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 Class

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FELIX KOLOTINSKY, individually and on behalf of all others similarly situated, *Plaintiff,* v. AMAZON.COM, Inc., a Delaware corporation, and AMAZON ADVERTISING, LLC, a Delaware limited liability company *Defendants*.	Case No.: **CLASS ACTION COMPLAINT FOR:** **(1) Violation of Cal. Penal Code § 638.51;** **(2) Violation of Cal. Penal Code § 502** **DEMAND FOR JURY TRIAL**

Plaintiff Felix Kolotinsky ("Plaintiff" or "Kolotinsky") brings this Class Action Complaint and Demand for Jury Trial against Amazon, Inc. and Amazon Advertising, LLC (collectively "Defendants" or "Amazon") for surreptitiously tracking and selling California residents' sensitive movements and locations. 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. Amazon is a technology company and a data aggregator that surreptitiously collects and sells information about consumers obtained from their mobile devices.

2. Amazon developed and disseminated a software development kit ("SDK") called the Amazon Ads SDK that enables backdoor access to consumers' devices and opens a direct data collection pipeline to Amazon and its advertising partners. On information and belief, tens of thousands of app developers have embedded Amazon's Ads SDK into their mobile apps, allowing Amazon to siphon data from consumers.

3. The data that Amazon collects from unsuspecting consumers is incredibly sensitive. Amazon collects timestamped geolocation data that reveals where a consumer lives and works, and which locations they frequent. The collected location data reveals sensitive information about each consumer, such as their religious affiliation, sexual orientation, and medical conditions. This enormous volume of data enables Amazon and its advertising partners to build a comprehensive profile about each consumer, including their movements and whereabouts.

4. Plaintiff and the putative Class are consumers whose sensitive data, including their location data, has been collected by Amazon in violation of Cal. Penal Code § 638.51 and Cal. Penal Code § 502. Neither Plaintiff nor any member of the putative Class has ever agreed to allow Amazon to collect or sell their sensitive data and there is no mechanism to opt out of Amazon's data collection practices.

PARTIES

5. Plaintiff Felix Kolotinsky is a natural person and citizen of the State of California.

6. Defendant Amazon.com, Inc. is a corporation organized and existing under the laws of Delaware with its principal place of business located at 410 Terry Avenue North, Seattle, Washington 98109.

7. Defendant Amazon Advertising, LLC is a limited liability company organized and existing under the laws of Delaware with its principal place of business located at 410 Terry Avenue North, Seattle, Washington 98109.

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 Defendants because Defendants conduct business in this District, have offices in California, 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 Plaintiff resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred, in a substantial part, in the District.

COMMON FACTUAL ALLEGATIONS

Amazon Surreptitiously Collects Precise Location Information from Millions of Mobile Devices

11. Amazon is a technology company that operates an advertising network. Their business model is to collect information from consumers and sell access to its ill-gotten data to brands and advertisers. Among the sensitive data Amazon collects from consumers is timestamped geolocation data.

12. The secret to Amazon's data pipeline is the collection of what the ad industry calls "first-party data," or data collected directly from consumers. Amazon accomplishes this task by developing an SDK called Amazon Ads.

13. 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.

14. Various developers have integrated the Amazon Ads SDK into their mobile apps. These apps include, among others NewsBreak and Speedtest by Ookla.

15. Amazon contracted with Speedtest by Ookla to provide its Amazon Ads SDK to be embedded in the Speedtest app. Amazon designed the Amazon Ads SDK so that Amazon could

collect sensitive consumer data from consumers, including Speedtest users, despite Amazon not having their consent to collect such data.

16. Amazon surreptitiously collects sensitive data from consumers through its Amazon Ads SDK. Amazon collects precise and timestamped latitude and longitude geolocation coordinates from consumers' devices, mobile advertising IDs ("MAIDs"), and device fingerprint data.

17. Device fingerprint data includes information about the consumer's hardware and software such as their device make and model, current operating system version, screen size, pixel density, among others.

18. The problem with the Amazon Ads SDK is that consumers do not know that by interacting with an app which has embedded the SDK that their sensitive data is being surreptitiously siphoned off by an unknown third party. Consumers are never informed about Amazon's SDK nor are they allowed to opt-in or opt-out of Amazon's data collection practices—if they even know what the Amazon Ads SDK is, let alone that it is embedded in the apps they are using. Amazon's unauthorized data collection was neither incidental nor accidental, but designed to covertly siphon sensitive data from consumers' mobile devices.

19. Indeed, when enabling location services within an app—for example a utility tool or a news 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. At no point does Amazon inform consumers that its SDK is collecting their sensitive geolocation data, nor does it prompt consumers to grant Amazon permission to access or collect any data whatsoever.

20. On information and belief, a consumer would not know that any given app has the Amazon Ads SDK third-party tracking software embedded. The entire data collection process takes place surreptitiously without the consumer's knowledge or consent.

Amazon Ensures that Collected Consumer Data Does Not Remain Anonymous

21. As a preliminary matter, geolocation information is sensitive data that necessarily reveals a consumer's identity. Geolocation coordinates together with timestamp data—exactly the

type of data Amazon collects—can reveal a consumer's home address, work address, and any other location they visit.

22. Indeed, researchers from MIT found that a small location data sample is sufficient to identify an individual. The researchers analyzed timestamped location data for 1.5 million individuals over 15 months and found that only four timestamped locations are sufficient to identify 95% of individuals. Given 11 data points, the researchers could identify all individuals in the study. The reason for the findings is obvious: individuals have unique movement patterns, and it is not likely that someone else will be in the same locations at four different times of the day.

23. The researchers commented that an individual may be identified with less than four data points simply by exploiting irregularities in an individual's behavior.

