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

[Additional Counsel on Signature Page]
Attorneys for Plaintiffs David Greenley, Shahnaz, and Sheri Bate and The Putative Class

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

DAVID GREENLEY, SHAHNAZ ZARIF, and SHERI BATE individually and on behalf of others similarly situated, Plaintiffs, vs. Kochava, Inc., Defendant.	CASE NO: 22-CV-01327 BAS-AHG SECOND AMENDED CLASS ACTION COMPLAINT 1. Invasion of Privacy; 2. violation of the California Computer Data Access and Fraud Act, California Penal Code § 502; 3. Violation of California Penal Code § 631; 4. Violation of California Penal Code § 632; JURY TRIAL DEMANDED

1. David Greenley, Shahnaz Zarif, and Sheri Bate ("Plaintiffs"), individually and on behalf of all other similarly situated California residents ("Class Members"), bring 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 Constitution, Article I, Section 1; the California Computer Data Access and Fraud Act ("CDAFA"), California

Penal Code § 502; the California Invasion of Privacy Act ("CIPA"), California Penal Code § 630, *et seq.*, including Sections 631, and 632, in relation to the unauthorized collection, recording, and dissemination of Plaintiffs' and Class members' personal information, geolocation data, and communication. Plaintiffs make these allegations on information and belief, with the exception of those allegations that pertain to Plaintiffs, or to Plaintiffs' counsel, which Plaintiffs allege on their personal knowledge.

NATURE OF THE CASE

2. The efforts of privacy-conscious individuals to avoid the improper collection and storage of personal information—particularly sensitive personal information—must be protected. As the Supreme Court recognized in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), location data is highly sensitive, not just because of what the data point alone says about an individual (*i.e.*, where they were at a particular time), but also because of the massive amount of personal information that can be extracted from location data (such as medical treatment, personal relationships, and private interests). As Chief Justice John Roberts stated, "a cell phone—almost a 'feature of human anatomy[]'—tracks nearly exactly the movements of its owner. . . . A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," and when a third-party has access to the information stored on one's cell phone, that entity "achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id*. at 2218 (internal citations omitted).

3. Kochava 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, and by intercepting location data consumers provide to mobile-phone applications that have incorporated Kochava's software developer kit (SDK).

4. App developers often use SDKs because the kits minimize development work and create a predictable stream of income that grows as more people use the app.

5. App developers embed SDKs into their app that, and may not know the full extent and functions of the code in the SDK. Some SDKs, unbeknownst to consumers, siphon consumers' location data directly to a data broker or advertising platform, and can even include the ability to track users' locations through public Bluetooth beacons, which enable fine-grained tracking indoors.

6. Data brokers, such as Kochava, provide SDK to app developers to assist them in developing their apps. But in exchange for doing so, they permit data brokers like Kochava to surreptitiously intercept location data they then use to profit at the expense of consumers.

7. Kochava does so by selling customized data feeds to its clients to, among other purposes, assist in advertising and analyzing foot traffic at stores or other locations. Among other categories, Kochava sells timestamped latitude and longitude coordinates showing the location of mobile devices.

8. Because the data is associated with particular device IDs, disaggregated data—such as location and other data that Kochava surreptitiously collects—, is later repackaged and sold to third parties by Kochava, without consumers' consent, and can be easily de-anonymized.

9. In 2013, researchers published in *Scientific Journal* a study concerning their analysis of 15 months of human mobility data like that collected and sold by Kochava. They concluded that even absent an "obvious identifier" like a name, addresses or a device ID, "if an individual's patterns are unique enough, outside information can be used to link the data back to an individual" and "that the uniqueness of human mobility traces is high and that mobility datasets are likely to be re-identifiable using information only on a few outside locations."

10. In other words, even data that lacks an identifier particular to a given individual can be de-anonymized with minimal effort. The device-specific location data Kochava collects and sells without consumers' consent thus poses ***even greater*** risks to

consumers themselves because it is not anonymized and can be combined with various unique mobile device identifiers, to identify the mobile device's user or owner.

11. As the FTC explains in a parallel enforcement action it recently initiated against Kochava, "precise geolocation data associated with MAIDs, such as the data sold by Kochava, may be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, and welfare and homeless shelters. For example, by plotting the latitude and longitude coordinates included in the Kochava data stream using publicly available map programs, it is possible to identify which consumers' mobile devices visited reproductive health clinics. Further, because each set of coordinates is time-stamped, it is also possible to identify when a mobile device visited the location. Similar methods may be used to trace consumers' visits to other sensitive locations."

12. The FTC's concerns regarding disaggregated location data are not mere hyperbole; they are concrete and particularized, as are the risks the surreptitious collection and sale of location data poses to consumers.

