Joshua B. Swigart (SBN 225557)
Josh@SwigartLawGroup.com
SWIGART LAW GROUP, APC
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
P: 866-219-3343
F: 866-219-8344

Attorneys for Plaintiff David Greenly and The Putative Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

DAVID GREENLEY, individually and on behalf of others similarly situated, Plaintiff, vs. Kochava, Inc., Defendant.	CASE NO: '22CV1327 BAS AHG CLASS ACTION COMPLAINT FOR DAMAGES: 1. UNLAWFUL WIRETAPPING AND INTERCEPTION OF ELECTRONIC COMMUNICATIONS, CAL. PEN. CODE § 631 2. UNLAWFUL RECORDING OF CONFIDENTIAL TELEPHONE CALLS, CAL. PEN. CODE § 632 3. UNLAWFUL RECORDING OF CELLULAR TELEPHONE CALLS, CAL. PEN. CODE § 632.7 4. UNLAWFUL USE OF ELECTRONIC TRACKING DEVICE UNDER CAL. PEN. CODE § 637.7 **JURY TRIAL DEMANDED**

INTRODUCTION

1. David Greenley ("Plaintiff"), individually and on behalf of all other similarly situated California residents ("Class Members"), brings this action for damages and injunctive relief against Kochava, Inc. ("Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, related entities for violations of the California Penal Code § 630, et seq., ("CIPA") including § 631 Wiretapping in relation to the unauthorized collection, recording, and dissemination of Plaintiff's and Class Members' data.

2. The California State Legislature passed CIPA in 1967 to protect the right of privacy of the people of California. The California Penal Code is very clear in its prohibition against unauthorized tapping or connection without the consent of the other person: "Any person who, by means of any machine, instrument, or contrivance, or any other matter, intentionally taps, or makes any unauthorized connection . . . 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 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 [violates this section]." Penal Code § 631(a).

3. The California State Legislature passed CIPA in 1967 to protect the right of privacy of the people of California, replacing prior laws, which permitted the recording of telephone conversations with the consent of one party to the conversation. The California Penal Code is very clear in its prohibition against unauthorized recording without the consent of the other person to the conversation: "Every person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying

or recording device, eavesdrops upon or records the confidential communication [violates this section]." Penal Code § 632(a).

4. In addition to the general protections afforded to confidential communications by California Penal Code §632, California Penal Code § 632.7 was added to CIPA in 1992 due to specific privacy concerns over the increased use of cellular and cordless telephones. Section 632.7 prohibits secretly recording all communications involving cellular and cordless telephones, not just confidential communications. Penal Code 637.2 permits Plaintiff to bring this action for any violation of Penal Code § 632 and provides for statutory damages of $5,000 for each violation.

5. Defendant made an unauthorized connection with Plaintiff's mobile device when Defendant collected and stored geolocation data specific to each consumer's mobile device and then provided such information to its clients for the purposes of targeted advertising.

6. Plaintiff brings this action for every violation of California Penal Code § 631 which provides for statutory damages of $2,500 for each violation, pursuant to California Penal Code § 631(a), and Penal Code § 632 for statutory damages of $5,000 for each violation under Penal Code § 637.2.

7. Defendant collected, sold, licensed, and transferred Plaintiff's precise geolocation data which were associated to visits to sensitive locations without Plaintiff's knowledge or consent. These actions cause or are likely to cause substantial injury to Plaintiff which are not outweighed by any benefits to the consumer or competition.

8. Plaintiff brings this class action on behalf of a class with four subclasses, as more fully defined infra, consisting of the Confidential Communication class.

9. Plaintiff makes these allegations on information and belief, with the exception of those allegations that pertain to Plaintiff, or to Plaintiff's counsel, which Plaintiff alleges on his personal knowledge.

10. Unless otherwise stated, all the conduct engaged in by Defendant took place in California.

11. All violations by Defendant were knowing, willful, and intentional, and Defendant did not maintain procedures reasonably adapted to avoid any such violation.

12. Unless otherwise indicated, the use of Defendant's name in this Complaint includes all agents, employees, officers, members, directors, heirs, successors, assigns, principals, trustees, sureties, subrogees, representatives, and insurers of the named Defendant.

JURISDICTION & VENUE

13. Jurisdiction is proper under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because Plaintiff, a resident of the State of California, seeks relief on behalf of a California class, which will result in at least one class member belonging to a different state than that of Defendant, a Delaware Corporation with its principal place of business in Idaho.

14. Plaintiff is requesting statutory damages of $2,500 per violation of Cal. Penal Code §631, $5,000 per violation of §632 under §637.2, and $5,000 per violation of §637.7 under §637.2, per unlawful interception, which, when aggregated among a proposed class number in the tens of thousands, exceeds the $5,000,000 threshold for federal court jurisdiction under CAFA.

15. Therefore, both diversity jurisdiction and the damages threshold under CAFA are present, and this Court has jurisdiction.

16. Because Defendant conducts business within the State of California, personal jurisdiction is established.

17. Venue is proper pursuant to 28 U.S.C. § 1391 for the following reasons: (i) the conduct complained of herein occurred within this judicial district; and (ii) Defendant conducted business within this judicial district at all times relevant.

PARTIES

18. Plaintiff is, and at all times mentioned herein was, a natural person and resident of the State of California who regularly visits and conducts business in the County of San Diego.

19. Defendant is, and at all times mentioned herein was, a Delaware corporation with its principal place of business located at 201 Church Street, Standpoint, Idaho.

20. Defendant has registered an agent of process with the Idaho Secretary of State, Doug Lieuallen, 201 Church Street, Sandpoint, Idaho 83864. Plaintiff alleges that at all times relevant herein Defendant conducted business in the State of California, in the County of San Diego, within this judicial district.

21. Defendant is, and at all times mentioned herein was, a "person", as defined by Cal. Pen. Code § 632(b).

Factual Allegations

Defendant Sells Precise Location Information for Millions of Mobile Devices

22. On August 29, 2022, the Federal Trade Commission filed a federal lawsuit against Defendant for its market conduct in illegally gathering geo-location data ("FTC Complaint").

