BRIAN SHULL, IL Bar No. 6293797
JULIA A. HORWITZ, DC Bar No. 1018561
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Phone: (202) 326-3734
Fax: (202) 326-3062
bshull@ftc.gov
jhorwitz@ftc.gov

ELIZABETH C. SCOTT, IL Bar No. 6278075
Federal Trade Commission
230 S. Dearborn St., Ste. 3030
Chicago, IL 60604
Phone: (312) 960-5609
Fax: (312) 960-5600
escott@ftc.gov

ATTORNEYS FOR PLAINTIFF

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO

FEDERAL TRADE COMMISSION, Plaintiff, v. KOCHAVA INC., corporation, Defendant.	**Case No. 2:22-cv-00377-BLW** **AMENDED COMPLAINT FOR PERMANENT INJUNCTION AND OTHER RELIEF**

Plaintiff, the Federal Trade Commission ("FTC"), for its Complaint alleges:

1. The FTC brings this action under Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b), which authorizes the FTC to seek, and the Court to order, permanent injunctive relief and other relief for Defendant's acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

2. Defendant Kochava Inc. ("Kochava") is a data broker that collects and sells consumers' personal data to its customers for their own uses. Kochava's violations of the FTC Act are in connection with acquiring and using consumers' sensitive, identifying information and disclosing the information to third parties without consumers' knowledge or consent.

3. Notably, Kochava collects consumers' precise geolocation information that is obtained from their mobile devices and that is associated with a persistent and individual identifier. This data is used to trace consumers' movements over a day, week, month, and even year, including to locations that are sensitive and personal. Kochava promises its customers that the data is so precise that it accurately places consumers' movements to within only a few meters – enough to not only tell what building the consumers are in, but even what room.

4. Kochava itself concedes that this data is not anonymous, but rather can be, and is, used to track and identify individual consumers. In many cases, Kochava provides data that directly links this precise geolocation data to identifying information about individual consumers, such as names, addresses, email addresses, and phone numbers.

5. Kochava's use and disclosure of this precise geolocation information invade consumers' privacy and cause or are likely to cause consumers substantial injury. In addition, Kochava collects, uses, and discloses enormous amounts of additional private and sensitive information about consumers. Kochava's use and disclosure of this data, whether alone or in conjunction with Kochava's geolocation data, also invade consumers' privacy and cause or are likely to cause consumers substantial injury.

JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345.

7. Venue is proper in this District under 28 U.S.C. § 1391 (b)(1), (b)(2), and (c)(2) and 15 U.S.C. § 53(b).

PLAINTIFF

8. The FTC is an independent agency of the United States Government created by the FTC Act, which authorizes the FTC to commence this district court civil action by its own attorneys. 15 U.S.C. §§ 41–58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

DEFENDANT

9. Defendant Kochava is a Delaware corporation with its principal place of business at 201 Church Street, Sandpoint, Idaho 83864. Kochava transacts or has transacted business in this District and throughout the United States.

COMMERCE

10. At all times relevant to this Complaint, Defendant has maintained a substantial course of trade in or affecting commerce, as "commerce" is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANT'S BUSINESS ACTIVITIES

Kochava Collects, Uses, and Discloses Massive Amounts of Information About Consumers

11. Kochava is a data broker, and its business is to sell information about consumers. It provides its customers, among other things, precise geolocation data collected from millions of

consumers' mobile devices. Through Kochava's services, customers can "[l]icense premium data" including the "precision location" of a consumer's mobile device.

12. Kochava's collection, use, and disclosure of precise geolocation data invade consumers' privacy by revealing their movements throughout a day, week, month, year, or even more, including their visits to sensitive locations—for example, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery.

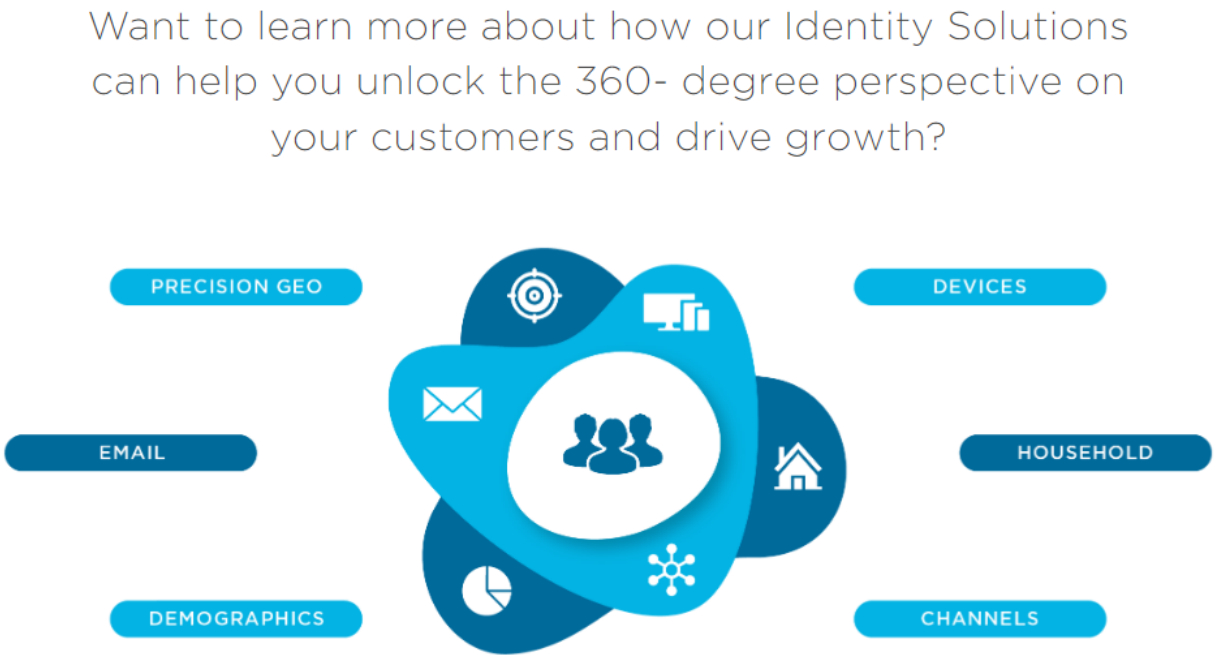
13. Kochava's precise geolocation data includes timestamped latitude and longitude coordinates showing the location of mobile devices over time. Kochava includes with each pair of coordinates a persistent identifier known as a Mobile Advertising ID ("MAID"). A MAID is assigned by a mobile device's operating system to allow companies to track a consumer's mobile activity and is used to send targeted advertisements.

