs ("MAIDs"), and device fingerprint data (which includes the consumer's device make and model, screen resolution, and operating system version).

17. Amplitude also collects precise and timestamped latitude and longitude geolocation coordinates from consumers' devices. This allows Amplitude to amass a database of consumers' whereabouts in real time.

18. At the forefront of Amplitude's data collection practices is obtaining consumer in-app activities in real time. Amplitude collects in-app search terms entered by the consumer, the pages requested by the consumer, and—in the case of certain shopping apps—the products the consumer viewed and the content of his or her shopping cart (collectively, the "In-App Activity").

19. Indeed, Amplitude designed its SDK to intercept the content of electronic communications between the consumer and the mobile app. Consumers entering text into a field in a mobile app or pressing a button intend to send messages to, or otherwise communicate with, the mobile app. Similarly, a mobile app rendering search results, a product page, or a web page also communicates with the consumer in response to his or her request. Amplitude's SDK collects, in real-time, the messages and/or communications intended for the mobile app such as search queries the consumer enters and sends to the mobile app service as well as the content of forms they fill out.

20. In the case of the DoorDash food delivery app, which embedded Amplitude's SDK, Amplitude collects sensitive consumer data. When logging into DoorDash, consumers can utilize the search bar to find food and/or restaurants in their area. Unbeknownst to consumers, Amplitude

collects all in-app selections such as the consumer's search terms, restaurants they viewed, meals and other products they added to their shopping cart, and precise current geolocation coordinates, in real time, including the consumer's name and email address.

21. The problem with Amplitude is that consumers do not know that by interacting with an app which has embedded Amplitude's SDK that their sensitive data is being surreptitiously siphoned off by an unknown third party. Consumers are never informed about Amplitude's SDK being embedded into the app, they never consent to Amplitude's data collection practices, nor are they allowed to opt-in or opt-out of Amplitude's data collection practices—if they even know who or what Amplitude is.

22. When enabling location services within an app—for example a dating app or a shopping app that necessarily requires the consumer to share his or her location *with the app*—the consumer grants consent *for only the mobile app* to use his or her location. Similarly, consumers inputting text in an app or selecting buttons intend to communicate with the mobile app service. At no point does Amplitude inform consumers that its SDK is collecting their sensitive geolocation data and In-App Activity, nor does it prompt consumers to grant Amplitude permission to access or collect any data whatsoever.

23. In the case of DoorDash, consumers are not informed by DoorDash, Amplitude, or anyone else that Amplitude's SDK is collecting their geolocation information and In-App Activity, nor are consumers prompted to grant Amplitude permission to access or collect any data whatsoever.

24. On information and belief, a consumer would never know whether any given app has the Amplitude SDK third-party eavesdropping and tracking software embedded. The entire data collection process takes place surreptitiously without the consumer's knowledge or consent.

25. Amplitude's interception of a consumer's In-App Activity reveals information about the consumer's interests, the apps they downloaded on to their phone, preferences, and shopping histories.

Amplitude's Data Collection Reveals Sensitive Information About Consumers

26. Amplitude's practice is far from inconsequential. Its surreptitious and routine collection of precise geolocation data reveals locations associated with medical care, reproductive health, religious worship, mental health, and temporary shelters such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery centers. As such, Amplitude's data collection may reveal, for instance, a consumer's religious affiliation, sexual orientation, medical condition, and even whether the consumer is part of an at-risk population.

27. Amplitude has also intercepted consumers' communications with mobile apps, which reveals information about a given consumer's interests, the apps downloaded onto their phone, preferences, and even shopping histories.

28. Amplitude has collected and correlated a vast amount of personal information about consumers without their knowledge and consent. Indeed, Amplitude collects information across multiple apps and identifies each consumer by a unique ID thus creating a digital dossier for the consumer, which includes information about the locations they have visited, the apps they use, their In-App Activity, and their interests, among other things.

29. To make matters worse, Amplitude has created a platform that allows the sharing of the data it harvested with even more unknown third parties. For example, Amplitude created integrations to share data with marketing and advertising platforms such as Facebook Ads, Google Ads, TikTok Ads, and Snapchat Ads.

30. Amplitude has also developed artificial intelligence tools to analyze the data it has surreptitiously and without consent collected from consumers. Amplitude admits that it built its Artificial Intelligence tools from "over 40 trillion [consumer] events processed." Events, of course, are in-app consumer interactions such as the search terms a consumer inputs and other in-app choices.

31. Ultimately, Amplitude's SDK has allowed it to secretly create a detailed log of Plaintiff's and the putative Class's precise movement patterns, along with a dossier of their likes and interests, all without their consent or permission.

FACTS SPECIFIC TO PLAINTIFF

32. Plaintiff Atkins downloaded and used the DoorDash food delivery and shopping app on his Android device within the last year.