23. The following factual summary includes facts obtained from the FTC Complaint; the Defendant's statements on its own website, and various other reliable public sources of information describing Defendant's data gathering business practices.

24. Defendant is, among other things, a location data broker that provides its customers massive amounts of precise geolocation data collected from consumer's mobile devices.

25. Defendant collects a wealth of information about consumers and their mobile devices by, among other means, purchasing data from other data brokers to sell to its own customers.

26. Defendant then sells customized data feeds to its clients to assist in advertising and analyzing foot traffic at stores or other locations. Defendant sells

timestamped latitude and longitude coordinates showing the location of mobile devices.

27. As noted in Defendant's explanation, each pair or timestamped latitude and longitude coordinates is associated with a "device_id_value," which is also known as 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. 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.

28. In describing its product in the online marketplace, Defendant has asserted that it offers "rich geo data spanning billions of devices globally." Defendant further claimed that its location data feed "delivers raw latitude/longitude data with volumes around 94[billion]+ geo transactions per month, 125 million monthly active users, and 35 million daily users, on average observing more than 90 daily transactions per device."

Defendant Provides Public Access to Plaintiff and Class Members' Location Data

29. According to the FTC Complaint, Defendant has sold access to its data feeds on online data marketplaces that are publicly accessible. Defendant typically charges a monthly subscription fee of thousands of dollars to access its location data feed but has also offered a free sample (the "Kochava Data Sample").

30. Defendant has made the Kochava Data Sample publicly available with only minimal steps and no restrictions on usage.

31. For example, according to the FTC the Kochava Data Sample was available on the Amazon Marketplace until approximately June 2022. In order to access the sample data feed, a purchaser simply needed a free AWS account. A purchaser would then search the AWS marketplace for "Kochava," which resulted in two available datasets – a $25,000 location data feed subscription and the free Kochava Data Sample.

32. The Kochava Data Sample consisted of a subset of the paid data feed, covering a rolling seven-day period. It was formatted as a text file, which could be converted into a spreadsheet, which contained over 327,480,000 rows and 11 columns of data, corresponding to over 61,803,400 unique mobile devices.

33. The FTC Complaint further explained that when an AWS purchaser clicked "subscribe" for the Kochava Data Sample feed, the purchaser was directed to a screen that included a "Subscription terms" notification that stated the Kochava Data Sample "has been marked by the provider [i.e., Kochava] as containing sensitive categories of information."

34. Below this notice, a form was displayed, requesting the purchaser's company name, name of purchaser, email address, and intended use case.

35. A purchaser could use an ordinary personal email address and describe the intended use simply as "business." The request would then be sent to Defendant for approval. Defendant has approved such requests in as little as 24 hours.

36. Once Defendant approved the request, the purchaser was notified by email and then gained access to the data, along with a data dictionary explaining the categories of data provided as detailed within the FTC Complaint.

37. The Kochava Data Sample included precise location data gathered in the seven days prior to the date Defendant approved the subscription request.

Defendant's Data Practices and Business Model

38. Defendant gathers and tracks specific consumer geolocation and other data about consumers, then combines it with other consumer data to create consumer reporting about individual consumers by tracking their mobile phone location and corresponding smartphone application and click-thru activity and usage.

39. According to Defendant's own website, "Kochava is the industry standard for secure, real-time data solutions. We help people-based marketers establish identity, define and activate audiences, and measure and optimize their marketing

across connected devices." https://www.kochava.com/company/ last accessed August 30, 2022.

40. Defendant also states that,

> Kochava Inc. is a real-time data solutions company offering the leading omni-channel measurement and attribution solutions for data-driven marketers. The Marketers Operating System™ (m/OS) from Kochava empowers advertisers and publishers with a platform that seamlessly integrates and manages customer identity, measurement, and data controls. Unlike the complicated, siloed tech stacks employed today, the m/OS takes the next step: unifying all of your data and critical omni-channel solutions into a cohesive, operational system that goes beyond data aggregation and reporting. The m/OS provides the foundation for limitless advertiser and publisher tools, including the option to build third-party solutions onto the platform. By design, m/OS facilitates success by making data accessible and actionable to maximize ROI.

https://www.kochava.com/kochava-announces-clue-as-newest-authorized-agency-partner/ last accessed August 30, 2022.

41. Defendant's LinkedIn page touts that:

> Kochava delivers what marketers need, when they need it, to establish customer identity and segment and activate audiences in a privacy-first world, leveraging data from the Kochava Collective for audience enrichment.

https://www.linkedin.com/company/kochava/about/ last accessed August 30, 2022.

42. Defendant lists its business sector specialties as, "Mobile Advertising Solutions, Mobile Tracking, Analytics, Mobile Gamification, Attribution for Connected Devices, Monetization, Mobile App Tracking, and App Analytics." Id.

43. According to its CEO, Charles Manning, Defendant

> Kochava offers a unique, holistic and unbiased approach to **mobile attribution analytics** and optimization. Via its platform, Kochava provides mobile advertisers with precise real-time visualization of campaign data that spans from initial launch through conversion and lifetime value (LTV) reporting, including comprehensive post-install event tracking. Kochava's tools enable customers to turn their data into actionable information. With over 3,000 publisher and network integrations including Facebook, Twitter, Google, Snap, Pinterest and

> Pandora, Kochava is trusted globally by the largest brands in mobile gaming, commerce, news and media. For more information visit www.kochava.com.

https://www.linkedin.com/in/charlesfmanning/ last accessed August 30, 2022 (bold underline added).