14. Kochava ensures that MAIDs provide no anonymity for consumers. Kochava sells data that directly links MAIDs to individual consumers' identifying information, and Kochava expressly encourages its customers to use this data. As a result, Kochava's customers can learn sensitive information about individual consumers who are identifiable without inference or additional steps.

15. Even if Kochava did not affirmatively connect MAIDS to individual consumers, precise geolocation data that tracks consumers' movements over time and is associated with a MAID or other persistent identifier is not anonymized data, as Kochava itself has recognized. Such data can be and is used to identify consumers and sensitive information about them.

16. In addition to precise geolocation data, Kochava amasses and discloses a staggering amount of sensitive and identifying information about consumers, including their names, MAIDs, addresses, phone numbers, email addresses, gender, age, ethnicity, yearly income, "economic stability," marital status, education level, political affiliation, "app affinity" (i.e. what apps consumers have installed on their phones), app usage, and "interests and behaviors."

17. Kochava tells potential buyers that its massive collection of consumer information provides a "360-degree perspective" on consumers:



18. Kochava emphasizes its ability to connect each individual consumer to multiple "data points" in order to ensure that its customers are able to continuously track consumers and connect consumers' activities with historic and new data. As identified in the above graphic, Kochava advertises being able to connect precise geolocation data with email, demographics, devices, households, and channels.

19. Unsatisfied with this already substantial violation of consumers' privacy, Kochava goes even farther. Kochava categorizes consumers into groupings in order to target consumers, often based on specific sensitive and personal characteristics or attributes identified from its massive collection of data about individual consumers.

20. Kochava sells all of this data as part of its "Kochava Collective," which it claims is the "world's largest independent mobile data marketplace." Kochava collects, stores, and shares information, which is often, on its face, sensitive or private, on hundreds of millions of consumers. This information is not readily observable by the public. Kochava obtains it from a myriad of sources, including from mobile apps and other data brokers.

21. Customers pay a monthly subscription, often in the tens of thousands of dollars, to access the data in the Kochava Collective. In some instances, Kochava also makes a free sample available.

22. Kochava sells data in several different forms in the Kochava Collective, including: 1) precise geolocation data; 2) comprehensive profiles of individual consumers (the "Database Graph"); 3) tracking consumers' uses of mobile apps on their devices (the "App Graph"); and 4) categorized consumers based on identified sensitive and personal characteristics and attributes ("audience segments").

23. Customers can and do purchase any and all of this data. Thus, Kochava's data identifies, for example, a woman who visits a particular building, the woman's name, email address, and home address, and whether the woman is African-American, a parent (and if so, how many children), or has an app identifying symptoms of cancer on her phone. This ability

to target consumers on such granular facts about them is precisely the point of the Kochava Collective, as Kochava makes clear to potential customers.

24. Each of Kochava's data points, whether used alone or in connection with other data provided by Kochava, invades consumers' privacy and causes or is likely to cause consumers substantial injury that is not reasonably avoidable by consumers.

Kochava's Geolocation Data: Feeds of Precise Geolocation Data about Consumers

25. Kochava acquires consumers' precise geolocation data from other data brokers. Kochava does not, itself, interact directly with individual consumers.

26. Kochava then sells access to the precise geolocation data to its customers as part of the Kochava Collective. The data is collected from a mobile device's GPS coordinates and may, at times, be augmented by other signals, such as WiFi. Kochava asserts that its precise geolocation data can often pinpoint a consumer's location to within less than 10 meters. Kochava's precise geolocation data includes data that tracks consumers' movements for at least the past year and is updated regularly as new information is obtained. The precise geolocation data includes consumers' movements as recent as the prior day.

27. This geolocation data includes timestamped latitude and longitude coordinates showing the location of mobile devices.

28. For example, in the Amazon Web Services ("AWS") Marketplace, a website through which customers could subscribe to Kochava's data feed until approximately June 2022, Kochava displayed the following table explaining the data it sells:

Field name	Description	Example	Data type
device_id_value	Unique device ID associated with the device	-	string
device_id_type	Device type associated with the device (IDFA and ADID only)	-	string
activity_timestamp	Timestamp of when the device hits the location	-	timestamp
latitude	Precise latitude of the device	-	string
longitude	Precise longitude of the device	-	string
horizontal_accuracy	Horizontal accuracty of the precision of the lat and lon (in meters)	-	string
ip_address	IP Address of the device	-	string

29. Each pair of timestamped latitude and longitude coordinates in Kochava's precise geolocation data feed is also associated with a "device_id_value." This device id is the phone's MAID.

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

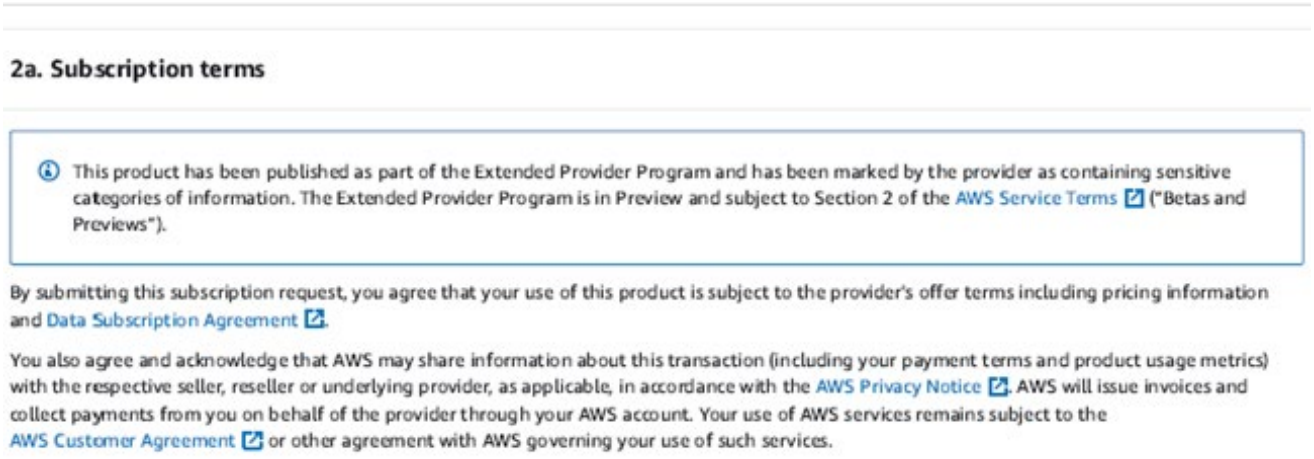
31. Kochava has also offered a free sample (the "Kochava Data Sample"). Kochava has made the Kochava Data Sample publicly available with only minimal steps to obtain the data and no restrictions on usage.

