Responses from companies

We reached out to all 47 companies mentioned in our story, “There’s a Multibillion-Dollar Market for the Location Data on Your Phone.” We received 12 responses, which we are including below. The emailed statements have been lightly edited, and for those who agreed to an interview, we are including selected quotes.

Acxiom

Sept. 14, 2021
Matt Ramsey, Senior Public Relations and Communications Specialist

Acxiom exclusively utilizes data that has been ethically sourced. We have long had a comprehensive data governance program – continually advanced – to use data responsibly, allow consumers to opt-out of marketing products at any time, and to protect personal information. As part of that process, we credential our data suppliers so that we understand who they are, that their data is collected properly, and that they have the right to share information with Acxiom and our clients. Our program also involves privacy impact assessments to ensure the data Acxiom and its clients use is always legal, transparent, fair and just; we hold our clients and partners to the same high standards of privacy and ethics that Acxiom continually maintains.

Acxiom does not collect or license movement data in the U.S., and no location data is used at the personally identifiable level. The data Acxiom licenses to brands is classified as non-sensitive – marketing data from publicly available information and trusted sources. Any location data is limited to insights related to visits to commercial locations such as grocery stores and car dealerships in order to provide relevant offers. Acxiom does not allow organizations or individuals to look up specific individuals. Further, this non-sensitive information comes to us from vetted, independent data providers in a pseudonymous state, meaning it does not include natural personal information like name or address. We use this pseudonymous data to create audiences of people likely to share common interests and characteristics (e.g., "probable coffee drinker”), which helps reputable brands and organizations better understand their current and potential customers by allowing them to ensure the marketing they send to people is more respectful and relevant, not random or intrusive.

We strongly believe in transparency, accountability and consumer control, and we take the safety and security of the individuals and the data we maintain about them very seriously.

Adsquare

Sept. 14, 2021
Christoph Herwig, VP Marketing

Adsquare is not a location data broker
Adsquare does not resell data in a raw format to third parties
Adsquare is an audience & location intelligence company analysing data and providing statistical outputs
Adsquare operates a platform that is used by businesses to plan, target and measure their advertising campaigns
Important to understand: Data quality and consent are paramount in our location panel. It's not about absolute numbers and scale, it's about a statistically relevant quantity to achieve representative results, e.g. uplift metrics or an indexing for locations

Adsquare doesn’t collect location data
Adsquare sources and aggregates location data from a variety of suppliers
The location data obtained has the explicit user consent for such data to be shared with Adsquare as a named recipient

Adsquare is always explicitly named as a recipient of such data and also names all of its recipients openly as part of our Privacy Policy and linked Partner List
Adsquare describes its purposes very concretely on the basis of the IAB Transparency and Consent Framework 2.0

Adsquare does not operate an SDK and Adsquare does not collect location data

Adsquare does not offer location data for sale on any platform
Adsquare is not listed on Alternative Data Group and does not have a business relationship with that organisation

Adsquare may be listed on Datarade, as it turns out now, but the Adsquare profile has not been written, posted, reviewed or approved by us. The website appears to be some sort of meta search platform. We don’t have a business relationship with Datarade either. It seems as if the company only wants to make their offering look good (by listing many organisations) in order to appear relevant. We will get in touch with them to correct this.

Adsquare does not “offer access to consumer location data”, there is no option for advertising clients to download datasets or get access to any personal data or location signals

Adsquare's solutions for Measurement and Out of Home are either based on aggregated and anonymized data sets or pure geo-contextual analysis without the use of any personal data. The collection of mobile location data requires the highest standards in terms of privacy and security. Unlike other companies in the market, Adsquare does not source any data from public sources such as RTB exchange traffic from the bid stream (although Adsquare might technically have consent via the bid stream we do not leverage this source due to missing direct privacy agreements with publishers). Adsquare only works with SDK derived signals with explicit consent from the data subject sourced from companies and publishers that went through a rigorous screening process and that we have strict privacy agreements with to make sure that e.g. consent is obtained correctly and Adsquare is named as a recipient etc..

Adsquare draws movement data from SDK technology companies and a wide variety of location-enabled apps including transportation, weather or social apps. The movement panel consists of a representative cross-section of the society in terms of socio- demographic characteristics.