44. One individual in the mobile analytics industry described the methodology and significance of mobile attribution analytics like those employed by Defendant:

> Attribution is how marketers understand the journey you take to arrive in their app and what you do once you've landed there. When done right, there's a data point for each of the actions a user takes on the journey, from clicking an ad to making a purchase.
>
> …
>
> **How does mobile attribution work?**
>
> So why is it important to run with an attribution provider and not just rely on something like Google Analytics? The most important reason is that implementing a mobile app tracking SDK enables you to make well-informed business decisions in real time. An attribution provider gives you a platform to discover where your users come from - if they arrived in your app via a video ad, for instance. We're then able to help you understand how that user moves through your app and how you can compare their journey to someone else who arrived via a different source.
>
> This lets you determine which are your best-performing campaigns, so you can pinpoint the most effective ads and iterate on them. With this information, you're able to optimize your creative assets and use hard data to get rid of failing ads and tweak the good ones. Greater knowledge about how your ads perform allows you to practice smart retargeting and build campaigns targeted. For example, you could specifically target users who tried out your app but didn't stick around.
>
> Your users will come from multiple advertising channels. If you cannot track the how, who, when and why of their journey to your app, you cannot know which of your networks are delivering users, the relative value of those users, or how much of your marketing budget is going directly towards fake clicks and fake installs.
>
> …
>
> **What happens when I click on an ad?**
>
> Let's say that you're using your iPhone to play a game. A video ad pops up within the game. You watch the video and click the call to action (CTA) to download the app at the end of it. The link takes you to the app in the iTunes store, but briefly redirects you through Adjust. This takes a fraction of a second but is a key step; it's how the attribution provider receives the first data point - the engagement with the ad.

> By clicking the link, going to the app store, downloading the app and opening it for the first time, the attribution provider will receive the following data points:
>
> Advertising ID - a string of numbers and letters that identifies every individual smartphone or tablet in the world
> IP address – a specific address that devices use to communicate with one another via the internet
> User agent – a line of text that identifies a user's browser and operating system
> Timestamp – When you clicked on the link
> First Install - Activates on first app open
> With this information, the attribution provider can determine whether the user is new or existing. If the user is new, the attribution provider will attempt to match the user's install to their engagement with a particular ad. This exchange of information can happen in several ways; the most common is for the app to integrate the attribution provider's SDK.
>
> An SDK (or software development kit) allows apps to communicate with [a mobile analytics company's] servers. App developers integrate the SDK into their app's code, much like if they had a car and a manufacturer gave them a new part for a bit of an upgrade. This creates a line of communication between the app and us through which we can provide attribution data in real time.

https://www.adjust.com/blog/mobile-ad-attribution-introduction-for-beginners/ last accessed August 30, 2022.

45. In addition, Defendant openly acknowledges that its software development kit (SDK), made available to and inserted by other companies as a plug-in to their own smartphone applications, intercepts and reads massive amounts of consumer data using its technology in order to identify unique consumers and report on their travel and habits for marketing, verification, and other purposes:

> **SDK Data Privacy and Safety**
> Various data is transmitted from the SDK to Kochava. This document describes SDK behavior and which datapoints are transmitted.
> …
>
> **When is data transmitted?**
> Data is transmitted only during app runtime milestones such as the first app launch, user session envelopes, and when performing host requested activities such as measuring an event. Data is not transmitted otherwise and can only be transmitted while the app is running. When not in use, the SDK remains idle, awaiting instruction from the host, and does not continuously transmit data to Kochava.

Is data encrypted?
Data is always encrypted during transmission via HTTPS.

Can data transmission be disabled?
Datapoint transmission may be disabled on an app-wide basis, rather than per-user basis. Many attribution-related datapoint transmissions may be disabled through your Edit App page in the dashboard, while others may be disabled upon request through your client success manager.

Can data be deleted upon request?
User data may be deleted from Kochava, so long as the request comes directly from the user.

Is the IP address transmitted?
The IP address of the device is an integral part of any network communication and is not explicitly set or controlled by the SDK; thus it is always transmitted when the device communicates with Kochava or any other entity. The IP address is used to derive a general location for purposes of analytics and reporting, but may also play a role in attribution depending on your attribution settings.

What data is transmitted?
Datapoints transmitted by the SDK are listed below. Keep in mind that some datapoints vary by SDK or platform, and datapoints are only transmitted if readily available for the given platform, and only if any required modules are present.

Android Specific Datapoints
These transmitted datapoints are specific to the Android SDK and are primarily used for attribution and install deduplication. Additionally, many of these datapoints are transmitted only if required modules are present.

Datapoint	***Description***
Google Advertising ID	Google Play Store advertising identifier.
Amazon Fire Advertising ID	Amazon advertising identifier.
Android ID	Android identifier.
Huawei Advertising ID	Huawei advertising identifier.

iOS Specific Datapoints
These transmitted datapoints are specific to the iOS/tvOS SDK and are primarily used for attribution and install deduplication.

Datapoint	***Description***
IDFA	Apple's identifier for advertisers. The IDFA is automatically redacted as of iOS 14.5 if ATT authorization has not been granted.
IDFV	Apple's identifier for vendors.
Apple Search Ads Results	Apple Search Ads attribution results.

Install Receipt	The install receipt, which is used for validation.

Other Identifiers
These transmitted datapoints are common across most SDK platforms and are primarily used for attribution and install deduplication.

Datapoint	***Description***
Facebook Attribution ID	Facebook's internal attribution identifier.
Kochava Device ID	Kochava's internal identifier, which is scoped to the current install, rather than the device.
User Agent	The user agent of the device.

App State Datapoints
These transmitted datapoints are common across most SDK platforms and describe the state of the app. They are used primarily for your analytics and reporting and do not play a role in attribution.

Datapoint	***Description***
App Name	The name of the app.
App Package/Bundle	The Bundle ID or package name of the app.
App Version	App version string(s).
Notifications Enabled	Whether notifications are enabled for the app.
Installer Package	The provider of the app installation (Android only).
Date of Install from Store	The date the app was installed (Android only).

Device State Datapoints
These transmitted datapoints are common across most SDK platforms and describe the state of the device. They are used for your analytics, reporting and fraud detection; they do not play a role in attribution.

Datapoint	***Description***
Architecture	The device architecture.
Battery Level	The current battery level.
Boot Time	When the device was last booted.
Battery Status	The status of the battery.
Cellular Carrier Name	The cellular carrier name.
Cellular Type	The cellular carrier type.
Device Type	The device model.
Display Width	The display width in pixels.
Display Height	The display height in pixels.
Locale Setting	The chosen locale setting.
Language Setting	The chosen language setting.
Network Is Metered	Whether the network is metered.
Network SSID	The SSID.
Network BSSID	The BSSID.