32. For example, the Kochava Data Sample was available on the AWS Marketplace until approximately June 2022. To access the Kochava Data Sample on the AWS Marketplace,

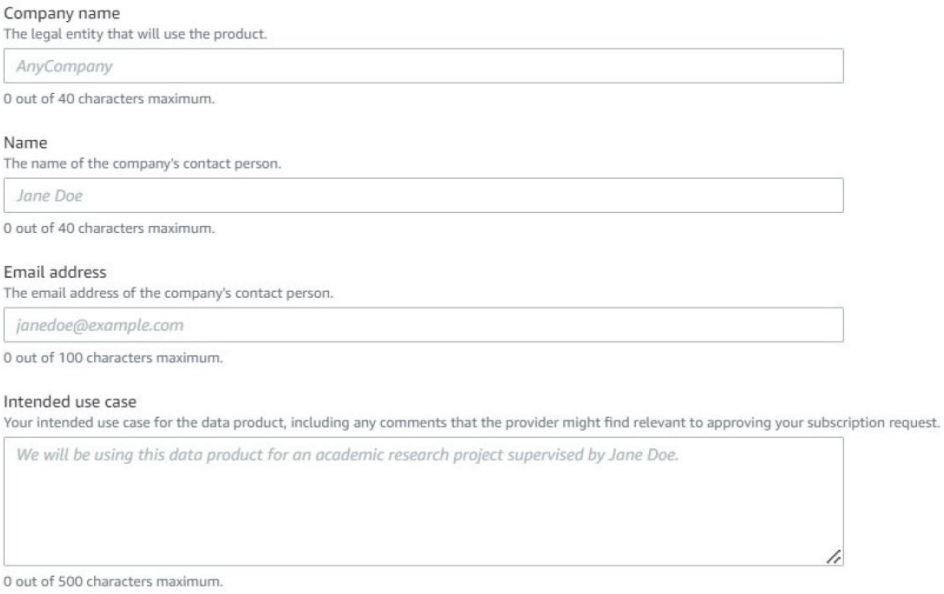
a purchaser needed a free AWS account. (Anyone can sign up for and obtain a free AWS account within minutes.) A purchaser would then search the AWS marketplace for "Kochava," which resulted in at least two available datasets appearing – a $25,000 location data feed subscription and the Kochava Data Sample.

33. 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. Put into a spreadsheet, one day of the Kochava Data Sample contained over 327,480,000 rows and 11 columns of data, corresponding to over 61,803,400 unique mobile devices.

34. When an AWS purchaser clicked on the "subscribe" button for the Kochava Data Sample feed, the purchaser was directed to a screen that included a "Subscription terms" notification that stated that the Kochava Data Sample "has been marked by the provider [*i.e.,* Kochava] as containing **sensitive categories of information**" (emphasis added):



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



36. A purchaser could use an ordinary personal email address, identify the company as "self," and describe the intended use simply as "business." The request would then be sent to Kochava for approval. Kochava has approved such requests in as little as 24 hours without any additional inquiries or requesting additional information about the purchaser or their intended use.

37. Once Kochava approved the request, the purchaser was notified by email and then gained unfettered access to the data, along with a data dictionary explaining the categories of data provided.

38. The Kochava Data Sample included precise location data gathered again and again from consumers' mobile devices in the seven days prior to the date Kochava approved the subscription request. The Kochava Data Sample is only a small subset of the full precise geolocation feed sold by Kochava.

39. Kochava's precise geolocation data can be used to identify consumers who have visited an abortion clinic and, as a result, may have had or contemplated having an abortion. In

fact, in just the data Kochava made available in the Kochava Data Sample, Plaintiff identified a mobile device that visited a women's reproductive health clinic and traced that mobile device to a single-family residence. The data set also reveals that the same mobile device was at a particular location at least three evenings in the same week, suggesting the mobile device user's routine. The data can also be used to identify medical professionals who perform, or assist in the performance, of abortion services

40. As another example, the data can be used to track consumers to places of worship, and thus reveal the religious beliefs and practices of consumers. In fact, Plaintiff identified in the Kochava Data Sample mobile devices that were located at Jewish, Christian, Islamic, and other religious denominations' places of worship.

41. As another example, the data can be used to track consumers who visited a homeless shelter, domestic violence shelter, or other facilities directed to at-risk populations. This information can reveal the location of consumers who are escaping domestic violence or other crimes. In addition, because Kochava's data allows its customers to track consumers over time, the data could be used to identify consumers' past conditions, such as homelessness. In fact, Plaintiff identified in the Kochava Data Sample a mobile device that appears to have spent the night at a temporary shelter whose mission is to provide residence for at-risk, pregnant young women or new mothers.

42. As another example, the data can be used to track consumers who have visited addiction recovery centers. The data can show how long consumers stayed at the center and whether a consumer relapses and returns to a recovery center.

43. Consumers do not expect or want data brokers to collect their precise geolocation

data. Indeed, data brokers' collection, aggregation, and disclosure of location data violate consumers' expectations of privacy. Consumers disapprove even more strongly when entities collecting their location data use it to make inferences about them. Consumers also do not consent to such collection or disclosure. And because consumers do not know that Kochava is collecting this data, consumers cannot avoid the harm resulting from the collection, use, or subsequent disclosure.

Kochava's Database Graph: Comprehensive Profiles about Consumers

44. Precise geolocation associated with persistent identifiers such as MAIDs is sufficient to identify consumers. But Kochava makes it even easier: for hundreds of millions of consumers, Kochava directly links MAIDs with other personally identifying information, such as names, email addresses, home addresses, and phone numbers. Indeed, Kochava creates comprehensive profiles on consumers that Kochava calls its "Database Graph" or "PII" (Personally Identifiable Information) graph.

45. Kochava collects data from other data brokers to build its Database Graph.

46. Kochava brags that its Database Graph identifies "over 300M unique individuals in the US" with up to "300 data points that can be tied to those profiles." In other words, Kochava's Database Graph encompasses nearly the entire United States, which has a population of 330 million individuals.

47. Kochava's Database Graph builds profiles about individual consumers and identifies their:

a) name;

b) address;

c) email address;

d) phone number; and

e) MAID.

