Society | DOI:10.1145/3344291

Sarah Underwood

Can You Locate Your Location Data?

Smartphone apps offering location data services may be desirable, but their ability to collect personal data that can be sold to third parties is less attractive.

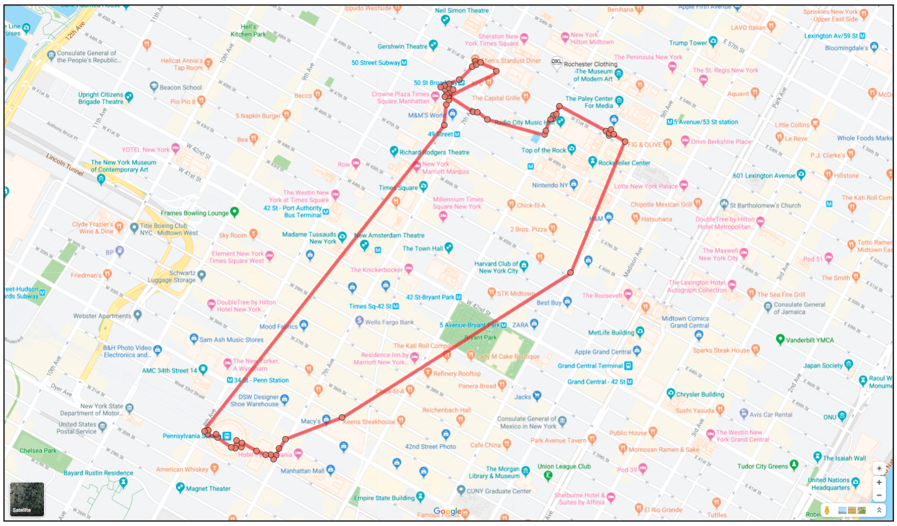
SHOPPING TRIP, SCHOOL pick-up, medical appointment, first date, divorce court, or something even more personal—whenever you carry a mobile device and wherever you take it, chances are data about your location is being collected.

Smartphone apps that are free to use on the basis that individuals find them desirable and therefore agree the apps can collect their location data seem to be reasonable, but exactly what data is collected, how it is used, and whether it is sold to third parties is a much bigger, darker picture that smartphone users are unlikely to see at first glance, and will only experience when their data is used for purposes far beyond their initial consent.

With a stringent data privacy law expected to be introduced in California in January 2020, increasing litigation on the potential misuse or abuse of personal location data, and rising public awareness that smartphone apps are not necessarily what they seem to be, location data has become a hot, contentious topic.

Frank Yoder, head of marketing at MightySignal, is a specialist in mobile app intelligence and the software development kits (SDKs) that are integrated in apps to perform anything from location data collection to in-app purchases and data monetization. Yoder says there are 43 location tracking SDKs for Apple iOS devices and 39 for Android devices. In total 6,725 apps run these SDKs.

MightySignal does not touch data or track location data per se, instead operating an SDK intelligence platform that continuously monitors apps and which SDKs they are installing or uninstalling, for reasons such as how well the SDK integrates with the app or whether there are better apps in the market using different SDKs. The company's customers are mostly SDK providers tracking their competitors and looking for opportunities as app providers change their SDK technology stacks.



One's location history often amounts to leaving a digital trail that is easily captured via smartphone apps.

MAP DATA ©2019 GOOGLE

SDK developers include Foursquare, which recently acquired Placed from Snap, parent of Snapchat, as well as Cuebiq, GroundTruth, and Factual. SDK developers also collect data and provide commercial location data services to help clients drive smarter digital products for better marketing and business decisions.

Cuebiq, by way of example, collects anonymous data from mobile devices when users download one of its partner apps and opt in to the app's location services. The company partners on more than 220 mobile apps that include the proprietary Cuebiq SDK. Valentina Marastoni-Bieser, executive vice president of marketing at Cuebiq, says the opt-in process is straightforward and explicit. When a user signs up for one of Cuebiq's partner apps, a prompt appears on their device to opt in to the app's location services. When users opt in, Cuebiq collects their data anonymously; they have the option to opt out at any time.

The resulting data is aggregated and analyzed for high-level, macro visitation trends, meaning the data collected does not contain any personally identifiable information. Brands and advertisers can access insights derived from Cuebiq's data using its artificial intelligence-driven business intelligence platform, Clara, which helps them map and measure offline customer trends, and shape strategic business decisions such as when to do promotions or where to build new locations. Its typical client sectors include quick service (or fast food) restaurants (QSRs), retailers, financial services, and automotive businesses.