Orientation	The device orientation.
OS Version	The version of the device OS.
Platform	The platform of the device.
Screen DPI	The screen DPI.
Screen Inches	The screen size.
Screen Brightness	The current screen brightness.
Signal Bars	The current cellular signal bars.
Timezone	The chosen timezone setting.

https://support.kochava.com/reference-information/sdk-data-privacy-and-safety/ last accessed August 30, 2022.

46. By actively intercepting this digital information without the consent of knowledge of consumers like Plaintiff, Defendant is able to deliver targeted advertising to those consumers while tracking their locations, spending habits, and personal characteristics, while sharing this rich personal data simultaneously with untold numbers of third-party companies by in essence "fingerprinting" each unique device and user, as well as connecting users across devices and devices across users.

47. Defendant, without consent, surreptitiously intercepts and collects Plaintiff's and Class Members' activity while using smartphone applications that have installed its SDK.

48. This data collection includes all sorts of website information, as well as Plaintiffs' and Class Members' respective IP addresses, browser and device information, user IDs, geolocation data, and other data, are used by Defendant to "fingerprint" individuals across the internet for Defendant's benefit, deriving revenue from the targeted marketing and sale of this information to third parties.

49. Defendant has a huge and diverse client base of paid recipients of this consumer reporting data that includes, amongst others:

- 7-Eleven
- Airbnb
- Audible.com
- Capcom
- CBS
- Chevron
- Chick-Fil-A
- Choice Hotels
- Discovery Channel

- Disney+
- Dunkin Doughnuts
- Groupon
- GSN Channel
- Hilton Hotels
- Intuit
- John Hancock
- Kroger
- Little Caesars
- McDonalds
- NBC
- WesternUnion
- Priceline
- Roku
- SiriusXM
- Sling
- Sonic
- Univision
- UFC
- Venmo
- Zappos

https://www.kochava.com/kochava-difference/?int-link=menu-competitive-differences last accessed August 29, 2022.

50. Upon good faith information and belief, Defendant and others installed software Defendant's SDK onto Plaintiff's cellular telephone which gathers geo-location data from Plaintiff's whereabouts, as well as his the previously described datapoints on his smartphone, but without Plaintiff's express consent or knowledge and then created consumer reports based upon this information.

51. Defendant uses its software to combine this information with other data points Defendant has obtained about Plaintiff to create a composite of Plaintiff's physical locations and consumer behavior.

//

//

//

Defendant's Data Can Be Used to Identify People and Track Them to Sensitive Locations

52. The FTC Complaint also details how precise geolocation data associated with MAIDs, such as the data sold by Defendant, may be used to track consumers to

sensitive locations, including places of religion, domestic abuse shelters, places inferring LGBTQ+ identification, medical facilities, welfare and homeless shelters, and reproductive health clinics.

53. Since each set of coordinates is time-stamped, it is also possible to identify when a mobile device visited a certain location.

54. Defendant does not anonymize the location data it provides, meaning it is possible to use the geolocation data combined with the mobile device's MAID to identify the user or owner of the device.

55. The location data sold by Defendant typically includes multiple timestamped signals for each MAID. By plotting each of these signals of a map, much can be inferred about the mobile device owners. For example, the location of the mobile device at night likely corresponds to the user's home address. This, coupled with other public records, can easily identify the name of the owner or resident of a particular address.

56. Defendant has even recognized that its data may be used to track mobile devices to home address. In its marketing on the AWS Marketplace, it has suggested "Household Mapping" as a potential use case of the data.

57. Defendant employs no technical controls to prohibit its customers from identifying consumers or tracking them to sensitive locations.

Defendant Practices Cause and Are Likely to Cause Substantial Injury to Consumers

58. As described above, the data collected, stored, and sold by Defendant may be used to identify individual consumers and their visits to sensitive locations. The collection and sale of such data poses an unwarranted and unauthorized intrusion into the most private areas of a consumer's life and caused or is likely to cause substantial injury to the consumers.

59. The dangers associated with Defendant's practices are numerous. For example, the data set makes it possible to identify a mobile device which visited a

reproductive health clinic or can demonstrate a person's routine by showing location data from a particular address, numerous times, in a single week.

60. Defendant collects and stores and disseminates this data all without the user's knowledge or consent.

61. Allowing a person access to such information, even for a seven-day period, can cause substantial injury to the user.

62. Identification of sensitive and private characteristics of consumers from the location data sold and offered by Defendant injures or is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms.

63. Such injuries are exacerbated by the fact that Defendant lacks any meaningful control over who accesses its location data feed.

64. The collection and use of their location data by Defendant are completely unknown and/or opaque to consumers, who typically do not know who has collected their location data and how it is being used—let alone to consent to the interception and use of that data.

65. Once the information has been collected and stored, the information can be sold multiple times to companies those consumers have never heard of and never interacted with. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

66. By Defendant's own admissions the data collected violates California's broad remedial statutory scheme supporting consumer privacy rights, as codified under Cal. Pen. Code § 630, et seq.

"Kochava operates two business units, which offer digital marketing and analytics services. It's [sic] primary business unit provides mobile advertising attribution through a set of customizable software tools ("Software as a Service" aka "SAAS") that allow Kochava's customers to obtain various data points and analytics for the customers' digital marketing campaigns and applications.

Specifically, Kochava develops a set of software tools and programs that device application ("app") developers can use to measure, track, organize, and visualize mobile app data for their marketing campaigns across marketing channels and partners. Kochava's secondary business unit, the Kochava Collective ("Collective"), is an aggregator of third-party provided mobile device data, which Kochava makes available through its proprietary data marketplace. *See Kochava, Inc. v. Federal Trade Commission*; 2:22-cv-00349-BLW (Dist. Idaho), ¶ 7.