13. For example, in 2018, *The New York Times* was able to use purportedly "anonymous" location data to follow multiple people into abortion clinics, follow them inside and unmask them. The article's authors reviewed a database of data collected by one app data collector, and determined that the data revealed locations that individuals' visited to within a few yards.[1]

14. Likewise, *The Pillar*, a Catholic Substack publication, successfully outed a homosexual priest using location data purchased from a data broker like Kochava. Although the data was not associated with names or particular addresses, investigators

[1] Jennifer Valentino-DeVries et al, *Your Apps Know Where You Were Last Night, and They're Not Keeping it Secret*, New York Times (Dec. 10, 2018), available at: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?mtrref=www.vice.com&gwh=3919FC4278D0708838A67ACD4CF87224&gwt=pay&assetType=PAYWALL.

isolated location data from a dating app, Grindr, showing that the device frequently was found at the priest's residence. By cross-referencing that device ID with other locations known to be frequented by the priest, investigators were able to confirm the device ID was associated with the priest, and that his mobile device frequently visited gay bars and private residences associated with other Grindr users.[2]

15. Mobile device data, such as the kind that Kochava surreptitiously collects from consumers, can be used to identify specific individuals—even without information such as the person's name or address—and determine specific locations that the individual visited, all without informing or obtaining consent from the person tracked.

CALIFORNIA VIGOROUSLY PROTECTS INDIVIDUALS' PRIVACY

16. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

17. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

18. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. and Amends. to Cal.

[2] Joseph Cox, *The Inevitable Weaponization of App Data is Here*, Vice (July 21, 2021), available at: https://www.vice.com/en/article/pkbxp8/grindr-location-data-priest-weaponization-app.

Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn.*, (1994) 7 Cal.4th 1, 81, (Mosk, J., dissenting).

19. The California State Legislature passed CIPA in 1967 to protect the right of privacy of the people of California.

20. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." Cal. Penal Code § 630.

21. 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).

22. 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).

23. Defendant made an unauthorized connection with Plaintiffs’ and Class members’ mobile devices when Defendant collected and stored their personal information, geolocation data specific to each consumer’s mobile device, and communications, and then provided such information to its clients for the purposes of targeted advertising.

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

25. Plaintiffs bring this action for violations of Plaintiffs’ and Class members’ right to privacy, both under common law and under the California Constitution; CDAFA; and 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); Penal Code § 632, which provides for statutory damages of $5,000 for each violation under Penal Code § 637.2; violations of the UCL; and for unjust enrichment.

26. Plaintiffs bring this class action on behalf of a class, as more fully defined infra, consisting of the Confidential Communication class.

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

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

29. 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

30. Jurisdiction is proper under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because Plaintiffs, residents 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.

31. Plaintiffs are requesting damages, including statutory damages of $2,500 per violation of Cal. Penal Code §631, $5,000 per violation of §632 under §637.2, 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.

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

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

34. 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

35. Each 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. Plaintiff Zarif is a resident of the City of San Diego, County of San Diego, California. Plaintiff Bate is a resident of the City of Encinitas, County of San Diego, California.

36. Each Plaintiff owns, carries, and regularly uses a cellular device that contains Defendant's Kochava monitoring and intercepting SDK software.

37. Each Plaintiff owns a mobile cellular telephone phone that use application(s) containing the Defendant's software development kit (SDK).

38. Each Plaintiff regularly uses their cell phone to access these application(s) in which Defendant utilizes its embedded SDK to track his geolocation, and to monitor and intercept communications related to their personal characteristics, mode of living, purchase decisions, personal choices, app selections, spending habits, and click choices, amongst others.

39. Each Plaintiff values their privacy, as most people do. Even when each Plaintiff turned the location tracking off on their mobile device, Defendant's SDK nevertheless continued to track their movements, monitor their application selections, choices and uses, and combined that valuable private information with other data sets to sell to third-parties for advertising, sales, and marketing purposes against their wishes.

40. Each Plaintiff did not know until recently that their purchase decisions, their movements, and their locations, were being tracked by Defendant to market, sell, and advertise to them.

41. 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.

42. 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.

FACTUAL ALLEGATIONS

Defendant Sells Precise Location Information for Millions of Mobile Devices

43. 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").

44. 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.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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 Plaintiffs'
and Class Members' Location Data

50. 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").

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

52. 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.

53. 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.

54. 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."

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

56. 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.

57. 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.

58. 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

59. 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.

60. 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 November 18, 2022.

61. 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 November 18, 2022.

62. 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, last accessed November 18, 2022.

63. 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.*

64. 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 November 18, 2022 (bold underline added).