As previously mentioned, Adsquare sources and aggregates location data from a variety of suppliers. The location data obtained has the explicit user consent for such data to be shared with Adsquare as a named recipient. Adsquare does not offer access to consumer location data, there is no option for advertising clients to download datasets or get access to any personal data or location signals.
Adsquare is an audience & location intelligence company analysing data and providing statistical outputs.

When analysing location data, it's not about absolute numbers, e.g. with regards to footfall measurement, it's about understanding the success of a campaign by analysing a statistically relevant sample size and comparing it to a baseline of activity.

Customers don't "use" our location data as they don't have access to our data. Again, Adsquare does not share location data with third parties. Adsquare uses location data for analytical purposes and the result is comparative values or index values on a spatial level.
Location data is anonymised and not tied to consumer identities. Adsquare does not de-anonymize location data and does not work with third parties (e.g. identity solution vendors) to do so.

As mentioned above, there are many apps with a location use case, e.g. a weather app, where a considerate proportion of users is happy for location signals to be shared.

With existing clients, Adsquare is fully transparent about our supply partners. The list of our suppliers is deliberately not disclosed to the public. The partnerships represent a competitive advantage for us. But that is not the point. What is important is that our partners and the app publishers have a consent mechanism in place according to the regulations and that they name Adsquare as a partner, and that is the case.

Adsquare ensures compliance with data privacy regulations by our partners through an own due diligence process, contractual paperwork and regular audits.
Detailed RFI is shared to understand data sourcing methodologies and legal basis.
Apps are downloaded to understand consent mechanisms in place.
Adsquare's data partners are contractually obliged to adhere to all local data privacy legislations incl. detailed opt-in and transparency requirements in a separate "Data Privacy Addendum".
Purposes for data licensing are based on IAB TCF 2.0.
Regular check of consent mechanisms from an end user's point of view.

Adsquare's suppliers have to list Adsquare as a recipient of their data.
Adsquare describes the opt out process in detail in its privacy policy. Users can enter their Mobile Advertising ID for Adsquare to delete all associated records.
Furthermore, the app publishers ask whether and which data may be collected after download and list all partners with whom it is shared. With the new update from Apple and the introduction of ATT, the consent is now already collected by the OS providing an additional step towards more transparency and more informed decisions by end users.

Final remarks:

Legislators, operating systems, app developers and third parties set clear guidelines that ensure data protection. Adsquare not only adheres to these guidelines, but also helps to shape them in cooperation with independent organisations. Furthermore, every user is responsible and able to allow ad tracking or not. There are people who willingly share their data in order to benefit from certain functionality or in order to receive personalised advertising.
Adsquare is fully committed to providing privacy-friendly advertising technology as summarized below. We believe a privacy-first approach to digital advertising is a positive step, for both consumers and the industry.

Adsquare was founded in Europe and respected data privacy even before GDPR came into play.
Adsquare only collects data from partners with explicit consent from end users for this data to be shared.
Adsquare offers planning, targeting and measurement solutions that are based on a focused methodology that prioritises accuracy over volume – certified by independent bodies.
Adsquare's Proximity Targeting allows you to target the right local context of users without relying on any online identifiers.
Adsquare invested into new innovative products, e.g. with "Audiences in Motion" we combine location context with audience index scores, actionable on a spatial level - again without sharing personal data as an output with any party.

Advan Research

Sept. 13, 2021
Yiannis Tsiounis, CEO

We are not a data broker, we do not have nor power an SDK, we do not collect data ourselves, and we do not sell raw location data directly nor through marketplaces. We purchase data from data brokers, i.e., are consumers of that data, and of course we require our suppliers to guarantee explicit opt-in from every user.

“How many people out of the millions of downloaded applications actually read the privacy policy? Even if it says on the first line we collect the location data, which most of the applications do these days. People accept it.”

“We buy data directly or indirectly from aggregators from a couple of thousand applications.”

“What we provide is just aggregated metrics – what you would get if you would sit outside a Walmart with a people counter every day for the last five years, we will just give it to you”

“We don't have a product off the shelf that you can buy and generate data on the device level basis – other people have. We don't specifically because it opens up a can of worms.”

“There's the 80/20 rule: 80% of your data comes from 20% of your sources. So we do know some of the largest applications, but there's a tail of small applications, maybe 1,000 apps at any given time and have 5-10,000 users. We don't necessarily know all of them. And don’t particularly care.”