48. The inclusion of the MAID in this dataset ensures that MAIDs offer consumers no anonymity from Kochava or its customers.

49. Kochava's Database Graph also identifies consumers' sensitive characteristics, including:

a) ethnicity;

b) gender identity;

c) date of birth;

d) status as a minor;

e) status as a parent and number of children;

f) political association; and

g) marital status.

50. For example, as noted above, one data point Kochava discloses about a consumer is the consumer's gender identity. Kochava discloses whether the person identifies as "Male," "Female," or "Other:"

Gender	MALE	Gender of a person where it will be all capital alphabetic letters. Answers will include: "MALE" "FEMALE" "OTHER"

51. As another example, Kochava discloses to third parties a consumer's ethnicity:

Ethnicity	AFRICAN-AMERICAN	Ethnicity of a person. This will be all uppercase alphabetic letters. If there are multiple words please separate each one with "-" in between as shown in the example.

52. As another example, Kochava discloses to third parties a consumer's political affiliations:

Political Party Affiliation	REPUBLICAN	This is the political party that the person is affiliated with. All answers will have uppercase alphabetic letters. Acceptable answers include the following: "REPUBLICAN" "DEMOCRAT" "UKNOWN"

53. Other "data points" included in Kochava's Database Graph relate to consumers' education, economic status, employment, languages spoken, device settings, and social media presence.

54. Consumers routinely pay Kochava to access all of the information Kochava has about individual consumers. For example, in one case, a company contracted with Kochava to provide it with profiles on a "[m]inimum of 150M" US consumers every month and requested that every data point contained in the Kochava Collective, including each one identified above, be included in the profiles about individual consumers.

55. Kochava collects and discloses consumers' personally identifying information and sensitive information to third parties without consumers' knowledge or consent. Indeed, consumers do not know that Kochava has collected their information or is disclosing it to third parties.

56. Consumers have expressed concern about the amount of personal information various entities - like advertisers, employers, or law enforcement - know about them and about how such entities use their personal data. Consumers are increasingly reluctant to share their

personal information, such as digital activity, emails, text messages, and phone calls, especially without knowing which entities will receive it. This is precisely what Kochava does and its collection, use, and disclosure of consumers' personal information under such circumstances imposes an unwarranted invasion into consumers' privacy.

Kochava's App Graph: Tracking Consumers' Actions on Mobile Apps

57. In addition to precise geolocation information tracking consumers' daily movements and comprehensive profiles of personally identifying information about consumers, Kochava also collects, uses, and sells detailed information about what consumers do on their mobile devices through its App Graph and App Activity (collectively, Kochava's "App Graph").

58. Kochava's App Graph is based on a combination of data acquired from other data brokers and information Kochava collects about consumers' app usage through its own Free App Analytics Software Development Kit ("FAA SDK"). The FAA SDK is a set of digital software development tools compiled into one package, or "kit." App developers can install the FAA SDK in their apps to facilitate the tracking of ads and consumers' activities in the app.

59. When a consumer uses a mobile app in which Kochava's FAA SDK has been included, the FAA SDK passes information to Kochava about the user's activity on the app. In exchange for the free use of Kochava's FAA SDK, Kochava requires app developers to agree to grant Kochava a "perpetual, irrevocable, worldwide, transferrable unrestricted license" to consumer information collected via the FAA SDK. Kochava's license even survives a termination of the agreement between Kochava and the app developer, allowing Kochava to use the data forever.

60. Kochava's FAA SDK is installed in at least "10,000 apps globally" and Kochava claims that its App Graph, which includes information from the FAA SDK and information obtained from other data brokers, contains information about consumers' usage of over 275,000 mobile apps.

61. For example, information sold by Kochava as part of its App Graph includes:

a) the name of the app being used;

b) the date of the usage;

c) how long, in seconds, the app is used;

d) the type of actions the users takes in the app; and

e) how much money the user spends in the app.

All of this information is linked to the consumer's MAID and, as alleged above, Kochava connects MAIDs to consumers' precise geolocation as well as names, addresses, phone numbers, email addresses, and other identifying information.

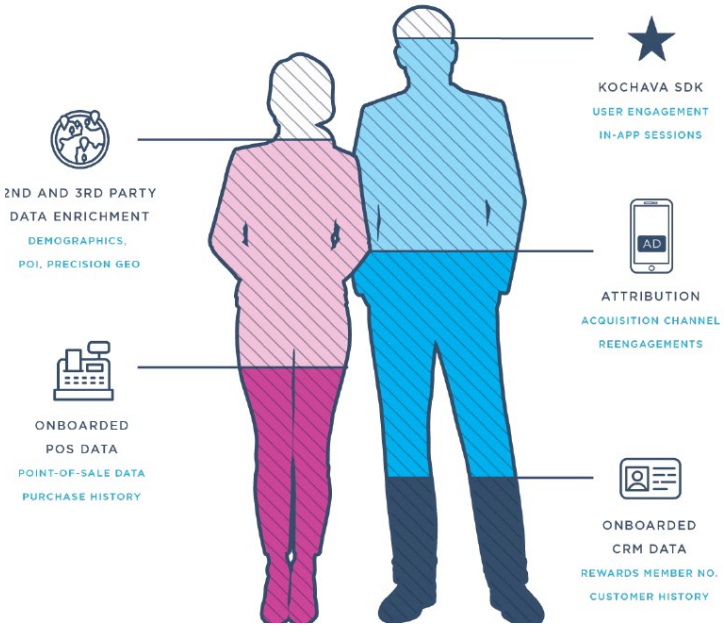
62. Many of these apps are used for private or sensitive purposes. For example, among the apps included in Kochava's App Graph are dating apps, including LGBTQ+-focused dating apps. Kochava's App Graph is also fed by apps that are used by certain religious groups, such as Muslim prayer apps, and apps that provide information about health issues, such as cancer or sexually transmitted infections.

63. Consumers do not know that Kochava collects this information about them or that Kochava then discloses the information to third parties that are not the app developer or publisher. Consumers do not consent to this collection or disclosure by Kochava.

Kochava's Audience Segments: Targeting Consumers on the Basis of Sensitive Attributes

64. Kochava does not just collect and disclose a massive amount of personal and sensitive information about consumers; it also analyzes the data in order to create additional data points to sell to its customers. For example, Kochava uses the data it collects to create "audience segments," or subsets of its database of consumer information that identify consumers based on interests or characteristics. Purchasing Kochava's "audience segments" allows Kochava's customers to identify and target consumers based on identified sensitive and personal interests or characteristics.

