The security risks of smartphone location tracking

PRIVORO®

Everywhere they go, smartphones leave behind a trail of digital breadcrumbs that can potentially give threat actors important clues about where and how users live their lives. Because smartphone users have only limited control over location tracking and little insight into how their location data is ultimately used, those wanting high assurance of location privacy must look to solutions beyond the phone.

HOW A SMARTPHONE'S LOCATION IS TRACKED

While location tracking is effectively baked into cellular functionality, it's also a key driver of monetization within the app economy. Multiple radios and sensors contained within a smartphone play a role in generating accurate location data.

Cellular delivery
Cellular providers need to know where each mobile device on their network is located at all times in order to deliver calls, texts and data. To do so, the network performs triangulation based on the signal strengths observed by different towers to generate an approximate location for the phone. Typically, urban areas contain more cell towers and thus provide more accurate readings. These locations are logged by the provider via detailed, up-to-the-minute records.

Location-based apps
Through location services, a smartphone allows apps and websites to gather and use information based on current phone location to provide a variety of location-based services, from mapping to weather. Location services can enlist GPS, cellular, WiFi and Bluetooth. A GPS receiver in the phone calculates its own position by determining how long it takes the radio signals from different GPS satellites to arrive. The locations of cell towers, WiFi hotspots and Bluetooth beacons within range of the phone can also inform location data.

Commonly, an app developer will embed a software development kit (SDK) into their app that essentially siphons location data directly to a data broker or advertising platform. This is a common practice because it saves development work around implementing features and creates a predictable stream of income that grows bigger as more people use the app.

Side channels
Though still largely in the realm of experimentation, researchers have demonstrated that a smartphone's location can be inferred using alternate resources contained within the phone, including those accessible without requiring explicit permission from the user.

For example, numerous research teams have demonstrated[1] that motion sensors can be used to figure out driving routes. Sensor readings from the accelerometer are used to determine acceleration patterns and stops, while readings from the gyroscope clarify turn angles and the digital compass shows the direction of travel. From there, map-matching algorithms can be used to match the inferred route to map data for the purpose of obtaining predicted location points.

Such a capability could be added to any app by a nefarious developer.

> *"The deepest privacy threat from mobile phones – yet one that is often completely invisible – is the way that they announce your whereabouts all day (and all night) long through the signals they broadcast."*
>
> - The Electronic Frontier Foundation

HOW THREAT ACTORS ACCESS SMARTPHONE LOCATION DATA

Threat actors have a number of tools at their disposal for accessing the historical and real-time location information of targeted smartphones.

Cellular infrastructure
Commercial surveillance companies offer tracking systems[2] that access carrier location databases, allowing end users to receive an individual's location history by simply inputting the target's phone number. These systems take advantage of the lax security of the SS7 network used by carriers to communicate with one another when directing cell services.

Alternatively, threat actors can hack a telecommunications company to steal location data. According to cybersecurity researchers from Cybereason, Chinese state-backed hacking groups compromised[3] multiple telecom providers across Southeast Asia from 2017 to 2021, stealing phone records and location data.

Data brokers
After receiving raw location data from an app developer, a data broker will often analyze the data and/or combine it with users' information to create or bolster detailed audience profiles. This information, which can include demographic details and even full names and contact information, can be pulled from other apps associated with the same mobile advertising identifiers as well as from offline sources. This enriched location data is then sold to any number of third parties. Threat actors can pose as a front company to purchase such data.

Threat actors can also hack the broker's database or leverage a compromised account to access the data.

Some vendors even offer location data products[4] that enable users to work with the information in unique ways, such as seeing all devices in a defined location or following a specific device around to see where it has been.

Spyware
For highly targeted location tracking, threat actors can employ smartphone spyware against an individual. Whether obtained commercially or developed in-house, such spyware can, in addition to gathering other sensitive information, track the target's location in real time.