65. Defendant describes in detail its process of using multiple distinct identifiers in order to attribute consumer decisions to advertisement strategies using mobile analytics:

> **[Kochava's] Attribution Overview**
>
> **FEATURE SUMMARY:** What is attribution and why do you need it? Attribution is the act of assigning credit to the advertising source that most strongly influenced a conversion (e.g. app install). It is important to know where your users are discovering your app when making future marketing decisions.
>
> The Kochava attribution engine is comprehensive, authoritative and actionable. The system considers all possible factors and then separates the winning click from the influencers in real-time. The primary elements of engagement are impressions, clicks, installs and events. Each element has specific criteria which are then weighed to separate winning engagements from influencing engagements.

> **Engagements**
> Kochava collects (via momentary redirect or network server ping) device information when an impression is served or a user clicks on an advertisement served by a network. Each of these engagements are eligible for attribution. This collected device information ranges from unique device identifiers to the IP address of the device at the time of click or impression, dependent upon the capabilities of the network.
>
> Kochava has thousands of unique integrations. Through the integration process, we have established which device identifiers and parameters each network is capable of passing on impression and/or click. The more device identifiers that a network can pass, the more data is available to Kochava for reconciling clicks to installs. When no device identifiers are provided, Kochava’s robust fingerprinting logic is employed which relies upon IP address and device user agent. The integrity of a fingerprint match is lower than a device-based match, yet still results in over 90% accuracy.
>
> The Kochava system also determines whether a device has previously engaged with an advertisement. When multiple engagements of the same type occur, they are identified as duplicates to provide advertisers with more insight into the nature of their traffic.
>
> Kochava tracks every engagement with every ad served, which sets the stage for a comprehensive and authoritative reconciliation process.
>
> **Installs**
>
> Once the app is installed and launched, Kochava receives an install ping (either from the Kochava SDK within the app, or from the advertiser ’s server via Server-to-Server integration). The install ping includes device identifiers as well as IP address and the user agent of the device. The data received on install is then used to find all matching engagements based on the advertiser’s settings within the Postback Configuration and deduplicated. For more information on campaign testing and device deduplication, refer to our Testing a Campaign support document.
>
> **Events**
> The advertiser has complete control over the implementation of tracking events within the app. In the case of reconciliation, the advertiser has the ability to specify which post-install event(s) define the conversion point

> for a given campaign. The lookback window for event attribution within a reengagement campaign can be refined within the Tracker Override Settings. If no reengagement campaign exists, all events will be attributed to the source of the acquisition, whether attributed or unattributed (organic).

https://support.kochava.com/reference-information/attribution-overview, last accessed November 18, 2022.

66. 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 November 18, 2022.

67. 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 November 18, 2022 (bold underline added).

68. Defendant's novel approach to intercepting and recording this information, especially the IDFV, is now more important than ever to its business model since the advent of Apple's iPhone Application Tracking Transparency Tracking (ATT) framework.

69. ATT requires a consumer to affirmatively opt-in to allowing Defendant and others to track their device unique identification number for advertisers on their iPhones:

What is IDFV?

Identifier for Vendors (IDFV) | Definition

> IDFV stands for "identifier for vendors" and is a universally unique identifier (UUID) used by Apple on many of its devices, including iPhone, iPad, etc. The IDFV is 32 characters long with 4 dashes and can be used to distinguish individual devices engaging with an app.
>
> Unlike the identifier for advertisers (IDFA) which is unique to each app on a device, the IDFV is unique to the app developer account, and is identical across all apps published by that developer that are on the user's device. This enables the IDFV to be used for attribution on cross-promotional acquisition efforts within a developer's own portfolio of apps. Availability of the IDFV will not be affected by the AppTrackingTransparency (ATT) framework, which requires user opt-in to access the IDFA.

https://www.kochava.com/glossary/idfv/#:~:text=IDFV last accessed October 5, 2022.

70. On industry website described the importance to digital marketing campaigns of capturing IDFV:

> **Why is the Identifier for Vendor (IDFV) important?**
>
> IDFVs are important as they provide a means to run cross-promotional iOS campaigns which include 'limit ad tracking' (or LAT) users — without relying on fingerprinting. So long as an IDFV is passed in the tracker URLs, the IDFV can provide marketers with more accurate attribution data for iOS campaigns.

https://www.adjust.com/glossary/idfv/ last accessed November 18, 2022.