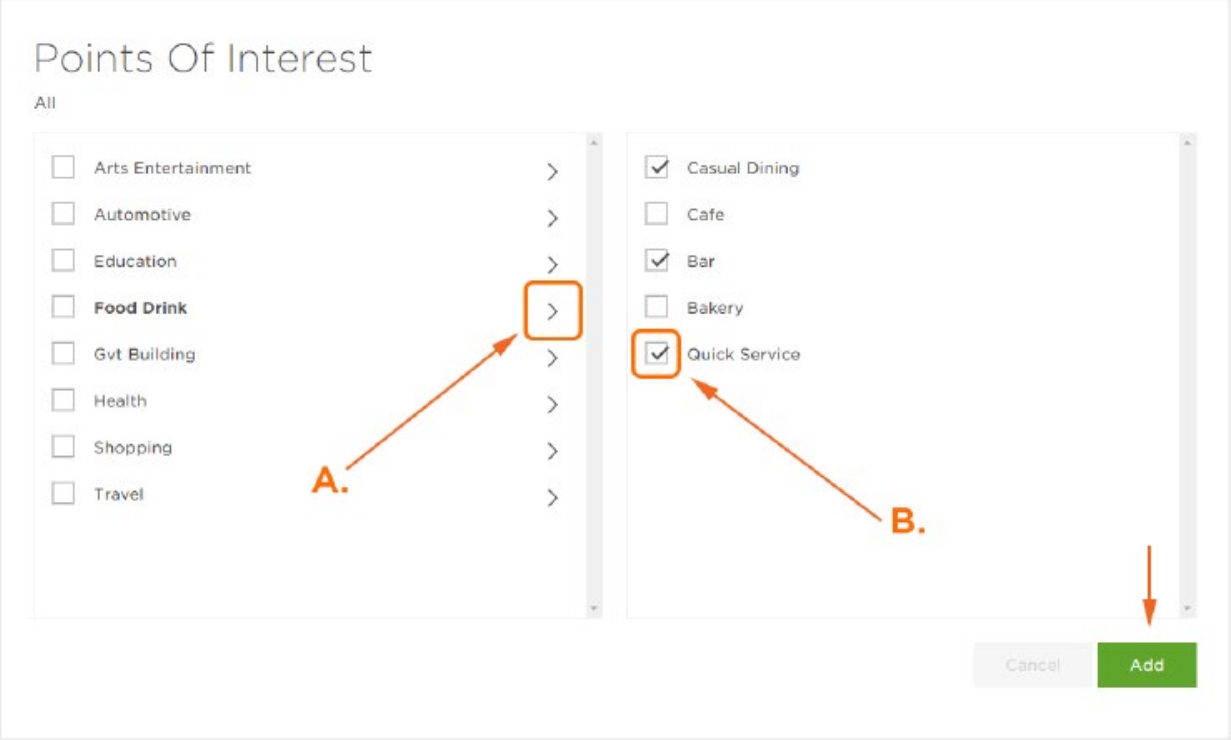
65. Kochava's audience segments are based on the wide array of information Kochava collects about consumers, such as information from its SDK and information collected from other data brokers, as this graphic from a Kochava webpage about its audience segments demonstrates:



66. Kochava explains that it creates and refines audience segments "by a variety of metrics such as geography, demographics, points of interest, app usage and web usage." Each

audience segment contains a list of the MAIDs of consumers that meet the specified interests or characteristics. As alleged above, Kochava also matches MAIDs to consumers' names, addresses, phone numbers, email addresses, and other identifying information.

67. For example, Kochava's audience segments target consumers based on places they have visited, including locations associated with "Education," "Gvt Building," and "Health":

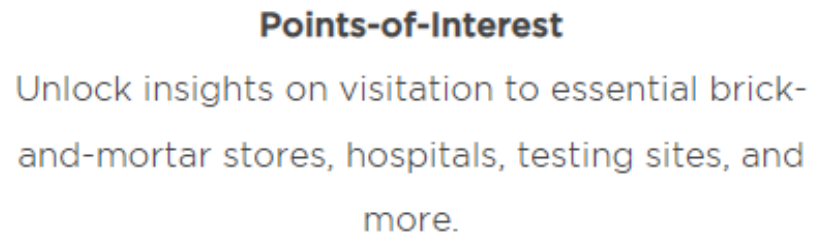


Customers may select a category of locations they wish to track (as Kochava demonstrates in this graphic through the orange arrows and boxes) or may identify a single location to track.

68. As one example of this, in advertising the power of its data to target consumers based on their political associations, Kochava explains that its audience segments allow customers to "[f]ind devices that intersect with important events or locations, or seek out devices that spend time in areas targeted by your campaign" and "[u]nderstand voter visitation to home,

work, places of business, government buildings, and more." And showing the multiplying invasiveness of Kochava's data, Kochava suggests further tracking a consumer's "political leanings based on apps the voter has installed on their mobile device."

69. As another example, on a webpage advertising how Kochava's data could be used to study the effects of COVID-19, Kochava acknowledges that its data has included visitation information to sensitive locations such as hospitals and testing sites:



70. Other audience segments are based on sensitive characteristics of consumers.

71. For example, one audience segment sold by Kochava is "Expecting Parents," which, in this iteration, includes over 11.4 million MAIDs:

This iteration of this audience segment is created based on consumers' usage of pregnancy, ovulation, or menstruation tracking apps.

72. Kochava also builds audience segments of consumers based on their "interests and behaviors." Kochava explains that these audience segments are built based on an online "Content Taxonomy."