24. By collecting timestamped geolocation data, unique device identifiers, and device fingerprint data, Amazon can connect an ostensibly "anonymous" ID (such as a MAID or other unique device identifier) to an individual and then collect data on their interests and activities.

25. Amazon touts that it uses its technology to identify consumers by "harness[ing] billions of unique, proprietary signals . . . even when ad identifiers are not present." Indeed, Amazon promises its advertisers that "it leverages unique first-party data and AI to deliver impactful ads even without traditional identifiers, ensuring your campaigns remain effective in a changing landscape."

26. Most importantly, Amazon creates a comprehensive consumer profile by combing both online and in-person consumer activities. Amazon's advertising network offers its advertisers "easy-to-use tools and billions of proprietary audience signals *informed by online and offline touchpoints*." (emphasis added). These touchpoints include consumers' Amazon shopping activities and the locations they visit. Amazon explains, "audience insights are informed by billions of signals, including Amazon shopping signals, to build a holistic picture of a particular audience."

Amazon's Data Collection Reveals Sensitive Information About Consumers

27. Amazon's practice is far from inconsequential. Its surreptitious and routine collection of precise geolocation data can reveal 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, Amazon'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.

28. Amazon has effectively fingerprinted consumers and has correlated a vast amount of personal information about them entirely without consumers' knowledge and consent. Amazon has created profiles on consumers including information about locations they have visited and "billions of unique proprietary signals" including their "Amazon shopping signals."

29. Ultimately, the Amazon Ads SDK has allowed Amazon 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

30. Plaintiff Kolotinsky downloaded the "Speedtest by Ookla" app on his Android device and has used it within the last year.

31. While using the Speedtest mobile app, Plaintiff enabled location services for the sole purpose of sharing his location with Speedtest. The developers of the Speedtest mobile app have embedded the Amazon Ads SDK into their mobile app, allowing Amazon to collect Plaintiff's timestamped geolocation information, unique device IDs, device fingerprint data, and information about which locations he visited.

32. Plaintiff did not grant Amazon consent or permission to collect any information from his device whatsoever, let alone his precise geolocation information.

33. Prior to collecting timestamped geolocation information, unique device IDs, device fingerprint data, and information about which locations he visited, neither Amazon nor Speedtest informed or otherwise disclosed to Plaintiff that Amazon's Ads SDK was embedded in the Speedtest app, or that if he used the Speedtest app, Amazon would collect his precise geolocation information. Plaintiff did not consent to Amazon's collection.

CLASS ACTION ALLEGATIONS

34. **Class Definition**: Plaintiff Felix Kolotinsky 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 of others similarly situated, defined as follows:

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

Excluded from the Class 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 Class; (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.

35. **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, Defendants have surreptitiously collected timestamped geolocation information from millions of consumers who fall into the definition of the Class. Class members can be identified through Defendants' records.

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

(a) Whether Defendants used a pen register;

(b) Whether Defendants obtained consent from Plaintiff and the Class or otherwise obtained a warrant to install and use a pen register;

(c) Whether Defendants accessed Plaintiff's and the Class's computer systems; and

(d) Whether Defendants sought Plaintiff's and the Class's permission to access their computer systems.

37. **Typicality**: Plaintiff's claims are typical of the claims of the Class members in that Defendant accessed Plaintiff's device and siphoned his geolocation information and other personal information without his consent, causing him the same injuries Defendant caused all other members of the Class.

38. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class 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 Class. That is, Plaintiff and the Class members sustained damages as a result of Defendants' conduct. Plaintiff also has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiff nor his counsel has any interest adverse to the Class.

39. **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 Class 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.

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

FIRST CAUSE OF ACTION
Violation of Cal. Penal Code § 638.51
(On behalf of Plaintiff and the Class)

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

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

43. 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).

44. Defendants' 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 Class members' timestamped geolocation information and identifying information such as their MAIDs and device fingerprint data—from electronic communications transmitted by their devices. Furthermore, Defendants' SDK is a device or process that identifies consumers, gathers data, and correlates data through sophisticated device fingerprinting and its consumer identification functionality.

45. Defendants were not authorized by any court order to use a pen register to track Plaintiff's and Class members' location and personal information, nor did it obtain consent from Plaintiff and the Class to operate such a device.

46. Plaintiff and the Class seek injunctive relief and statutory damages in the amount of $5,000 per violation pursuant to Cal. Penal Code § 637.2.

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

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

48. 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.*

49. Plaintiff's and the Class members' mobile devices are "computers" or "computer systems" within the meaning of § 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.

50. 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).

51. Defendants knowingly "accessed" Plaintiff's and the Class members' computers and/or computer systems because it purposefully gained entry to and/or caused output from their mobile devices to obtain geolocation information and personal information.

52. Plaintiff and the Class suffered damage and/or loss resulting from Defendants' conduct described herein. Specifically, (1) Defendants' SDK occupied Plaintiff's and the Class's storage space on their devices without authorization, (2) Defendants' SDK caused data to be output from Plaintiff's and the Class's mobile devices over their cellular data plan, (3) Defendants' acts used computer resources of the device, and (4) Defendants were unjustly enriched and profited from the data taken from Plaintiff and the Class.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Felix Kolotinsky individually and on behalf of the Class, prays for the following relief:

(a) An order certifying the Class as defined above, appointing Felix Kolotinsky as the representative of the Class, and appointing his counsel as Class Counsel;

(b) An order declaring that Defendants' actions, as set out above, violate Cal. Penal Code § 638.51; and violate the California Computer Data Access and Fraud Act, Cal. Penal Code § 502.

(c) An injunction requiring Defendants 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,

FELIX KOLOTINSKY, individually and on behalf of all others similarly situated,

Dated: January 29, 2025

By: */s/ Jared Lucky*
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 Class