67. Defendant itself admits that it tracks sensitive consumer geo location data, in violation of California law:

"The FTC's allegations regarding Kochava's alleged business practices illustrate a lack of understanding of Kochava's services. As part of its Collective services, Kochava does not uniquely identify users, but collects Mobile Advertising Identifier (MAID) information and links it to hashed emails and primary IP addresses in relation to Kochava's Data Marketplace. Although the Kochava Collective collects latitude and longitude, IP address and MAID associated with a consumer's device, Kochava does not receive these data elements until days after (unlike a GPS tool, for instance), Kochava does not identify the location associated with latitude and longitude, nor does Kochava identify the consumer associated with the MAID. As such, Kochava does not collect, then subsequently sell data compilation that allows one to track a specific individual to a specific location. Even if an injury to the consumer did indeed occur, it is reasonably avoidable by the consumer themselves by way the opt-out provision to allow the data collection. In other words, the consumer agreed to share its location data with an app developer. As such, the consumer should reasonably expect that this data will contain the consumer's locations, even locations which the consumer deems is sensitive. Prior to the data collection, a disclaimer or a warning was also provided to a consumer regarding collection of data from all." *Id*. at ¶ 19 locations, including sensitive ones.

68. In fact, Defendant recognizes the damage it has done to California consumers and in response to an imminent FTC action, it proactively introduced a new feature that allegedly now blocks the gathering of private, sensitive, location data related to health care facilities:

"On August 10, 2022, Kochava, announced a capability for its Kochava Collective marketplace. The Kochava Collective is an independent data marketplace for connected mobile devices. The new capability is a "Privacy Block" which removes health services location data from the Kochava Collective marketplace. Privacy Block aggregates health services locations which have been identified by a broad range of industry partners into a unified, super- set definition of health services locations. Privacy Block bolsters consumer privacy by leveraging multiple vendor location definitions for what each vendor determines is a health services location, and blocks the onward transfer of this data. Kochava invited data brokers and adtech industry vendors to register to participate with Privacy Block and contribute to the database. In addition, those in the health services sector were invited to register to block their location directly in Privacy Block. Even if consumers previously consented to share their location data, Privacy Block blocks the sharing of health services locations." *Id.* at ¶¶ 26-27

Defendant's Unlawful Recording of Confidential Communications

69. California Penal Code § 632(a) prohibits recording of such confidential communications, including digital communications like those between Plaintiff and Defendant, without the consent of the other person states:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio [violates this section].

70. California Penal Code § 632.7(a) is clear in its prohibition against such unauthorized recording of any communications without the consent of all parties to the communication:

> "Every person who, without the consent of all parties to a communication, intercepts or receives and intentionally records, or assists in the interception or reception and intentional recordation of, a communication transmitted between two cellular radio telephones, a cellular radio telephone and a landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone [violates this section]."

71. California Penal Code § 637.2 permits Plaintiff to bring this action for any violation of California Penal Code § 632.7(a) and provides for statutory damages of $5,000 for each violation.

72. Defendant recorded or otherwise made an unauthorized connection to Plaintiff's confidential communications in violation of California's statutory and common law against such unlawful intrusions into a person's private affairs, including the California Constitution's prohibition in Article 1, Section 1.

73. This suit seeks only damages and injunctive relief for recovery of economic injury and it expressly is not intended to request any recovery for personal injury and claims related thereto.

74. Plaintiff is informed and believes, and thereon alleges, that Defendant intentionally recorded a confidential communication as prohibited by California Penal Code § 632.

75. Plaintiff is informed and believes, and thereon alleges, that Defendant intentionally recorded a communication transmitted between a cellular radio telephone and a landline telephone without Plaintiff's consent as prohibited by California Penal Code § 632.7(a).

76. Defendant violated Plaintiff's constitutionally protected privacy rights by failing to advise or otherwise provide notice at the beginning of the recorded

communication with Plaintiff that the communication would be recorded, and Defendant did not try to obtain the Plaintiff's consent before such recording.

77. The recording or other unauthorized connection was done without Plaintiff's prior knowledge or consent. Plaintiff was damaged thereby, as detailed herein, in at least an amount permitted by the statutory damages mandated by California Penal Code § 637.2(a).

78. Defendant, its employees or agents, secretly recorded a cellular communication made involving Plaintiff and others. At no time before, during, or after any of the communications was Plaintiff warned, told, advised or otherwise given any indication by Defendant, its employees or agents, that the content of his communications were recorded.

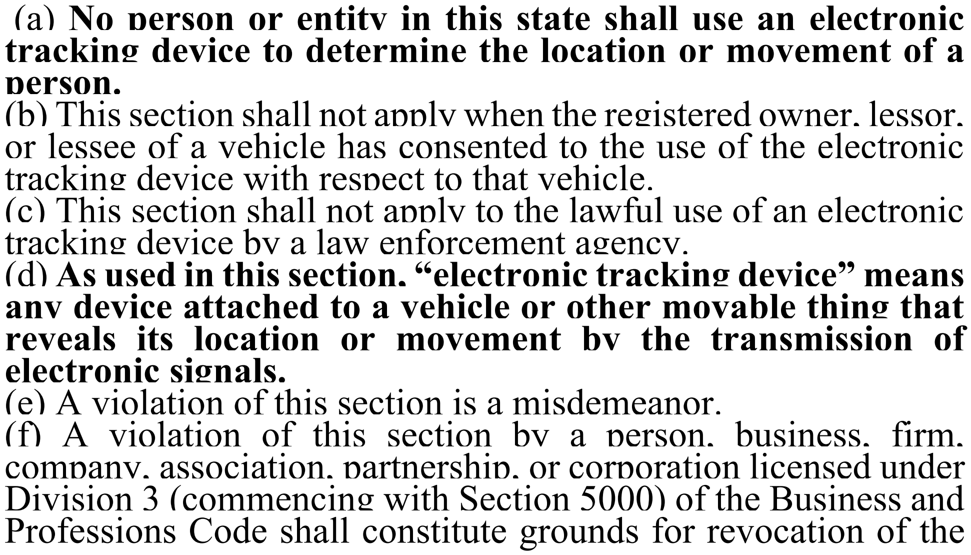
79. As a result thereof, Plaintiff has been damaged as set forth in the Prayer for Relief herein.