“So the apps that have a legitimate need to collect this kind of data, where the end user has reason to allow them to collect the data at all times are apps that give you weather alerts, Walking around, driving around...Apps that will give you coupons. I want cheap gas as I'm driving around, so you need to know where I am…. They give you directions. So these are the types of applications that typically tend to provide this data.”

“We do know some of the applications and we also know the largest applications we've tested, we've downloaded the application to see what the user sees and what the and that the user can turn things off.”

“There's only so much you can squeeze into the notification message. You get one line, right? So you can’t say all of that in the notification message. So they word it differently every time. You only get to explain to the user ‘I need your location data for X. Y. Z.’”

“I would say three layers of businesses in the marketplace:
There are the smartphone applications that collect the data.

Then there are the data aggregators that collect the data from multiple applications and sell in bulk. And then there are analytics companies which buy data either from aggregators or from applications and perform the analytics. And everybody sells to everybody else."

"For example, we know that the average income in this neighborhood by census data is $50,000. But then there are two devices. One went to Dollar General and McDonald's and Wal Mart and the other one went to a BMW dealer and Tiffany's...So they probably make more money."

Amass Insights

Sept. 14, 2021
Jordan Hauer, CEO

"We've identified over 16,000 data providers at this point. We have a pretty in depth taxonomy on how we categorize all those providers. So for example, I took a look and we had 320 location data providers."

"The most inefficient part of the whole whole process is actually not delivering the data. It's actually finding what you're looking for and making sure that it's compliant, making sure that it has value and that is exactly what the provider says it is."

"We're open to working with any different type of company or individual. You know we've been approached by entrepreneurs that are trying to start a new data provider business and need to source data. That's been a new area of growth for us actually."

Amazon

Sept. 22, 2021
Claude Shy, Account Supervisor

To become a data provider on AWS Data Exchange, data providers must agree to the Terms and Conditions for AWS Marketplace Providers ("AWS Marketplace Terms & Conditions"). Data providers must use a valid legal entity domiciled in the United States or a member state of the EU, supply valid banking and taxation identification, and be qualified by the AWS Data Exchange business operations team. Each data provider will also undergo a detailed review by the AWS Data Exchange team prior to being granted permission to list data products on the catalog.

As mentioned, data providers must use a valid legal entity domiciled in the United States or a member state of the EU, supply valid banking and taxation identification, and be qualified by the AWS Data Exchange business operations team. Each data provider will also undergo a detailed review by the AWS Data Exchange team prior to being granted permission to list data products on the catalog.

AWS is setting the standard for privacy and security in the data marketplace. Only qualified data providers will have access to the AWS Data Exchange. Potential data providers are put through a rigorous application process. Data providers looking to exchange PII/PHI will have to be accepted into the Extended Provider Program. Providers in this tier are vetted even more carefully and undergo a significantly more in-depth review, including confirming and explaining how they gain consent from individuals, how they monitor their customers' use of data, and what their formal process is to handle opt-out requests.

Cuebiq

Sept. 9, 2021
Bill Daddi, Spokesperson

Cuebiq sources data exclusively through direct app integrations. Each partner app clearly presents to its end users a named consent, separate from the operative system location consent, where the user is informed about the partnership with Cuebiq and the specific use cases Cuebiq will use the data for and is asked consent to share data with Cuebiq and Its Partners.

In the same upfront consent window the user can click on a link and visit the privacy center of Cuebiq where they can find additional information on Cuebiq and its use cases. In the same consent the user can click on a link to get to a list of Cuebiq's trusted partners with whom we may be sharing some derivative data with. It is all extremely transparent and the opt-in rates clearly confirm that the users are fully aware of what is happening because the opt-in rates can be as low as less than 20%, depending on the app.

Users who visit the privacy center of Cuebiq can easily find in a short, simple and understandable format information on how to opt-out from Cuebiq and on how to exercise their data rights such as accessing the data collected by Cuebiq or demanding a full erasure of all data.

We do not publicly release a list of our partner apps for competitive reasons. The end users of any app working with Cuebiq though will know that Cuebiq is a partner of the app and will receive the consent window above, that is what matters.

We do not release a public list of all our clients and partners for the same competitive reasons. A list of trusted partners whom we can have a derivative data sharing with is public and published on our website.

The accuracy of the location data is checked by detecting anomalies, such as outliers in terms of visits to certain commercial venues, outliers in terms of distance traveled in a given time.