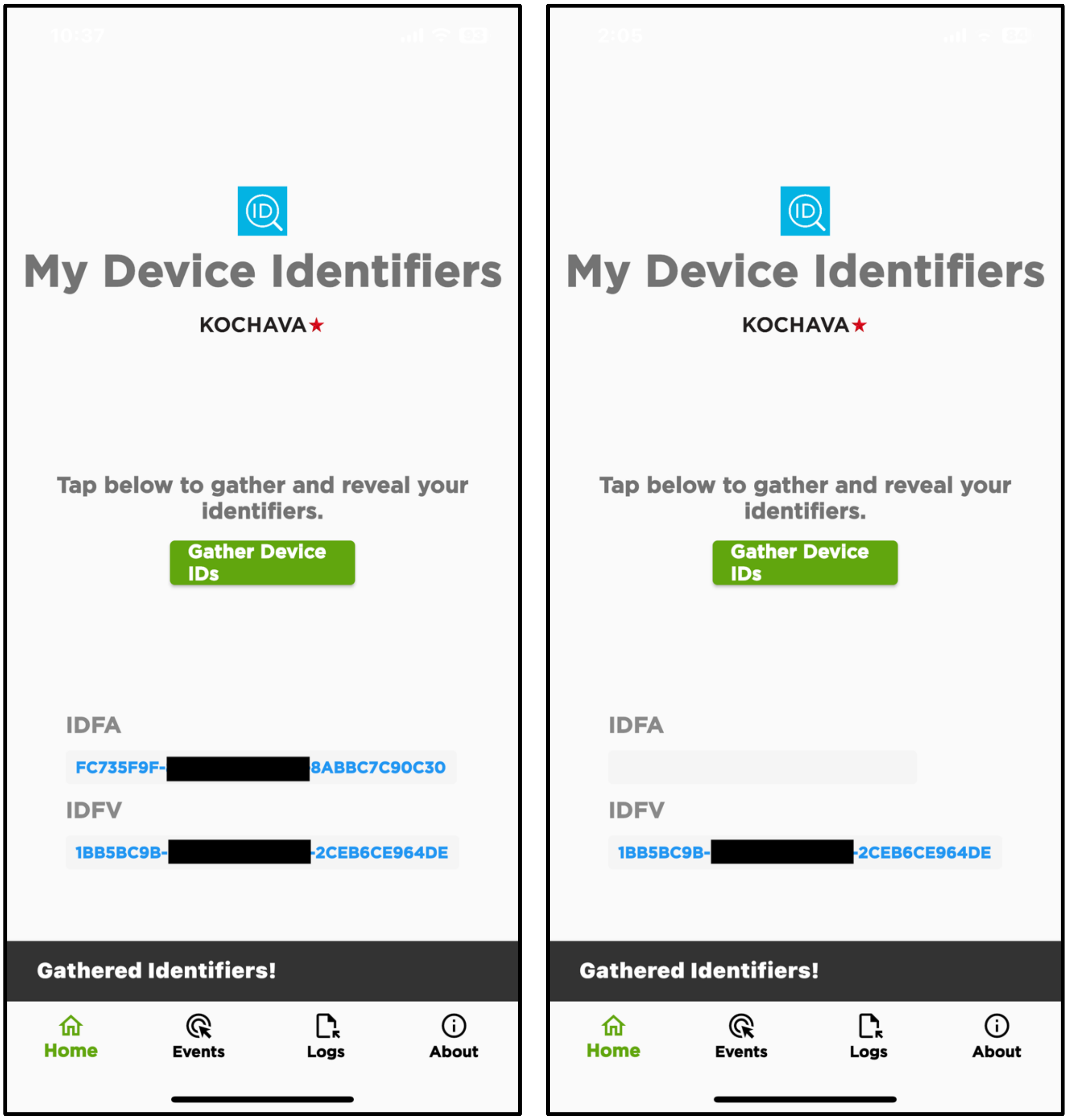
71. Despite Apple's efforts to provide greater privacy to its users, Defendant ignored these efforts and bypassed the intent of the ATT framework and instead redoubled its efforts to ensure that even users who had turned off app tracking on their phones would still be tracked without their knowledge and consent.

72. Defendant intercepts and tracks iPhone users, such as Plaintiffs, communicated choice with respect to Apple's no-tracking setting and the fact that they have told apps not to track them and thereafter communicates even that choice to its

clients in their reporting. https://support.kochava.com/analytics-reports-api/reports-overview/ last accessed November 18, 2022.

73. Defendant has actually published a testing app for its customer developers on Apple's Store that demonstrates how Kochava actively collects both IDFA and IDFV, even after a consumer thinks they have disabled all tracking by apps on an iPhone, as shown below:

Fig. 1 – Screenshots from Kochava ID Tracking App



Tracking Turned On

My Device Identifiers

KOCHAVA★

Tap below to gather and reveal your identifiers.