33. To use the DoorDash mobile app, Plaintiff enabled location services for the sole purpose of sharing his location with DoorDash. The developers of the DoorDash mobile app have embedded the Amplitude SDK into their mobile app allowing Defendant to collect his timestamped geolocation information, device IDs, device fingerprint data, information about which app(s) he uses on his mobile device, search terms he input into the DoorDash app, the products he placed in his shopping cart, and the restaurants and products he viewed. Furthermore, Amplitude collected his name and email address and correlated his In-App Activity and geolocation information with him.

34. Plaintiff did not grant Defendant consent or permission to collect any information from his device whatsoever, let alone his precise geolocation information and In-App Activity.

35. Neither Defendant nor DoorDash informed or otherwise disclosed to Plaintiff that Amplitude's SDK was embedded in the DoorDash app, or that if he used the DoorDash app, Defendant would collect his personally identifiable information, precise geolocation information, and In-App Activity. Plaintiff did not consent to Defendant's collection.

CLASS ACTION ALLEGATIONS

36. **Class Definitions**: Plaintiff Kyle Atkins brings this proposed class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and Rule 23(b)(3) on behalf of himself and a Class and Subclass (collectively the "Classes") of others similarly situated, defined as follows:

> **Class**: All individuals who downloaded and used an app on their mobile device (1) with the Amplitude SDK embedded into the app and (2) that did not publicly disclose "Amplitude" in any of the app's notices or disclosures.
>
> **California Subclass**: All California residents who downloaded and used an app on their mobile device (1) with the Amplitude SDK embedded into the app and (2) that did not publicly disclose "Amplitude" in any of the app's notices or disclosures.

Excluded from the Classes are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest and its

officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

37. **Numerosity**: The exact number of Class members is unknown and not available to Plaintiff at this time, but it is clear that individual joinder is impracticable. On information and belief, Defendant has surreptitiously collected timestamped geolocation information and the In-App Activity of millions of consumers who fall into the definition of the Class and Subclass. Class members can be identified through Defendant's records.

38. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the putative Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

(a) Whether Defendant intercepted the contents of communications from Plaintiff and the Classes;

(b) Whether Defendant used a pen register;

(c) Whether Defendant obtained consent from Plaintiff and the Classes or otherwise obtained a warrant to install and use a pen register;

(d) Whether Defendant accessed Plaintiff's and the Classes' computer systems;

(e) Whether Defendant made an unauthorized connection with Plaintiff's and the Classes' mobile devices; and

(f) Whether Defendant used or attempted to use any information obtained from Plaintiff's and the Classes' mobile devices.

39. **Typicality**: Plaintiff's claims are typical of the claims of members of the Classes in that Plaintiff, like all members of the Classes, has been injured by Defendant's misconduct at issue.

40. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex

litigation and class actions. Plaintiff's claims are representative of the claims of the other members of the Classes. That is, Plaintiff and the members of the Classes sustained damages as a result of Defendant's conduct. Plaintiff also has no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to the Classes.

41. **Superiority**: Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Classes is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions will be ensured.

42. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definitions" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of Wiretap Act
18 U.S.C. § 2510, *et seq.*
(On behalf of Plaintiff and the Class)

43. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

44. The Wiretap Act generally prohibits the intentional "intercept[ion]" of "wire, oral, or electronic communication[s]." 18 U.S.C. § 2511(1)(a).

45. By designing the Amplitude SDK to contemporaneously and secretly collect In-App Activity—including the search terms and other text input into mobile apps by Plaintiff and the Class members—Defendant Amplitude intentionally intercepted and/or endeavored to intercept the contents of "electronic communication[s]" in violation of 18 U.S.C. § 2511(1)(a).

46. Plaintiff and the Class did not consent to Defendant's collection, interception, or use

of the contents of their electronic communications. Nor could they—Defendant's collection of In-App Activity is entirely without the Plaintiff's and the Class's knowledge. Indeed, when Plaintiff and the Class interacted with a mobile app that embedded the Amplitude SDK, Amplitude did not announce its presence nor inform Plaintiff and the Class that it is collecting, intercepting, or using the content of the communications intended for the mobile app.

47. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff and the Class because it used the intercepted communications for its own purposes. Defendant Amplitude used Plaintiff's and the Class's In-App Activity to correlate data across various mobile apps to create a unified customer profile that included Plaintiff's and the Class members' In-App Activity and interests. Furthermore, Defendant used Plaintiff's and the Class's In-App Activity to develop and train its Artificial Intelligence.

48. Defendant never obtained any consent whatsoever from Plaintiff and the Class.

49. Plaintiff and the Class suffered harm as a result of Defendant's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(c)(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of California Invasion of Privacy Act
Cal. Penal Code § 638.51
(On behalf of Plaintiff and the California Subclass)

50. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

51. California law prohibits the installation of a pen register without first obtaining a court order. Cal. Penal Code § 638.51.

52. The statute 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." Cal. Penal Code § 638.50(b).

53. Defendant's SDK is a "pen register" because it is a device or process that records addressing or signaling information—in this instance, Plaintiff's and the California Subclass members' location and personal information—from electronic communications transmitted by their devices. Furthermore, Defendant's SDK is device or process that gathers data, identifies consumers, and correlates data across various mobile apps to ascertain Plaintiff's and the California Subclass members' In-App Activity and interests.