Snap collects location data through its Snapchat app. It does not sell the data, but does use it for its own commercial purposes, such as location-based ad targeting and provision of services such as geofilters that allow mobile users to add a location illustration to their 'snaps', and Snap Map, which lets users share their location with friends on a map. This is turned off by default and can be switched on and off at any time. Rather than selling data services, Snapchat allows brands to advertise to its audience through a mixture of in-app advertising formats such as Snap ads and commercials.

Keen on data privacy, Snap's privacy policy states: "When you use our services, we may collect information about your location. With your permission, we may also collect information about your precise location using methods that include GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compasses."

Users must give device-level permission for location data to be collected by the Snapchat app. Prior to Snapchat collecting location data from users, it requires express consent through an in-app location consent pop-up. Users can opt out of location data collection and location sharing at any time, and they can delete most of their stored data at any time in the 'setting' tab of the app. Under GDPR, European Union users also have the 'right to object' to Snapchat's use of their information.

Policies like these are used by most app publishers, but for personal location data to have become such a controversial and touchy topic, something else must be going on under the hood.

A recent study by online security start-up vpnMentor, set up by ex-Google marketer Ariel Hochstadt, reviewed the privacy policies of some of the most popular apps to discover how they really track individuals' every move. In terms of location, the study reports that apps such as Tinder continue to track your location when the app is not in use. Facebook and Instagram not only track your location, but also save your home address and most commonly visited locations.

Anonymity, often proclaimed by location data collectors and providers, can raise similar unforeseen issues for smartphone users. While some applications of location data, such as those in financial services, have no interest in individual profiles and offer broader economic information, data collected by many apps is not truly anonymous. Personal identifiers such as names can be removed from the data, but the data may also include elements tied to individuals, such as a device service number or IP address. If these elements are not eliminated, they can be used to recreate profiles that may not have a name but are not anonymous.

Serge Egelman, research director of the Usable Security & Privacy Group at the International Computer Science Institute (ICSI) and a member of the department of electrical engineering and computer sciences at the University of California, Berkeley, says the biggest issues around personal location data are that consumers do not necessarily have an indication of when their data is being collected, and also have a poor understanding of how that data is used.

Egelman cites reports earlier this year of law enforcement gaining access to Google's mobile location history database, known internally as Sensorvault, using 'geofence' warrants that specify a geographic area and time period. Google gathers information from the database about devices meeting the warrant criteria and initially labels them with anonymous identity numbers. Detectives look at locations and movement patterns to see if any appear relevant to their investigation and, if so, ask Google for names and other sensitive information. Such situations are helpful to law enforcement, but constitute an abusive use of personal data for those in the geofence area who are identified but have done no wrong.

Of course, individuals have to give Google permission to collect their data, which they usually do, even though they don't necessarily know the details of the data that is collected and thatit is kept for an indefinite period. As Egelman says, "You wouldn't expect to be implicated in a crime just by using a Google service; that's scary. How can people control this kind of thing when they don't know what it is?"

Data collected by many apps is not truly anonymous. Personal identifiers can be removed from the data, but the data may include elements tied to individuals.

While both the iOS and Android platforms have permissioning systems that come into play when an app tries to access location data and respond to user decisions on whether they want location data turned on or off, Egelman says the problem is that there is no real context. When the users say 'yes' to location data, they don't know whether this is more desirable for the user or for the app tracking the user. The first time the user clicks the button for data, the data may be desirable, perhaps pointing to shops nearby. Once the button is clicked, however, these platforms use that permission in perpetuity, and that use could be for something that is not desirable to the user.

There is also the issue of apps that collect data with consent from their users, and sell it to third-party advertisers without the consent of users. This problem is manifested in an ongoing legal dispute that started early this year between the Los Angeles city attorney and The Weather Channel app, a subsidiary of IBM. The lawsuit claims the app did not adequately disclose to users how their location information would be used, and calls The Weather Company's practices 'fraudulent and deceptive', saying they violate California's Unfair Competition Law. The lawsuit explains that after downloading the app, users are prompted to allow it to access their location data, but how that data will be shared, or sold, is not noted.

"The permission prompt also fails to reference or link to any other source containing more detailed information about what users' geolocation information will be used for," states the lawsuit. The app's privacy policy does note that data could be used for targeted advertising and might be shared with partners, but the attorney argues that users have no reason to look at the policy, as the prompt does not suggest their data will be used in these ways.