Gather Device IDs

IDFA

FC735F9F-[redacted]8ABBC7C90C30

IDFV

1BB5BC9B-[redacted]-2CEB6CE964DE

Gathered Identifiers!

Tracking Turned Off

My Device Identifiers

KOCHAVA★

Tap below to gather and reveal your identifiers.

Gather Device IDs

IDFA

IDFV

1BB5BC9B-[redacted]-2CEB6CE964DE

Gathered Identifiers!

74. In other words, even when consumers like the Plaintiffs tried to protect their privacy by disabling IDFA device tracking, Defendant eviscerated those efforts by doing an end-run around those consumer protections and gathered IDFV and other fingerprinting information which allowed to continue to track consumers without their knowledge or consent, thus further invading their privacy.

75. By actively intercepting this digital information, including IDFV, 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.

76. Defendant, without consent, surreptitiously intercepts and collects Plaintiffs' and Class Members' activity while using smartphone applications that have installed its SDK both as to Apple iPhone and Android mobile devices.

77. 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.

78. Defendant intercepts, tracks and passes along the search terms used by a device user which resulted in that user clicking on a particular advertisement as well as other user-specific communications with the application into which its SDK has been integrated on their Apple or Android device. https://support.kochava.com/analytics-reports-api/reports-overview, last accessed November 18, 2022.

79. Defendant also tracks, intercepts, receives and records specific communications from its SDK-installed apps such as customer's usernames, customer emails and customer IDs on their Apple or Android cellular telephone devices. *Id.*

80. Defendant tracks, intercepts, receives and records a user's activities within an app after it has been installed, including the length of time it observed a user's behavior within the app, the event that generated the highest revenue, a list of all interactions the user took within the app, the range of revenue generated, and the total number of user events recorded with the names of each event on their Apple or Android device. *Id.*

81. Defendant's SDK has the ability to be customized by its end-user developers to pass customized communication parameters back to Defendant based upon user inputs to their Apple or Android device. *Id.*

82. Defendant's SDK tracks, intercepts, receives, records and communicates the gender of a user, as well as their longitude, latitude, country, state, and city when they communicate with an app on their mobile Apple or Android device. *Id.*

83. 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.

84. Upon good faith information and belief, Defendant and others installed software Defendant's SDK onto Plaintiffs' cellular telephones which intercepts, receives and records geo-location data from Plaintiffs' whereabouts, as well as their previously described datapoints on their cellular smartphones, but without Plaintiffs' express consent or knowledge and then created consumer reports based upon this intercepted and recorded information.

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

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

86. The FTC Complaint also details how precise geolocation data associated with Apple's IDFA and Android's ADID, collectively referred to herein as MAIDs (mobile advertising identifiers), 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.

87. Defendant's methodology for intercepting these communications and surreptitiously tracking these geolocations through its SDK are essentially identical between Apple iPhones and Android devices, with small technical differences based upon each devices operating systems.

88. For example, Apple refers to its unique advertising identification number on a device as an IDFA, whereas Android refers to this advertising identifier as an ADID, although they are functionally identical for Defendant's purposes in that they provide a unique advertising identifier for the device that is being intercepted and tracked by Defendant.

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

90. 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.

91. If the MAID for a particular device is unavailable to Defendant because tracking has been disabled on the device, Defendant uses a myriad of other techniques such as IDFV, fingerprinting, and other strategies to positively identify the device's user.

92. The location data sold by Defendant typically includes multiple timestamped signals for each MAID and IDFV. 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.

93. 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.

94. 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

95. 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.

96. 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.

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

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

99. 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.

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

101. 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.

102. 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.

103. 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.

104. 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 locations, including sensitive ones.

Id. at ¶ 19.

105. 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 Disclosure of Telephonic Messages

106. 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.

107. 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.

108. Plaintiffs are informed and believes, and thereon alleges, that Defendant intentionally intercepted, received, recorded and then disclosed Plaintiffs' 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 further herein.

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

110. These disclosures of Plaintiffs and Class Member's telephonic messages by Defendant as described further herein was unauthorized and done without their prior knowledge or consent. Plaintiffs 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.

111. As a result thereof, Plaintiffs have been damaged as set forth in the Prayer for Relief herein.

112. Plaintiffs seek statutory damages and injunctive relief under California Penal Code § 637.2.

PLAINTIFFS' AND CLASS MEMBERS' PERSONAL INFORMATION AND GEOLOCATION DATA CONSTITUTE COMMUNICATIONS

113. The data that Defendant intercepts and transmits, from Plaintiffs' and Class members' mobile devices, directly communicate specific device user decisions, actions, choices, and activities of such users such as selection of search terms, click choices, purchase decisions and/or payment methods, amongst others.