80. Plaintiff seeks statutory damages and injunctive relief under California Penal Code § 637.2.

Defendant's Unlawful Use of an Electronic Tracking Device

81. California Penal Code § 637.7 prohibits the use of surreptitious electronic tracking devices:

> **§ 637.7. Electronic tracking device**



> (a) **No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.**
> (b) This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle.
> (c) This section shall not apply to the lawful use of an electronic tracking device by a law enforcement agency.
> (d) **As used in this section, "electronic tracking device" means any device attached to a vehicle or other movable thing that reveals its location or movement by the transmission of electronic signals.**
> (e) A violation of this section is a misdemeanor.
> (f) A violation of this section by a person, business, firm, company, association, partnership, or corporation licensed under Division 3 (commencing with Section 5000) of the Business and Professions Code shall constitute grounds for revocation of the

> license issued to that person, business, firm, company, association, partnership, or corporation, pursuant to the provisions that provide for the revocation of the license as set forth in Division 3 (commencing with Section 5000) of the Business and Professions Code.

82. This suit seeks only damages and injunctive relief for recovery of economic injury and it expressly is not intended to request any recovery for personal injury and claims related thereto.

83. Plaintiff is informed and believes, and thereon alleges, that Defendant intentionally used an electronic tracking device as prohibited by California Penal Code § 637.7.

84. Plaintiff is informed and believes, and thereon alleges, that Defendant intentionally tracked Plaintiff's geolocation on his movable device without Plaintiff's consent as prohibited by California Penal Code § 637.7.

85. Defendant violated Plaintiff's constitutionally protected privacy rights by failing to advise or otherwise provide notice at the beginning of the recorded tracking of geolocation data with Plaintiff that the sensitive and private geolocation data would be recorded, and Defendant did not try to obtain the Plaintiff's consent before such use of an electronic tracking device and the recording of its results.

86. The use of the electronic tracking device by Defendant as described further herein was unauthorized and done without Plaintiff's prior knowledge or consent. Plaintiff was damaged thereby, as detailed herein, in at least an amount permitted by the statutory damages mandated by California Penal Code § 637.2.

87. Defendant, its employees or agents, secretly recorded a cellular communication made involving Plaintiff and others. At no time before, during, or after any of the communications was Plaintiff warned, told, advised or otherwise given any indication by Defendant, its employees or agents, that the content of his communications were recorded.

88. As a result thereof, Plaintiff has been damaged as set forth in the Prayer for Relief herein.

89. Plaintiff seeks statutory damages and injunctive relief under California Penal Code § 637.2.

Defendant's Unlawful Disclosure of Telephonic Messages

90. California Penal Code § 637 prohibits the disclosure of telephonic messages (emphasis added):

> **§ 637. Disclosure of telegraphic or telephonic message; punishment; exception**
>
> Every person not a party to a telegraphic or telephonic communication who **willfully discloses the contents of a telegraphic or telephonic message, or any part thereof, addressed to another person,** without the permission of that person, unless directed so to do by the lawful order of a court, is punishable by imprisonment pursuant to subdivision (h) of Section 1170, or in a county jail not exceeding one year, or by fine not exceeding five thousand dollars ($5,000), or by both that fine and imprisonment.

91. This suit seeks only damages and injunctive relief for recovery of economic injury and it expressly is not intended to request any recovery for personal injury and claims related thereto.

92. Plaintiff is informed and believes, and thereon alleges, that Defendant intentionally disclosed Plaintiff's and the other Class Members telephonic messages, and or parts thereof, while using its software devices on cellular telephones, as prohibited by California Penal Code § 637, and as described furthet herein.

93. Defendant violated Plaintiff's constitutionally protected privacy rights by failing to advise or otherwise provide notice at the beginning of the disclosing such telephonic messages by Plaintiff that the sensitive and private messages would be disclosed, and Defendant did not try to obtain the Plaintiff's consent before such disclosures.

94. These disclosures of Plaintiff and Class Member's telephonic messages by Defendant as described further herein was unauthorized and done without their prior knowledge or consent. Plaintiff and the other Class Members were

damaged thereby, as detailed herein, in at least an amount permitted by the statutory damages mandated by California Penal Code § 637.2.

95. As a result thereof, Plaintiff has been damaged as set forth in the Prayer for Relief herein.

96. Plaintiff seeks statutory damages and injunctive relief under California Penal Code § 637.2.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this lawsuit as a class action on behalf of himself and Class Members of the proposed Classes. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

98. Plaintiff proposes the following four Classes consisting of and defined as follows:

A. The Confidential Communication Class for Violation of Penal Code §631, consisting of;

All persons in California whose communications were intercepted and recorded without their consent by Defendant, and or its agents.

B. The Confidential Communication Class for Violation of Penal Code § 632, consisting of;

All persons in California whose conversations were recorded without their consent, by Defendant, and or its agents, within the one year prior to the filing of the Complaint.

//

//

//

C. **The Cellular Phone Communication Sub-Class for Violation of Penal Code §632.7, consisting of;**

> All persons in California whose cellular telephone conversations were intercepted and recorded without their consent, by Defendant, and or its agents, within the one year prior to the filing of the Complaint.

99. Excluded from the Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and its legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiff reserves the right to redefine the Class and to add subclasses as appropriate based on discovery and specific theories of liability

100. **Numerosity**: The Class Members are so numerous that joinder of all members would be unfeasible and impractical. The membership of the entire Class is currently unknown to Plaintiff at this time; however, given that, on information and belief, Defendant accessed millions of unique mobile devices, it is reasonable to presume that the members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court.

101. **Commonality**: There are common questions of law and fact as to Class Members that predominate over questions affecting only individual members, including, but not limited to:

- Whether, within the statutory period, Defendant intercepted any confidential communications with Class Members;
- Whether, the intercepted communications concerned confidential communications Class Members;

//

- Whether, within the statutory period, Defendant transmitted any confidential communications of Class Members to a third party;

- Whether Defendant had, and continues to have, a policy during the relevant period of intercepting digital communications of Class Members;
- Whether Defendant's policy or practice of intercepting Class Members digital communications constitutes a violation of Cal. Penal Code § 631;
- Whether Defendant's policy or practice of recording telephone communications with Class Members constitutes a violation of Cal. Penal Code § 632
- Whether Defendant's policy or practice of recording telephone communications with Class Members constitutes a violation of Cal. Penal Code § 632.7;
- Whether Defendant's policy or practice of utilizing electronic tracking devices with respect to Class Members digital communications constitutes a violation of Cal. Penal Code § 637.7;

102. **<u>Typicality</u>**: Plaintiff's wire and cellular telephone communications were intercepted, unlawfully tapped and recorded without consent or a warning of such interception and recording, and thus, his injuries are also typical to Class Members.