73. This taxonomy includes sensitive and private characteristics about consumers, including:

a) "Reproductive Health;"

b) "Cancer;"

c) "Women's Health;"

d) "Divorce;"

e) "Bereavement;"

f) "Eldercare;"

g) "Adoption and Fostering;"

h) "Special Needs Kids;"

i) "Sexual Conditions;"

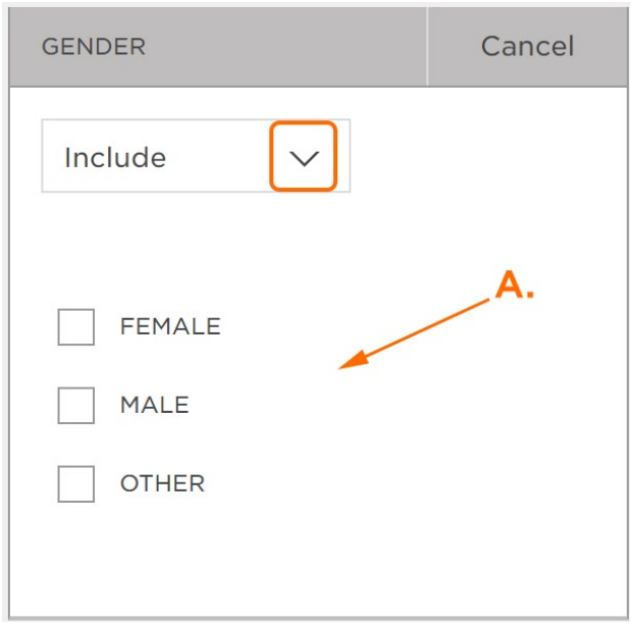
j) "Pregnancy;"

k) "Vaccines;"

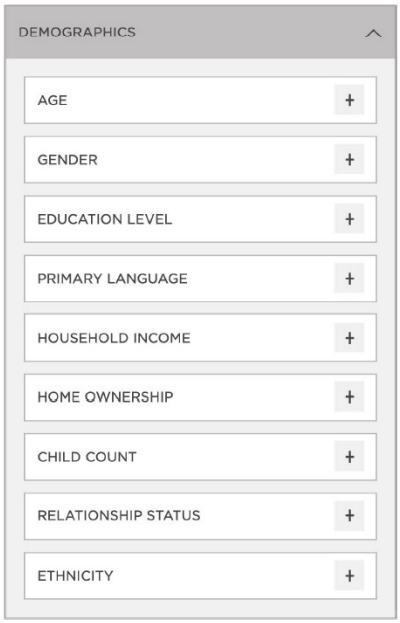
l) "Judaism;" and

m) "Islam."

74. As another example, Kochava's audience segments may be broken out by gender identity:



75. As another example, Kochava's audience segments may be broken out by other demographic information such as "Ethnicity:"



76. Using these audience segments, a Kochava customer can, for example, purchase a list of all the pregnant consumers, or all the divorced consumers, or all the Jewish consumers, or all the pregnant Muslim women in Kochava's database. Indeed, Kochava advertises such use

cases expressly in its marketing material. It tells prospective customers they can "target parents with different ages of children, new parents, single individuals in the dating market, etc." Kochava's success explicitly depends on its ability to create, market, and sell these detailed sets of data about consumers.

Kochava's Data Is Not Anonymized and Identification Regularly Happens in the Consumer Data Marketplace

77. Kochava's data is not anonymized and is linked or easily linkable to individual consumers. Indeed, Kochava actively markets its ability to link consumers' real names, addresses, email addresses, and phone numbers to sensitive information, including their gender, marital status, and age:

> From the 320M+ unique monthly visitors, create people profiles and garner names, addresses, marital status, education level, economic stability, yearly income, email addresses, phone numbers, gender, and age.

78. Each of Kochava's products discussed above is associated with a consumer's MAID. MAIDs are the framework for tracking and targeting consumers in the mobile marketplace and MAIDs offer no anonymity in the marketplace. Many businesses, including Kochava, regularly link consumers' MAIDs to other information about them, such as names, addresses, and phone numbers. Indeed, Kochava offers its customers the ability to do this as a feature of the Kochava Collective through its Database Graph. Thus, although a MAID is supposedly resettable by consumers (to the extent that consumers even know that their devices have MAIDs, that consumers can reset their MAIDs, or how they might try to do so), Kochava's services mean that resetting a MAID offers no privacy protections to consumers. Kochava

advertises this ability explicitly, boasting that the Kochava Collective contains "other points to connect to and securely solve for identity."

79. Indeed, as part of its Database Graph, Kochava associates multiple MAIDs with a single consumer, ensuring that individual consumers are tracked across devices and even potentially after resetting a MAID.

80. As part of its "360-degree perspective," Kochava connects MAIDs with practically any part of a consumer's identity. For example, Kochava advertises that customers are able to search through its "500M+ MAIDs" to identify, among other things, the consumer's name, address, phone number, email address, gender, age, yearly income, "economic stability," marital status, education level, app affinity, and interests and behaviors.

81. Kochava's customers do not need to mine other sources of data to breach any purported wall of consumer anonymity. This ability is a featured product of Kochava.

82. Nor is this data aggregated in any way that provides consumers with privacy protections. Indeed, Kochava emphasizes its ability to identify individual consumers by bragging that: "the Collective can tie the IDs to **a single user** using a match key (e.g., email address, phone number, mobile advertising ID [MAID], cookie, addresses, etc.) for **one-to-one advertising**" (emphasis added).

83. Moreover, even if Kochava did not link consumers' MAIDs to their names, email addresses, and other identifying information, MAIDs in combination with the precise geolocation data sold by Kochava in its data feeds also reveal the identity of consumers. The location data sold by Kochava typically includes multiple timestamped location signals for each MAID. By plotting each of these signals on a map, the identification of consumers is

straightforward. For example, the location of a mobile device at night likely corresponds to the consumer's home address. Indeed, Kochava explicitly makes this exact conclusion, as it explained while marketing its product to potential customers:

- We determine a home location by looking at the resting lat/long of a given device between the hours of 10pm and 6am and omit known business locations.

84. Kochava recognizes that, because of the unique nature of precise geolocation gathered from mobile phones and what it reveals about consumers, the data is not anonymized. For example, in a news article about Kochava's data, Kochava's Chief Executive Officer, Charles Manning, criticized, on privacy grounds, a competitor's use of precise geolocation data to publicly track the spread of COVID: "But one of the challenges I saw in that demo, although it was very slick and very appealing to watch, there was really no notion of anonymized, aggregated date there. You're looking at specific devices." Mr. Manning made such criticism despite Kochava's own collection, use, and sale of precisely the same type of data and the company's lack of any meaningful controls for the use of that data.

85. In its marketing on the AWS Marketplace, Kochava further recognized the ease with which the location data it sells can, by itself, identify consumers, including where they live. In that marketing, Kochava identified "Household Mapping" as a use case of the data:

HOUSEHOLD MAPPING:

Group devices by dwelling time and frequency at shared locations to map individual devices to households.

86. Indeed, Kochava brags that it has itself identified "180M+ unique monthly households" with, among other things, email addresses, phone numbers, and MAIDs associated with the household.