114. Defendant goes beyond simply gathering static information with its SDK but rather actively monitors, intercepts, and records specific user input events and choices that a mobile device user communicates through their mobile device by that user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response.

115. Defendant thereafter combines and aggregates these device users' intercepted communications with other data it has gather about a particular user to create actionable intelligence about that user to others for the ultimate purpose of marketing, adverting, and selling to products and services to that user.

116. Moreover, the geolocation data that Defendant gathers and combines with all of the other communication information it intercepts is inextricably linked to those communications and is essential in providing context and clarity to those communications.

117. For example, the fact that a person communicates by selecting a button to purchase a coffee at a ballpark holds an entirely different meaning that if that same person purchases a coffee at an abortion clinic. Likewise, a person ordering a pizza at the beach sends a different communication than if they had ordered that same pizza from a hospice.

118. Defendant's geolocation tracking is an essential element of the communications which it intercepts and is inseparable from it contextually.

PLAINTIFFS AND CLASS MEMBERS WERE HARMED BY THE INVASION OF THEIR PRIVACY

119. Plaintiffs and Class members are harmed by Defendant's multiple invasions of their privacy.

120. Defendant obtained personal data, communications, and information about Plaintiffs and Class members, including Plaintiffs' and Class members' location data.

121. The data, information and communications that Defendant surreptitiously obtains from Plaintiffs' and Class members' cellphones can and are used by Defendant and the third parties to whom Defendant sells Plaintiffs' and Class members' information to identify them and make personalized advertisements to Plaintiffs and Class members individually.

122. Even when individuals attempt to take affirmative steps to protect their privacy, Defendant designed its SDK to circumvent those efforts. Defendant's SDK continues to track Plaintiffs' and Class members' movements, monitor their application selections, choices, uses, and communications, and combined that valuable private information with other data sets to sell to third-parties for advertising, sales, and marketing purposes against their wishes.

123. Defendant fails to inform or obtain consent from Plaintiffs and Class members track, collect, obtain, and sell their data, location history, communications and personal information.

124. Moreover, the depth and breadth of data and communications that Defendant surreptitiously obtains from Plaintiffs and Class members can be easily used to individually identify Plaintiffs and Class members and their movements and habits. As shown in the articles cited above, including to identify individual's residences, places of employment, and locations they have visited, and such information could be used against, in various manners.

CLASS ACTION ALLEGATIONS

125. Plaintiffs bring this lawsuit as a class action on behalf of themselves and, pursuant to Federal Rule of Civil Procedure 23, on behalf of all those similarly situated. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of those provisions.

126. Plaintiffs propose the following Class, consisting of and defined as follows:

> All persons in California downloaded an app with Kochava's SDK on the personal mobile device.

127. 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. Plaintiffs reserve the right to redefine the Class and to add subclasses as appropriate based on discovery and specific theories of liability

128. **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 Plaintiffs 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.

129. **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:

A. Whether Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances;

B. Whether Defendant's conduct invaded Plaintiffs' and Class members' privacy;

C. Whether Defendant knowingly accessed Plaintiffs' and Class members' computers;

D. Whether Defendant knowingly took, copied, or made use of data from Plaintiffs' and Class members' computers;

E. Whether Defendant had permission from Plaintiffs and Class members to access their computers;

F. Whether Defendant's SDK constitutes a pen register device;

G. Whether Defendant's SDK transmits data from Class members' mobile phones to itself;

H. Whether Defendant's SDK transmits Class members' communications to itself;

I. Whether Defendant intercepted Class members' confidential communications;

J. Whether Defendant disseminated information concerning Class members to third parties;

K. Whether Defendant disseminated Class members' confidential communications to third parties;

130. **Typicality**: Plaintiffs' 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.

131. Plaintiffs 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 Plaintiffs' and Class Members' digital communications, geolocations, and other sensitive personal data from their digital devices with others, and Defendant invading the privacy of said Plaintiffs and Class. Plaintiffs and Class Members were damaged thereby.

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

133. **Adequacy**: Each 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. Each Plaintiff acknowledges that he has an obligation to make known to the Court any relationships, conflicts, or differences with any Class Member. Plaintiffs' attorneys, the proposed class counsel, are versed in the rules governing class action discovery, certification, and settlement. In addition, Plaintiffs' 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. Plaintiffs have 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.

134. **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 Plaintiffs and Class Members are capable of proof at trial through evidence that is common to the Class rather than individual to its members.

135. **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.

136. Plaintiffs 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.

137. The Class may also be certified because:

A. 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

B. 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.

138. 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.

139. 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.