103. Plaintiff and Class Members were harmed by the acts of Defendant in at least the following ways: Defendant, either directly or through its agents, illegally intercepted, tapped, recorded, and stored Plaintiff and Class Members' digital communications, geolocations, and other sensitive personal data from their digital devices with others, and Defendant invading the privacy of said Plaintiff and Class. Plaintiff and Class Members were damaged thereby.

104. Further, the communications at issue were concerning matters which constitutes a "confidential" communication pursuant to California Penal Code §632.

105. **Adequacy**: Plaintiff is qualified to, and will, fairly and adequately protect the interests of each Class Member with whom he is similarly situated, as demonstrated herein. Plaintiff acknowledges that he has an obligation to make known to the Court any relationships, conflicts, or differences with any Class Member. Plaintiff's attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. In addition, Plaintiff's attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. The proposed class counsel is experienced in handling claims involving consumer actions and violations of the California Penal Code §§ 632 and 632.7. Plaintiff has incurred, and throughout the duration of this action, will continue to incur costs and attorneys' fees that have been, are, and will be, necessarily expended for the prosecution of this action for the substantial benefit of each Class Member.

106. **Predominance**: Questions of law or fact common to the Class Members predominate over any questions affecting only individual members of the Class. The elements of the legal claims brought by Plaintiff and Class Members are capable of proof at trial through evidence that is common to the Class rather than individual to its members.

107. **Superiority**: A class action is a superior method for the fair and efficient adjudication of this controversy because:

a. Class-wide damages are essential to induce Defendant to comply with California and Federal law.

b. Because of the relatively small size of the individual Class Members' claims, it is likely that only a few Class Members could afford to seek legal redress for Defendant's misconduct.

c. Management of these claims is likely to present significantly fewer difficulties than those presented in many class claims.

d. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law.

e. Class action treatment is manageable because it will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would endanger.

f. Absent a class action, Class Members will continue to incur damages, and Defendant's misconduct will continue without remedy.

108. Plaintiff and the Class Members have all suffered and will continue to suffer harm and damages as a result of Defendant's unlawful and wrongful conduct. A class action is also superior to other available methods because as individual Class Members have no way of discovering that Defendant intercepted and recorded the Class Member's telephonic digital communications without Class Members' knowledge or consent.

109. The Class may also be certified because:

- the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudication with respect to

  individual Class Members, which would establish incompatible standards of conduct for Defendant;
- the prosecution of separate actions by individual Class Members would create a risk of adjudications with respect to them that 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; and

- Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final and injunctive relief with respect to the members of the Class as a whole.

110. This suit seeks only damages and injunctive relief for recovery of economic injury on behalf of Class Members and it expressly is not intended to request any recovery for personal injury and claims related thereto.

111. The joinder of Class Members is impractical and the disposition of their claims in the Class action will provide substantial benefits both to the parties and to the court. The Class Members can be identified through Defendant's records.

First Cause of Action

Unlawful Wiretapping and Interception of Electronic Communication

California Penal Code § 631

112. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs.

113. At all relevant times to this complaint, Defendant intercepted and recorded components of Plaintiff's and the putative class' private telephone communications and transmissions when Plaintiff and other Class Members accessed Defendant's software via their cellular mobile access devices within the State of California.

114. At all relevant times to this complaint, Plaintiff and the other Class Members did not know Defendant was engaging in such interception and recording and therefore could not provide consent to have any part of their private and confidential videoconferencing communications intercepted and recorded by Defendant and thereafter transmitted to others.

115. Plaintiff was completely unaware that Defendant had intercepted and stored his geolocation and other personal data and communications on his mobile device until well after the fact and was therefore unable to consent.

116. At the inception of Defendant's illegally intercepted and stored his geolocation and other personal data, Defendant never advised Plaintiff or the other Class Members that any part of this sensitive personal data would be intercepted, recorded and transmitted to third parties.

117. Plaintiff was completely unaware that components of his private use of his mobile device were in part being recorded and stored and thereafter transmitted to third parties.

118. To establish liability under section 631(a), a plaintiff need only establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner," does any of the following:

> Intentionally taps, or makes 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***
>
> Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or 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***
>
> Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> ***Or***
>
> 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.

119. 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 Litigation, --- F.3d --- 2020 WL 1807978 (9th Cir. Apr. 9, 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

120. Defendant's 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.

121. At all relevant times, by using Defendant's MAID software and SDK as well as tracking Plaintiff's and Class Member's geolocation, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiff and class members on the one hand, and the specific sites and locations Plaintiffs and Class Members visited on the other.

122. At all relevant times, by using Defendant's geolocation tracking software technology, Defendant 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 Plaintiff and putative class 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.

123. Plaintiff and Class Members did not consent to any of Defendant's actions in implementing these wiretaps within its geolocation tracking software. Nor have Plaintiff or Class Members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Plaintiff and Class Members' electronic communications.

124. Plaintiff's and the Class Members devices of which Defendant accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

125. Defendant violated Cal. Penal Code § 631 by knowingly accessing and without permission accessing Plaintiffs' and Class members' devices in order to obtain

their personal information, including their device and location data and personal communications with others, and in order for Defendant to share that data with third parties, in violation of Plaintiff's and Class Members' reasonable expectations of privacy in their devices and data.

126. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information and personal communications with others.

127. The violation of section 631(a) constitutes an invasion of privacy sufficient to confer Article III standing in that Plaintiff and each class member has suffered a concrete harm by having their privacy invaded by Defendant.

128. Plaintiff and Class Members seek all relief available under Cal. Penal Code § 631, including $2,500 per violation.

Second Cause of Action

Recording of Confidential Calls

Under California Penal Code § 632

129. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs.