Also, our clients can validate the accuracy of our insights by looking at statistically significant correlation between aggregate data in terms of store visits that we provide with their own aggregate data in terms of sales. If our estimates of visits are accurate there will be correlation with their own aggregate sales first party data

We agree with the statement that location data, like any other dataset , can be potentially reverse-engineered to identify users by overlaying additional data. This is an overall problem of any category of data.

In the last decade we have seen a great development of a new set of technologies called "Privacy technologies" that are focused on truly anonymizing datasets.

Examples of these technologies include differential privacy techniques that add selectively noise to avoid identification, encryption of attributes such as IDs, federated learning that can enable to train AI models leveraging multiple datasets but without any access to the underlying data, data clean rooms where the data can be queried but not accessed and just privacy safe insights can be exported.

These technologies can enable privacy-safe open data ecosystems that are paramount to democratize access to data and to fuel equitable, unbiased AI innovations across thousands of organizations , all of that in a privacy safe way.

Without similar ecosystems, a few big tech players will have exclusive access to data and will dictate all AI innovation, with clear risks in terms of accountability and fairness.

Cuebiq has been a leader in applying these techniques in the geospatial sector, we significantly invested in many of the above technologies and developed patent-pending privacy tech solutions that are at the core of our mission to create a privacy-safe open data ecosystem for mobility analytics.

An example of privacy tech that we apply is represented by differential privacy algorithms that will process the data points that are in residential areas to aggregate them to a granularity level that will contain thousands of residents.

Foursquare

Sept. 9, 2021
Ashley Dawkins, VP of Communications

Foursquare receives location data from a few types of sources: owned and operated applications, apps that use our location tools (when the app developer permits us to use such data), and carefully vetted suppliers. We collect, use, share, and/or store data in compliance with applicable laws, and we always mandate our partners to collect consent. Beyond simply collecting required consent in our Foursquare apps, we are careful to use direct and transparent language explaining how we use the data that is collected, and our sharing practices. We only collect data where required consent has been given.

Our data supports products that help many of the world's largest enterprises and advertisers (including quick-service restaurant brands, travel and hospitality brands, retailers, etc.) reach consumers with relevant advertisements, understand the effectiveness of their advertising, and analyze and visualize data to drive decisions (such as inventory planning, site selection, consumer app experience improvement, etc.).

Importantly, we do not sell location (i.e. GPS) data to government entities for national security, law enforcement, and other similar purposes. We believe such data sales should be banned and encouraged our industry associations, the IAB and NAI, to endorse Senator Wyden's bill on this matter (The 4th Amendment is Not for Sale Act), which they did.

We do not claim that the location data we collect and use to build products is "anonymous." Such data is collected (with consent) in association with mobile ad identifiers (MAIDs), email addresses, or hashed email addresses, and when companies refer to this data collection as anonymous, that is misleading. Most privacy laws also consider precise location data to be personal data or personal information, even without an identifier.

To protect user privacy, our products incorporate a number of privacy-protecting measures, such as never sharing raw location data, the hashing of identifiers, obfuscation of the exact visit time, the removal of inferred home and work visits from data deliveries, and policies governing the delivery of data at the category of business or chain level rather than the specific venue level. We also do not segment or persistently identify users on the basis of inferences about certain characteristics such as sensitive health conditions, religion, sexual preference, immigration status, or status as active-duty military personnel. Examples of sensitive places include specialty physicians offices, religious centers, women's shelters, military locations, and LGBTQ centers, among others.

Our owned and operated mobile apps - Swarm, CityGuide, and Rewards - provide a considerable portion of the data used to power our products and services. Additionally, we receive data from some of the apps that have integrated our SDK, as well as certain third-party data suppliers.

Our dataset is validated by our first-party data (users “checking-in” to businesses) and leverages our proprietary Places (POI) database, which both serve as a truth set for scoring and qualifying third-party data. We leverage this truth set to understand the accuracy of location signals coming from other apps. This allows us to vet and filter data. Filtering means we've removed poor quality, inaccurate data that our competitors don't remove. All data used in our product has been analyzed, cross-referenced, de-duped and validated so that only the most accurate location data is retained. This validation process, or feedback loop, is unique to Foursquare.

We believe that users have a right to know how and when their data is being collected and shared. As such, Foursquare collaborates with partners to implement direct and transparent language in their own apps, explaining how the location data that is collected is used. Partners are contractually prohibited from sharing data with Foursquare if the user has not provided the required consent. Foursquare also has a review process in place that regularly assesses the privacy practices of our developer and data supply partners.