87. Companies and other entities are using precise geolocation data to identify consumers and their activities by tracking their movements – this does and is happening in the marketplace. In one well-publicized example, a group used precise mobile geolocation data to identify by name a Catholic priest who visited LGBTQ+-associated locations, thereby exposing the priest's sexual preferences and forcing him to resign his position. As another example, journalists who purchased precise mobile geolocation from a data broker were able to track consumers over time and, as a result, identify several consumers, including military officials, law enforcement officers, and others. One person the journalists were able to identify by name (and who confirmed her identity) was tracked attending a prayer service at a church.

Kochava Causes Substantial Injury to Consumers by Invading Consumers' Privacy

88. Kochava collects, discloses, and uses sensitive information about consumers that invades consumers' privacy. Kochava obtains this sensitive or private data from a myriad of sources. The data Kochava collects, uses, and discloses provides a comprehensive picture of consumers' private lives, both online and offline, which cannot be obtained through physical observation in public spaces. It provides an unprecedented view into a consumer's personal actions, decisions, and behaviors. Kochava's practices intrude into the most private areas of consumers' lives and cause or are likely to cause substantial injury to consumers.

89. For example, Kochava discloses such sensitive characteristics as gender identity, medical conditions, ethnicity, and religious activity. Kochava also discloses information that

exposes aspects of a consumer's life that are private and sensitive, including, as an example, information about a consumer's family. As alleged above, Kochava discloses a consumer's marital status, number of children, and even whether those children may have special needs.

90. Kochava also collects and discloses, without consumers' knowledge, profiles of consumers' activities on mobile apps, including apps related to women's health, the LGBTQ+ community, and medical conditions. Such information includes the amount of time a consumer is on an app, what actions the consumer takes, and even the amount of money spent on the app.

91. Kochava's disclosure of precise geolocation data also reveals sensitive information about consumers, including visits to sensitive locations such as reproductive health clinics and places of worship. Such tracking is central to Kochava's and its customers' use of the geolocation data. Kochava uses records of consumers' precise geolocation over time to categorize consumers into audience segments and then sell lists of consumers to others with promises that the details revealed by consumers' movements will assist the third parties to identify and target individual consumers.

92. Kochava not only discloses sensitive information about consumers, it also uses this information to allow third parties to easily target consumers. Kochava and its customers create, sell, and use audience segments that target consumers based on sensitive characteristics, including gender identity, ethnicity, religion, political activity, medical issues, and visits to sensitive locations.

93. For example, in addition to Kochava's own uses, a customer that has purchased location data from Kochava in turn also sells its own audience segments. One such segment is "New Parents/Expecting," which it has characterized as identifying consumers "attending

Lamaze, birthing, breastfeeding, new parent support groups, etc. events." Another audience segment sold by the same customer is "Likely Republican Voter," which the customer identified as being based on consumers' visits to "Republican focused political events and events and venues affiliated with conservative topics."

94. Kochava's invasion of privacy affects millions of consumers. Kochava's Database Graph alone exposes the information of over 300 million US consumers. As another example, Kochava's "Expecting Parents" audience segment includes over 11 million MAIDs. And as also alleged above, Kochava directly ties a MAID to a consumer's name and other demographic, location, or identifying information, such as an email address, through its "360-degree perspective."

95. The sensitivity of this data is also high. For example, as noted, Kochava tracks women's uses of apps relating to pregnancy, ovulation, and menstruation in order to, among other things, target women who are pregnant or are considering becoming pregnant. Issues relating to pregnancy, ovulation, and menstruation are highly personal, private, and sensitive. Kochava, however, sells this information to third parties—third parties which the consumer has never heard about or interacted with—and, indeed, advertises that customers can use this data to identify and target consumers.

96. Kochava's collection, disclosure, and use of sensitive information that identifies highly sensitive and personal information about consumers, including consumers' health conditions, gender identity, religious practices, political activities, app usage, and visits to sensitive locations is a substantial injury to consumers' privacy rights.

Kochava Causes or Is Likely to Cause Consumers to Suffer from Stigma, Discrimination, Physical Violence, Emotional Distress, and Other Harms

97. In addition to invading consumers' privacy, Kochava's practices cause or are likely to cause other forms of injury to consumers, including stigma, discrimination, physical violence, emotional distress, and other harms.

98. For example, through Kochava's precise geolocation data, Kochava's customers are able to target consumers who have visited sensitive locations, exposing the consumers to these additional injuries.

99. Moreover, the likelihood of such injuries is exacerbated by Kochava's lack of controls surrounding who accesses this data, and how those entities use it. Indeed, as alleged above, Kochava provided consumers' precise geolocation data to a customer even though the customer provided minimal information to the company.

100. As alleged above, data associated with MAIDs is not anonymous. Using Kochava's data, identifying consumers by name or other identifying information is easy, whether through tracking their movements through Kochava's precise geolocation data or through other Kochava data, like its Database Graph.

101. In fact, identifying and targeting based on precise geolocation collected from mobile devices has and does occur. For example, as alleged above, a Catholic priest was outed and forced to resign his position based on location data that was collected from his mobile device and then sold to a group who used it to track priests' movements. In addition to precise geolocation data, the group that outed the Catholic priest also identified the priest as using the

Grindr app, an app associated with the LGTBQ+ community, through data obtained from a data broker.

102. Kochava's audience segments, including the ones that identify consumers based on sensitive characteristics, are also associated with MAIDs. As alleged above, Kochava connects such MAIDs to individual consumers. Thus, Kochava sells data that associates individual consumers to health conditions, gender identity and sexual orientation, political activity, and religious practices, among other sensitive characteristics, which puts individuals at significant risk of stigma, discrimination, physical violence, emotional distress, and other harms.

103. Even without using Kochava's data to connect a MAID to a consumer's name, email address, phone number, or other identifying information, the MAID itself is used to target consumers based on a particular interest or characteristic. MAIDs are unique personal identifiers that advertisers and advertising platforms use to identify a device to send a targeted advertisement. Indeed, targeting individual consumers is the MAIDs' primary purpose and MAIDs may be used to harm consumers.

104. Such targeting and harm occur in the data marketplace. For example, the Massachusetts Attorney General brought a law enforcement action in 2018 against a data broker that sent targeted advertisements about abortion and alternatives to abortion to the broker's "abortion-minded women" audience segment using consumers' MAIDs. The "abortion-minded women" audience segment was identified as consumers who, according to their precise geolocation, were "close to or entered the waiting rooms of women's reproductive health clinics." The data broker collected these consumers' MAIDs and used them to serve the consumers the targeted ads.