130. At all relevant times hereto, Defendant had and followed a policy and practice of using a telecommunications system that enabled it to surreptitiously record confidential communications between Plaintiff and Class Members, and third parties.

131. Because of the nature of its business, the geolocation and other private and sensitive data and communications that Defendant surreptitiously recorded of Plaintiff and the Class Members were, by definition, "confidential" communications as a matter of law.

132. At all relevant times Plaintiff and all Class Members have an expectation of privacy in their communication that were intercepted and recorded by Defendant,

and did not expect, or have knowledge of, any such illegal recording or other unauthorized connections to their communications.

133. At all relevant times hereto, Defendant had and followed a policy and practice of not advising or warning Plaintiff and Class Members at the beginning of a communication that their confidential communications with third parties would be recorded.

134. Defendant failed to obtain consent of Plaintiff and Class Members prior to recording any of their confidential communications.

135. Because Defendant and its employees and agents recorded or otherwise made unauthorized connections to Plaintiff's and other Class Members' confidential communications, Defendant is liable for the greater of $5,000 per violation or three times the amount of actual damages sustained by each Plaintiff and Class Member.

136. Plaintiff is seeking only the statutory damages for the members of the Class under this cause of action.

137. Such conduct by this Defendant was willful, deliberate, malicious and intentional, and in violation of California Penal Code §§ 632 and 637.2. Such conduct violated the California Privacy Act, set forth in California Penal Code §§ 630, et seq.

138. As a result of such unlawful conduct, Plaintiff and the Class Members were damaged, in an amount according to proof.

//

//

//

THIRD CAUSE OF ACTION
RECORDING OF CELLULAR CALLS
UNDER CALIFORNIA PENAL CODE § 632.7

139. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs.

140. At all relevant times hereto, Defendant had and followed a policy and practice of using software systems that enabled it to surreptitiously record cellular telephone communications between Plaintiff and Class Members, and other third parties.

141. At all relevant times hereto, Defendant intentionally and secretly recorded cellular communications concerning confidential matters between Defendant and Plaintiff and Class Members.

142. At all relevant times hereto, Defendant had and followed a policy and practice of not advising or warning Plaintiff and Class Members at the beginning of a communication that their cellular communications with third parties would be recorded.

143. Defendant failed to obtain consent of Plaintiff and Class Members prior to recording any of their cellular communications.

144. This conduct by Defendant violated section 632.7(a) of the California Penal Code.

145. Plaintiff and Class Members are entitled to recovery of statutory punitive damages in the amount of $5,000 per violation of Cal. Pen. Code § 632.7.

146. Plaintiff's counsel is also entitled to attorneys' fees and costs pursuant to Cal. Code of Civ. Proc. § 1021.5.

//

//

//

//

//

//

Fourth Cause of Action
Unlawful Use of Electronic Tracking Device
Under California Penal Code § 637.7

147. Plaintiff repeats, re-alleges, and incorporates by reference, all other paragraphs.

148. At all relevant times hereto, Defendant had and followed a policy and practice of using software systems that enabled it to surreptitiously intercept and record Plaintiff's geolocation data.

149. At all relevant times hereto, Plaintiff and the Class Member's geolocation data was inherently private in nature and they did not consent to sharing that private information with Defendant.

150. At all relevant times hereto, Defendant had and followed a policy and practice of not advising or warning Plaintiff and Class Members that their geolocation information would be intercepted and recorded to be later provided to third parties.

151. Defendant failed to obtain consent of Plaintiff and Class Members prior to intercepting and recording any of their geolocation data.

152. This conduct by Defendant violated section 637.7 of the California Penal Code.

153. Plaintiff and Class Members are entitled to recovery of statutory punitive damages in the amount of $5,000 per violation of Cal. Pen. Code § 637.2.

154. Plaintiff's counsel is also entitled to attorneys' fees and costs pursuant to Cal. Code of Civ. Proc. § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class Members pray that judgment be entered against Defendant, and Plaintiff and the Class be awarded damages from Defendant, as follows:

- Certify the Class as requested herein;
- Appoint Plaintiff to serve as the Class Representative for the Class; and
- Appoint Plaintiff's Counsel as Class Counsel in this matter for the Class.

In addition, Plaintiff and the Class Members pray for further judgment as follows against Defendant:

UNLAWFUL WIRETAPPING AND INTERCEPTION OF ELECTRONIC COMMUNICATIONS UNDER CALIFORNIA PENAL CODE § 631

- $2,500 to each Class Member pursuant to California Penal Code § 631(a) for each such unlawful interception of communications;
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further occurrence of such illegal acts pursuant to California Penal Code § 631;
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

RECORDING OF CONFIDENTIAL COMMUNICATIONS UNDER CALIFORNIA PENAL CODE § 632

- $5,000 to each Class Member pursuant to California Penal Code § 637.2(a) for each such unlawful recording;
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further occurrence of such illegal acts pursuant to California Penal Code § 637.2(b);
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

RECORDING OF CELLULAR COMMUNICATIONS UNDER CALIFORNIA PENAL CODE § 632.7

- $5,000 to each Class Member pursuant to California Penal Code § 637.2(a) for each such unlawful recording;
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further occurrence of such illegal acts pursuant to California Penal Code § 637.2(b);

//

- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

UNLAWFUL USE OF ELECTRONIC TRACKING DEVICE UNDER CALIFORNIA PENAL CODE § 637.7

- $5,000 to each Class Member pursuant to California Penal Code § 637.2(a) for each such unlawful tracking;
- Reasonable attorneys' fees pursuant to Cal. Code of Civ. Proc. § 1021.5;
- Injunctive relief to prevent the further occurrence of such illegal acts pursuant to California Penal Code § 637.2(b);
- An award of costs to Plaintiff; and
- Any other relief the Court may deem just and proper including interest.

TRIAL BY JURY

155. Pursuant to the Seventh Amendment to the Constitution of the United States of America, Plaintiff and Class Members are entitled to, and demand, a trial by jury.

Respectfully submitted

,

SWIGART LAW GROUP

Date: September 6, 2022

By: *s/ Joshua Swigart*
Joshua B. Swigart, Esq.
Josh@SwigartLawGroup.com
Attorneys for Plaintiff