Los Angeles city attorney Michael Feuer told *The New York Times*, "If the price of getting a weather report is going to be the sacrifice of your most personal information about where you spend your time day and night, you sure as heck ought to be told clearly in advance." This is not a one-off problem, nor one with an easy solution. As Egelman asks, "How can you make a decision about how data is used, when it is sold on?"

Egelman's research team has been examining how mobile apps access sensitive data, and recently commercialized a search engine called AppCensus (https://search.appcensus.io/) that looks up the privacy behaviors of free apps (it is still free for consumers). The platform acted as a test bed for research into the behavior of 6,000 free Android children's apps. The team reported that more than half the apps shared details with third-party companies that may have violated the Children's Online Privacy Protection Act (COPPA), which provides digital privacy protections (including for location data) for children under 13.

While location data made its name in advertising, initially by the likes of Facebook, Google, and Twitter, it has since become key to sectors such as financial investment, where firms are looking for new ways to find investment returns that exceed a market index or benchmark. Providers of location data services (or alternative (alt) data, as it is known in this heavily regulated sector) are scrupulous about data privacy, do not use personal data for compliance reasons, and only use alt data to demonstrate trends. They are, however, very knowledgeable about its promises and failures.

Abraham Thomas, chief data officer at Quandl, a provider of insights from alternative data, recalled, "Twenty years ago, Wall Street investment firms sent junior analysts to malls at the weekend to count cars; if there were a lot of cars, the economy was booming. If there weren't, it was in recession."

Technology can now track retail customer activity in near-real-time across the entire country, covering every mall and every store. However, as Thomas points out, to be useful, location data needs to be accurate in every sector. Problems here include the vast number of smartphones in the world, poor GPS signals, and cellular coverage that is limited by thick walls and sends truncated location data that adds bias to the data.

New York City-based Thasos Group also provides what it calls 'actionable information from real-time location data' for investment firms, and publishes an annual Retail REIT (Real Estate Investment Trust) performance update. Thasos co-founder and chief product officer John Collins says the company licenses location data from app aggregators, primarily SDK providers and sometimes brokers.

> **"This is a market failure based on data asymmetry. Consumers don't have enough information, and those that could provide [it] choose not to."**

Thasos products are built on location data collected with user consent and sold on an anonymous basis. The company insists, like Snap, that apps must include secondary consent disclosure, which mean the app will collect location data among other data, use the data for a variety of purposes, monetize the data by selling it on an anonymous basis, and allow users to opt out of the process by turning off location services.

This plays into the requirements of the forthcoming California Consumer Privacy Act (CCPA) that will give residents of California extended rights around their personal data. Specifically, they will be able to:

- know what personal information is being collected about them;
- access that information;
- know if their personal information is disclosed, and if so to whom; and
- know if their personal information is sold, and have the right to opt out of the sale.

The legislation extends beyond existing U.S. data privacy laws, although the rights it bestows are not as prescriptive as those of the European Union's General Data Protection Regulation (GDPR), which took effect in May 2018.

As well as improving data privacy, CCPA raises questions about users having to turn off many of their apps if they don't want to share their location data. Collins suggests few apps, mainly weather and navigation apps, actually require location data to function, and that a number of apps that collect location data have stopped selling the data. According to Collins, "It is better for apps to keep their user base than require secondary disclosure. Where location data is not strictly needed by an app, users can still use its core functionality."

With the implementation of the California privacy law just months away, attorneys are lobbying legislators about a federal law, which is almost certain to follow. It is unclear how the federal government will act, but any legislation is expected to be less onerous in terms of personal consent requirements than the California law.

Meantime, Egelman concludes, "This is a market failure based on data asymmetry. Consumers don't have enough information, and those that could provide the information choose not to. This discrepancy is coming to a head right now. We need more regulation."

Further Reading

California Consumer Privacy Act
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

General Data Protection Regulation
https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

Won't Somebody Think of the Children? - Examining COPPA Compliance at Scale, Berkeley Laboratory for Usable and Experimental Security (BLUES), April 25, 2018,
http://bit.ly/2IkZpX0

Who's Watching You?, *vpnMentor*,
https://www.vpnmentor.com/research/whos-watching-you/#/

Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works, *The New York Times*, April 13, 2019
https://nyti.ms/2MVf9EF

L.A. is suing IBM for illegally gathering and selling user data through its Weather Channel app, *Los Angeles Times*, Jan. 4, 2019
https://lat.ms/2FfGxa2

Thasos 2019 Retail REIT Performance Update, Thasos Group
http://thasosgroup.com/blog/2019-retail-reit-performance-update/

Sarah Underwood is a technology writer based in London, U.K.

© 2019 ACM 0001-0782/19/9 $15.00