Foursquare’s location data is always associated with Mobile Advertising Identifiers (MAIDs). If a person wants to opt-out, they can do so at https://foursquare.com/data-requests/, or within their settings in our owned and operated apps. Once they provide their MAID, Foursquare can delete the data. Foursquare honors opt-out of sale, access, and deletion requests from verified consumers globally, not just in jurisdictions where this is required by law, such as California.

A person can also use the DAA’s AppChoices tool to opt-out of the collection and use of mobile app data by Foursquare across apps over time on a device for interest-based advertising purposes (including cross-device linking for such purposes), and for ad delivery and reporting purposes To exercise this opt-out, a person can download the AppChoices app onto their mobile device and opt-out through the app.

We collaborate with all of our SDK partners to help ensure that they are implementing direct and transparent language in their own apps and public-facing privacy statements that explains how the location data that is collected is used. Additionally, partners are contractually prohibited from sharing data with Foursquare if the user has not provided consent required by law, self-regulatory guidelines, and/or app store terms and conditions. Foursquare also has a review process in place that regularly assesses the privacy practices of our developer partners.

Google

Sept. 17, 2021
Scott Westover, Google spokesperson

The Google Play team is always working to strengthen privacy protections through both product and policy improvements. When we find apps or SDK providers that violate our policies, we take action.

Mobilewalla

Sept. 14, 2021
Laurie Hood, Chief Marketing Officer

Mobilewalla provides data and insights to help organizations better understand and predict consumer behavior. Our solutions help businesses get more out of their AI investments by making their predictive modeling more effective.

Mobilewalla acquires data from various third parties in the digital ecosystem including publishers, demand side platforms (DSP), data management platforms (DMP) and data aggregators. We do not provide data in real-time. We are able to infer or derive device level behavioral and demographic characteristics by applying artificial intelligence techniques to our data set creating attributes and features. We do not have, nor do we provide, data that can be tied directly to an individual.

We take consumer privacy and consent seriously and as a steward of this data are compliant with all local, national and international regulations (such as CCPA and GDPR). We do not provide data for law or immigration enforcement or surveillance purposes.

Privacy and Consent Specific Practices

- Each Mobilewalla data partner must meet rigorous criteria and are required to represent and warrant things such as:
    - they have a consent and privacy framework and associated processes for active compliance
    - the data provided to us has been obtained lawfully and in compliance with the local regulations where the data was sourced
    - they have the legal right to sell and transfer the data to us

- they will electronically provide us with any requests from users that have communicated to them any of the following: opt out, data deletion, information requests, do not track (DNT), do not sell, consent withdrawals and any other similar user requests
- the partner clearly discloses in their privacy policy how the user's data will be processed, including that third parties will/may process their data, and that a user has a clear and easy way to communicate their consent and privacy requests to the partner both electronically or by written means

As well, we take the following additional steps:

- Our customers complete a data usage form as part of the contract process that outlines the use cases for the data they are sourcing from Mobilewalla to ensure data is being used appropriately
- We process opt outs received through our data partners, the Digital Advertising Association, opt-out request proxy companies as well as through direct submissions at multiple points in our processing to ensure that data is not used in compliance with regulations
- Our privacy policy is accessible from multiple places on our website as are links to our opt-out pages, we also accept opt-out requests by email and mail

---

Narrative

Sept. 13, 2021
Nick Jordan, CEO and Founder

"You know, from afar, we may look like a broker, but we're really just giving them the technology that lets them buy and sell the data."

"We take software and license it to the buyers and sellers of the data. So the buyers and sellers can work directly with each other as opposed to working through Narrative."

"It's not our data, we're not buying it, we're not selling it."

"It should be noted that not all of the data that goes into the platform is geolocation data…. Think of an event as a single row of data. Think of it as a timestamp and then some number of fields that represent an observation or a declaration of some kind."

“The participants in the platform are required to make sure that they're adhering to whatever local laws and regulations are required. We do give them tools that let them do things like anonymization to the extent that they're sending it to us and it's not anonymized as a best practice. We prefer that they do everything on their side before it comes into the platform.”

Placer.ai

Sept. 14, 2021
Ethan Chernofsky, VP Marketing Placer.ai

We have a very strong commitment to privacy and focus significant engineering resources to ensure we comply with the highest standards.