54. Defendant was not authorized by any court order to use a pen register to track Plaintiff's and the California Subclass members' location and personal information, nor did it obtain consent from Plaintiff and the California Subclass to operate such a device.

55. Plaintiff and the California Subclass seeks injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

THIRD CAUSE OF ACTION
Violation of the California Comprehensive Computer Data Access and Fraud Act
Cal. Penal Code § 502
(On behalf of Plaintiff and the California Subclass)

56. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

57. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act ("CDAFA") to "expand 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). In enacting the statute, the Legislature emphasized the need to protect individual privacy: "[The] Legislature further finds and declares that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals[.]" *Id.*

58. Plaintiff's and the California Subclass members' mobile devices are "computers" or "computer systems" within the meaning of Section 502(b) because they are devices capable of being used in conjunction with external files and perform functions such as logic, arithmetic, data storage and retrieval, and communication.

59. Defendant violated the following sections of CDAFA § 502(c):

a. "Knowingly accesses and without permission . . . uses any data, computer, computer system, or computer network in order to . . . wrongfully control or obtain money, property, or data." *Id.* § 502(c)(1).

b. "Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network." *Id.* § 502(c)(2).

c. "Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network." *Id.* § 502(c)(7).

60. Defendant "accessed" Plaintiff's and the California Subclass members' computers and/or computer systems because it gained entry to and/or caused output from their mobile devices to obtain geolocation information and personal information.

61. Defendant was unjustly enriched with the data it obtained from Plaintiff and the California Subclass.

62. Plaintiff and the California Subclass now seek compensatory damages, injunctive relief, disgorgement of profits, other equitable relief, punitive damages, and attorneys' fees pursuant to § 502(e)(1)–(2).

FOURTH CAUSE OF ACTION
Violation of the California Wiretap Act
Cal. Penal Code § 631
(On behalf of Plaintiff and the California Subclass)

63. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

64. The California Wiretap Act, Cal. Penal Code § 631, prohibits:

> Any person [from using] any machine, instrument, or contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electrically, 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[.]

65. Defendant's SDK intercepted Plaintiff's and California Subclass members' specific input events such as the content of their search terms, page views, button presses, and other choices on their mobile devices, including their affirmative actions (such as installing a mobile app on their device), and therefore constitute communications within the scope of the California Wiretap Act.

66. Defendant's SDK made an unauthorized connection with Plaintiff's and the California Subclass members' devices and obtained their sensitive information including their movements, geolocation information, search terms, In-App Activity, mobile device IDs, device fingerprint data, and information about the mobile app(s) they downloaded.

67. Plaintiff and the California Subclass did not consent to Defendant's collection or use of their communications. Nor could they—Defendant's collection of In-App Activity is entirely without the Plaintiff's and the California Subclass's knowledge. Indeed, when Plaintiff and the California Subclass interacted with a mobile app that embedded the Amplitude SDK, Amplitude did not announce its presence nor inform Plaintiff and the California Subclass that it is collecting or using the content of the communications intended for the mobile app.

68. Furthermore, Defendant did not act as a mere extension of the mobile app used by Plaintiff and the California Subclass because it used the collected communications for its own purposes. Defendant Amplitude used Plaintiff's and the California Subclass's In-App Activity to develop and train its Artificial Intelligence systems.

69. Furthermore, Defendant attempted to and/or shared the data it wrongfully obtained from Plaintiff and the California Subclass to third parties including advertisers and other platforms.

70. Defendant never obtained any consent whatsoever from Plaintiff and the California Subclass.

71. Plaintiff and the California Subclass seek an injunction and damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kyle Atkins individually and on behalf of the Classes, prays for

the following relief:

(a) An order certifying the Class and the California Subclass as defined above, appointing Kyle Atkins as the representative of the Class and the California Subclass, and appointing his counsel as Class Counsel;

(b) An order declaring that Defendant's actions, as set out above violate the Wiretap Act, 18 U.S.C. § 2510; the California Invasion of Privacy Act, Cal. Penal Code § 638.51; the California Comprehensive Computer Data Access and Fraud Act, Cal Penal Code § 502; and the California Wiretap Act, Cal. Penal Code § 631.

(c) An injunction requiring Defendant to cease all unlawful activities;

(d) An award of liquidated damages, disgorgement of profits, punitive damages, costs, and attorneys' fees;

(e) Such other and further relief that the Court deems reasonable and just.

JURY DEMAND

Plaintiff requests a trial by jury of all claims that can be so tried.

Respectfully submitted,

KYLE ATKINS, individually and on behalf of all others similarly situated,

Dated: August 8, 2024

By: */s/ Rafey S. Balabanian*
One of Plaintiff's Attorneys

Rafey Balabanian (SBN 315962)
rbalabanian@edelson.com
Jared Lucky (SBN 354413)
jlucky@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: 415.212.9300
Fax: 415.373.9435

Schuyler Ufkes*
sufkes@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor

Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

*Pro hac vice admission to be sought

Counsel for Plaintiff and the Putative Classes