105. As another example, another group advertised the ability to reach "abortion-vulnerable women" by capturing "the cell phone IDs [i.e. MAIDs] of women coming and going from Planned Parenthood and similar locations and then serve them life-affirming ads" online using those MAIDs, including on their Facebook, Instagram, and other social media feeds. According to news reports, one such ad read, "Took the first pill at the clinic? It may not be too late to save your pregnancy." According to the reports, the ads pointed consumers to websites that attempted to persuade consumers to attempt a scientifically unsupported "abortion reversal" procedure. The group further alarmingly asserted on its website that its product "takes the guesswork out of the marketing equation" because its customers will "no longer have to wonder if women can find *you*. Now, you'll find *them*!" These ads served by the group were seen 14.3 million times.

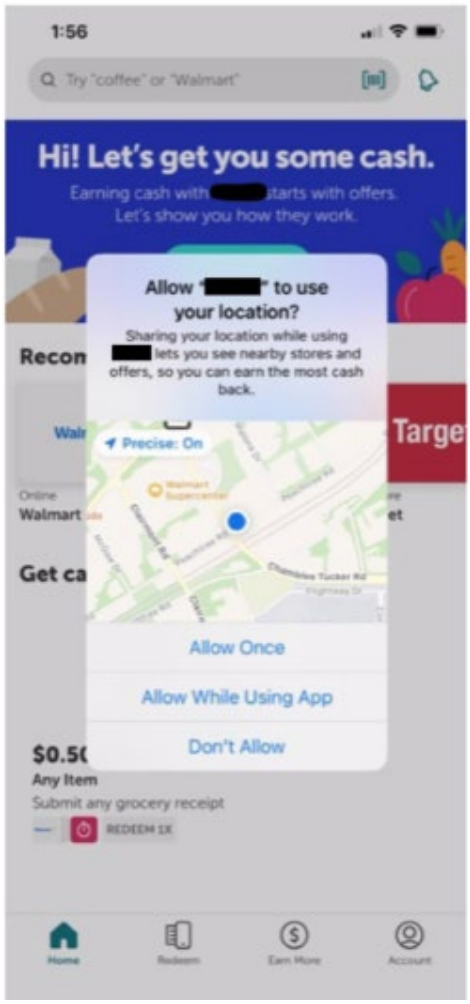
106. The data products sold by Kochava, including consumers' precise geolocation data, are used by Kochava's customers to identify and target consumers based on sensitive characteristics and cause or are likely to cause substantial injury in the form of stigma, discrimination, physical violence, emotional distress, and other harms.

The Substantial Injury Caused by Kochava's Actions Is Not Reasonably Avoidable by Consumers or Outweighed by Countervailing Benefits

107. The collection and use of data collected from their mobile devices and other online sources are opaque to consumers, who typically do not know who has collected their data or how it is being used. To the extent that consumers are even given a chance to opt in to a particular collection of information, such opt-in processes typically do not explain to the consumer that Kochava will receive the data, use it to classify the consumer based on sensitive

characteristics, and disclose such information to additional third parties unknown to the consumer. Indeed, in many instances, consumers believe or are told they are opting in to data collection for wholly different purposes.

108. For example, this is a consent screen that Kochava provided to a prospective customer showing what a consumer sees when a particular app requests access to their phone's location data:



In this consent screen, the consumer is lured in with the message "Let's get you some cash" and is told they should share their location to "see nearby stores and offers, so you can earn the most

cash back." This is not a Kochava app, nor is Kochava mentioned anywhere on the consent screen.

109. Nothing in this consent screen informs the consumer that their location data will be collected by Kochava, which will then sell it to others or put it to myriad other uses to generate revenue for Kochava.

110. Indeed, once information is collected about consumers from their mobile devices or other sources, the information can be and, in many instances, is provided multiple times to companies that consumers have never heard of and never interacted with. Consumers have no insight into how this data is used – they do not, for example, typically know or understand that the information collected about them can be used to track and map their past movements and that inferences about them and their behaviors will be drawn from this information. Consumers are therefore unable to take reasonable steps to avoid the above-described injuries.

111. These injuries are exacerbated by the fact that Kochava lacks any meaningful controls protecting consumers' privacy. Kochava could implement safeguards to protect consumer privacy, such as blacklisting sensitive locations from its data feeds or removing sensitive characteristics from its data. Such safeguards could be implemented at a reasonable cost and expenditure of resources. However, far from protecting consumers' privacy, Kochava actively promotes its data as a means to evade consumers' privacy choices. Thus, the harms described above are not outweighed by countervailing benefits to consumers or competition.

* * *

112. Based on the facts and violations of law alleged in this Complaint, the FTC has reason to believe that Defendant is violating or is about to violate laws enforced by the Commission.

VIOLATIONS OF THE FTC ACT

113. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

114. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Count I

Unfair Use and Sale of Sensitive Data

115. In numerous instances, Defendant has used and disclosed data gathered from consumers' mobile devices and other sources, including precise geolocation data, app usage, and personally-identifying information, that reveals sensitive and private information about consumers.

116. Defendant's actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition.

117. Therefore, Defendant's acts or practices as set forth in Paragraph 115 constitute unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45(a), (n).

CONSUMER INJURY

118. Consumers are suffering, have suffered, and will continue to suffer substantial injury as a result of Defendant's violations of the FTC Act. Absent injunctive relief by this Court, Defendant is likely to continue to injure consumers and harm the public interest.

PRAYER FOR RELIEF

Wherefore, Plaintiff requests that the Court:

A. Enter a permanent injunction to prevent future violations of the FTC Act by Defendant; and

B. Award any additional relief as the Court determines to be just and proper.

Respectfully submitted,

Dated: June 5, 2023

/s Brian Shull

BRIAN SHULL, IL Bar No. 6293797
JULIA A. HORWITZ, DC Bar No. 1018561
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
Phone: (202) 326-3734
Fax: (202) 326-3062
bshull@ftc.gov
jhorwitz@ftc.gov

ELIZABETH C. SCOTT, IL Bar No. 6278075
Federal Trade Commission
230 S. Dearborn St., Ste. 3030
Chicago, IL 60604
Phone: (312) 960-5609
Fax: (312) 960-5600
escott@ftc.gov

Attorneys for Plaintiff
FEDERAL TRADE COMMISSION

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served on counsel of record by email on June 5, 2023.

/s/ Brian Shull

BRIAN SHULL
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Phone: (202) 326-3734
Fax: (202) 326-3062
bshull@ftc.gov

Counsel for Plaintiff