Based on the categories presented, we would fit into the following:

- A company that obtains location data originating from consumers’ mobile devices where it doesn’t have a direct relationship with the consumer whose data it’s obtaining
- A company whose marketing language offers app developers the use of an SDK in exchange for monetization or access to location data

We partner with mobile apps providing location services and receive anonymized aggregated data. Very critically, all data is anonymized and stripped of personal identifiers before it reaches us helping to ensure the standards set.

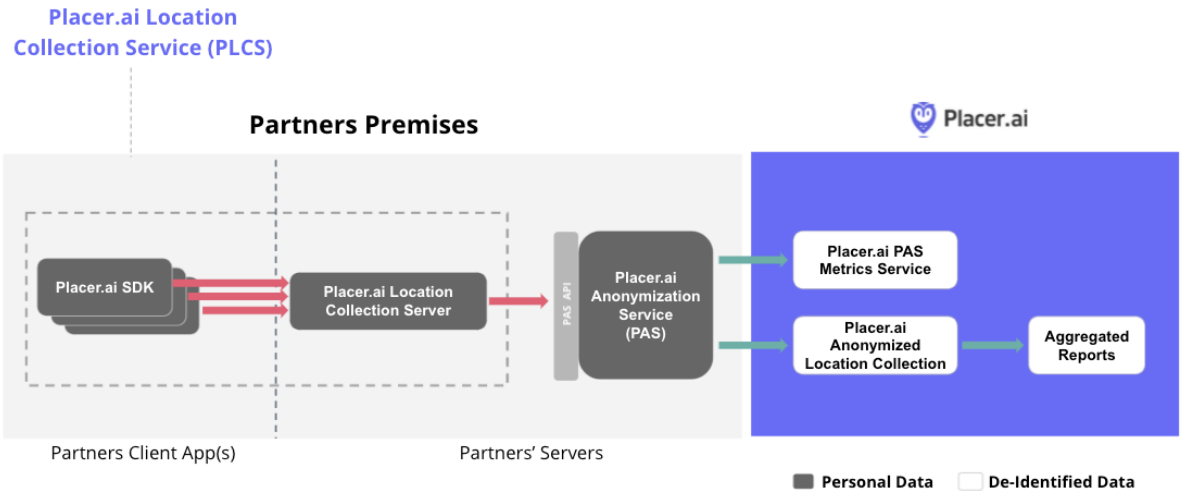
We also have a very thorough standard for our partners regarding consent and privacy criteria. This includes a requirement that users opt-in and can be easily removed if requested. Because of our technical privacy investments, we don’t know whose foot traffic contributed to the dataset. This is an especially important element for us as we look to create the technical limitations that will ensure an ongoing commitment to privacy.

As mentioned, a key element here is that we are not actually providing or selling the acquired data to anyone. We use the data as a panel to run AI and Machine Learning algorithms to make estimations on foot traffic patterns to Commercial Real Estate locations across the US. The information we provide our customers and users is based on these estimations, and not the data we aggregate. Regarding interaction with individuals, we don’t provide any data to customers, only the analysis and estimations, and this data is treated before we receive it so we are unable to identify individuals from the dataset.

In addition, we also always make sure that such derived estimations will be based on a minimum panel size of 50, regardless of how the user is attempting to slice and dice the data via the platform, thus preserving a K-anonymity of 50 at all times.

Regarding accuracy, we use a variety of mechanisms to measure the accuracy of our data including ‘source of truth’ data from customers and publicly available sources. This has enabled us to benchmark the estimations, and the market traction has been a strong validator of the quality and accuracy of our estimations.

We're including a simple architecture diagram here just to show where our technical privacy protections are located before we receive data and before we give customers access to our analysis. It’s a Privacy-by-Design architecture we developed in-house.



Reveal Mobile

Sept. 9, 2021
Dan Dillon, CMO

Reveal Mobile sells privacy-compliant data to agencies, retailers, media companies and brands.

Reveal Mobile does not collect, manage, market, or sell personally identifiable information (PII). We do not pair our data with any other data sets.

Reveal Mobile's data supply comes from people who have opted in to location services in the mobile apps they use.

A person can opt out of location services on their mobile device. If an app publisher registers an opted-out user, they pass that information to us to act on. We then pass the information forward, ensuring privacy compliance down the line. Reveal Mobile is CCPA compliant so a person can request that their data not be used or sold. Reveal Mobile honors all such requests.