CAUSES OF ACTION

COUNT ONE
Invasion of Privacy

140. Each Plaintiff repeats, re-alleges, and incorporates by reference preceding paragraphs above as if fully set forth herein.

141. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

142. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

143. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy

from both the government and private entities alike: “The right of privacy is the right to be left alone. It is a fundamental and compelling interest. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information.” Ballot Pamp., Proposed Stats. and Amends. to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*,530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one’s home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting).

144. Plaintiffs and Class members have a legally protected privacy interests, as recognized by the California Constitution, CIPA, common law and the 4th Amendment to the United States Constitution.

145. Plaintiffs and Class members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state and federal privacy laws. Plaintiffs and Class members were not aware and could not have reasonably expected that unknown third party would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiffs’ and Class members’ personal information with other parties.

146. Defendant’s conduct violates, at a minimum:

A. The right to privacy in data, communications and personal information contained on personal devices;

B. The California Constitution, Article I, Section 1;

C. The California Wiretapping Act;

D. The California Invasion of Privacy Act; and

E. The California Computer Data Access and Fraud Act.

147. Defendant's conduct in secretly intercepting and collecting Plaintiffs' and Class members' personal information, location data, and communications is an egregious breach of societal norms and is highly offensive to a reasonable person.

148. Defendant's conduct in analyzing, using, and sharing with third parties the personal information and communications that Defendant intercepted and took from Plaintiffs' and Class members is an egregious breach of societal norms and is highly offensive to a reasonable person, and violates Plaintiffs' and Class members' reasonable expectations of privacy.

149. Plaintiffs and Class members did not consent for Defendant to track, collect, or use their personal information and communications.

150. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiffs and Class members were injured and suffered damages. Plaintiffs and Class members are entitled to equitable relief and just compensation in an amount to be determined at trial.

151. Defendant was unjustly enriched as a result of its invasion of Plaintiffs' and Class members' privacy.

COUNT TWO
Violation of the California Computer Data Access and Fraud Act
Cal. Penal Code. § 502

152. Each Plaintiff repeats, re-alleges, and incorporates by reference preceding paragraphs above as if fully set forth herein.

153. The California legislature enacted the CDAFA with the intent of "expand[ing] the degree of protection afforded to individuals . . . from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a). The enactment of CDAFA was motivated by the finding that "the proliferation of computer technology has resulted in a concomitant proliferation of . . . unauthorized access to computers, computer systems, and computer data." *Id.*

154. Plaintiffs' and Class members' smartphone constitute "computers" within the scope of the CDAFA.

155. Defendant violated the following sections of the CDAFA:

A. Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

B. Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

C. Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

156. Defendant knowingly accessed Plaintiffs' and Class members' smartphones without their permission by including within the SDK, that Defendant provides to developers, software that intercepts and transmits data, communications, and personal information concerning Plaintiffs and Class members.

157. Defendant used data, communications, and personal information that it intercepted and took from Plaintiffs' and Class members' smart phones to wrongfully and unjustly enrich itself at the expense of Plaintiffs and Class members.

158. Defendant took, copied, intercepted, and made use of data, communications, and personal information from Plaintiffs' and Class members' smartphones.

159. Defendant knowingly and without Plaintiffs' and Class members' permission accessed or caused to be their smartphones by installing without Plaintiffs' and Class members' informed consent software that intercepts and/or takes data, communications, and personal information concerning Plaintiffs and Class members.

160. Plaintiffs and Class members are residents of California, and used their smartphones in California. Defendant accessed or caused to be accessed Plaintiffs' and Class members' data, communications, and personal information from California. On information and belief, Defendant uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning Plaintiffs and Class members.

161. Defendant was unjustly enriched by intercepting, acquiring, taking, or using Plaintiffs' and Class members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

162. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs and Class members suffered damages.

163. Pursuant to CDAFA Section 502(e)(1), Plaintiffs and Class members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

164. Pursuant to CDAFA Section 502(e)(2), Plaintiffs and Class members seek an award of reasonable attorneys' fees and costs.

165. Pursuant to CDAFA Section 502(e)(4), Plaintiffs and Class members seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.

COUNT THREE
Use of a Pen Register or Trap and Trace Device
Cal. Penal Code § 638.51

166. Each Plaintiff repeats, re-alleges, and incorporates by reference preceding paragraphs above as if fully set forth herein.

167. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling

information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

168. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

169. Defendant's SDK constitutes a "pen register" because it is a device or process that records addressing or signaling information—Plaintiffs' and Class members' location data and personal information—from the electronic communications transmitted by their smartphones.

170. Defendant was not authorized by any court order to use a pen register to track Plaintiffs' and Class members' location data and personal information.

171. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members suffered losses and were damaged in an amount to be determined at trial.

COUNT FOUR
Violation of the California Wiretapping Act
Cal. Penal Code § 631

172. Each Plaintiff repeats, re-alleges, and incorporates by reference preceding paragraphs above as if fully set forth herein.

173. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

174. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

175. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.*

176. The California Wiretapping Act prohibits:

> “any person [from using] any machine, instrument, [] contrivance, or in any other manner . . . [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

177. Plaintiffs’ and Class members’ specific user input events and choices on their mobile devices that are tracked by Defendant’s SDK communicates the user’s affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the Wiretapping Act.

178. Plaintiffs and Class members are residents of California, and used their smartphones within California. As such, Defendant intercepts, reads, or attempts to reads Plaintiffs’ and Class members’ data, communications, and personal information in California.

179. On information and belief, Defendant uses servers in California to intercept, track, process, or otherwise use Plaintiffs’ and Class members’ data, communications, and personal information within California.

180. Defendant intercepts Plaintiffs’ and Class members’ communications while they are in transit to and from Plaintiffs’ and Class members’ smartphones and the apps, app developers, and cellphone towers; Defendant transmits a copy of Plaintiffs’ and Class members’ communications to itself. Defendant uses the contents

of the communications to sell to third parties and in other methods for its own pecuniary gain.

181. Neither Defendant nor any other person informed Plaintiffs and Class members that Defendant was intercepting and transmitting Plaintiffs' private communications. Plaintiffs and Class members did not know Defendant was intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendant and thereafter transmitted to others.

182. Defendant's SDK constitutes a machine, instrument, contrivance or other manner to track and intercept Plaintiffs' and Class members' communications while they are using their smartphones.

183. Defendant uses and attempts to use or communicate the meaning of Plaintiffs' and Class members' communications by ascertaining their personal information, including their geolocation and places that they have visited, in order to sell Plaintiffs' and Class members' personal information to third parties.

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

185. At all relevant times to this complaint, Plaintiffs 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.

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

187. 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).

188. Defendant's use of MAIDs, IDFAs, IDFVs and its SDK are both a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct at issue here.

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

190. 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 Plaintiffs 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.

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

192. Plaintiffs' 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.

193. 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 Plaintiffs' and Class Members' reasonable expectations of privacy in their devices and data.

194. 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.

195. As a direct and proximate result of Defendant's violation of the Wiretapping Act, Plaintiffs and Class members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

196. Defendant was unjustly enriched by its violation of the Wiretapping Act.

197. Pursuant to California Penal Code Section 637.2, Plaintiffs and Class members have been injured by Defendant's violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff David Greenley, individually and on behalf of all others similarly situated, requests that this Court:

A. Determine that the claims alleged herein may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and issue an order certifying the Class defined above;

B. Appoint Plaintiffs as the representatives of the Class and their counsel as Class counsel;

C. Award all actual, general, special, incidental, statutory, punitive, and consequential damages, treble damages, and restitution to which Plaintiffs and the Class members are entitled by law;

D. Award pre-judgment and post-judgment interest on such monetary relief;

E. Grant appropriate injunctive and/or declaratory relief, including, without limitation, an order that requires Defendant to disclose its practices collecting and disseminating personal information, data, and communications, and to refrain from collecting, retaining, using and disseminating Plaintiffs' and Class members' personal information, geolocation data, and communications without disclosing the full extent of its practices;

F. Award reasonable attorneys' fees and costs; and

G. Grant such further relief that this Court deems appropriate.

JURY DEMAND

Plaintiffs, on behalf of themselves and the putative Class demand a trial by jury on all issues so triable.

Date: October 23, 2023 Respectfully submitted,

By: *s/ Joshua Swigart*
Joshua B. Swigart, Esq.
SWIGART LAW GROUP
2221 Camino del Rio S, Ste 308
San Diego, CA 92108
Telephone: 866-219-3343
Facsimile: 866-219-8344
Josh@SwigartLawGroup.com

Peter F. Barry (*Pro Hac Vice Pending*)
THE BARRY LAW OFFICE, LTD
333 Washington Ave No, Suite 300-9038
Minneapolis MN 55401-1353

Telephone: (612) 379-8800
pbarry@lawpoint.com

Daniel O. Herrera (*Admitted Pro Hac Vice)*
Nickolas J. Hagman (*Pro Hac Vice Pending*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

John J. Nelson (SBN 317598)
Milberg Coleman Bryson Phillips Grossman
280 South Beverly Drive
90212
Beverly Hills, CA 90212
619-209-6941
Email: *jnelson@milberg.com*

Attorneys for Plaintiff
and the Proposed Class