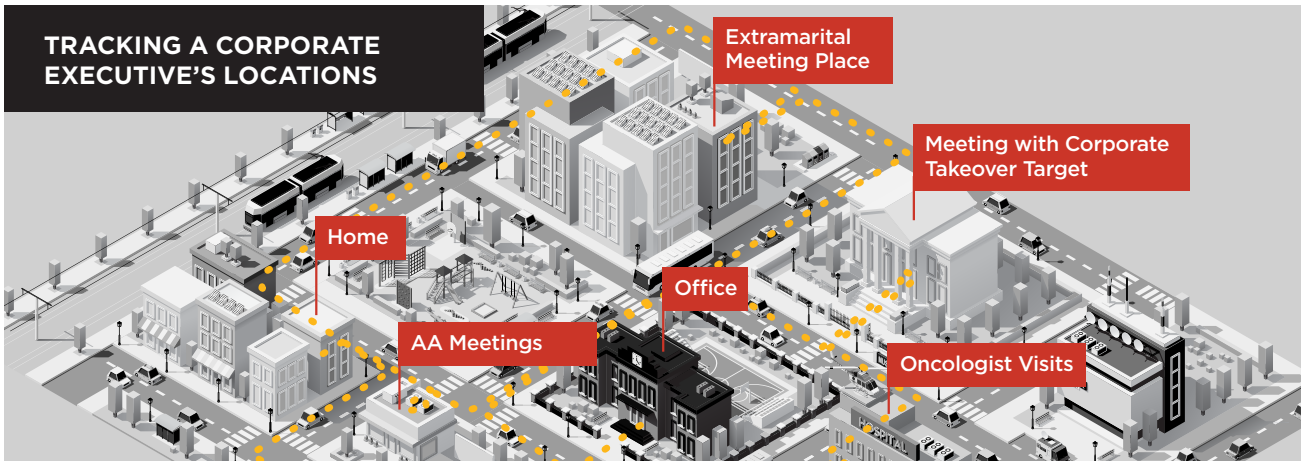
IMSI catchers
For location tracking within a defined geographic area, threat actors can make use of an IMSI catcher, which is essentially a fake cell tower designed to trick smartphones within range into connecting to it. To do so, the IMSI catcher can masquerade as a legitimate, preferred tower and even jam competing towers with white noise. Once connected to a targeted smartphone, the IMSI catcher can force the device to respond with its location, among other capabilities.

Tools specific to law enforcement
In addition to the methods above, law enforcement agencies have other mechanisms for obtaining smartphone location data. In democratically challenged countries, these tools can be used to facilitate harassment or repression of targeted individuals.

One such method is the cell tower dump, in which law enforcement goes directly to a cellular provider to obtain the telephone numbers of all devices registered on a particular cell tower at a certain time. The Ukrainian government reportedly employed[5] a tower dump in 2014 to discover all of the phones that were present at an anti-government protest.

Another method that has gained steam in recent years is the geofence warrant, whereby law enforcement asks a tech company (often Google) to provide a list of users who happened to be in a specific area at a given time.

> *"Once your location is collected, you'll never get it back — you'll never know where it's gone, who's bought it, who's looked at it."*
>
> - Stuart A. Thompson and Charlie Warzel, *The New York Times*



WHAT SMARTPHONE LOCATION DATA CAN REVEAL

While smartphone location data can certainly reveal an individual's home, place of business and other frequently visited sites, the data can also paint an incredibly vivid narrative of a person's life, as each location point is associated with a specific date and time. Threat actors can analyze the data to infer the person's behaviors and preferences and to detect actionable patterns. When combined with aggregated location data, an individual's location data can illuminate hidden associations and locations.

The following are some of the potential insights buried in location data:

- **Key locations:** An individual's home address isn't hard to pick out[6] from the data, as the smartphone will be in a fixed position for hours at a time as the target sleeps each night. If the target's identity is unknown, a threat actor can determine it using their inferred address and publicly available information.
- **Habits and routines:** Over a long-enough time frame, the target's routines will become clear. Perhaps there's a visit to the same coffee shop every morning, a weekly yoga class or a predilection for a certain fast-food establishment.
- **Preferences:** From repeated visits to similar types of places, one can draw conclusions about the target's preferences. For example, repeated visits to golf courses indicate a passion for golf. Similarly, the target's sexual preferences can be inferred based on the types of clubs they visit.
- **Health issues:** Location data can reveal long hospital visits, visits to health specialists, psychiatry sessions and other evidence of medical treatment.
- **Involvement in events:** If the target attended a protest, a party, a political rally or any other event, this would appear in the location data. Aggregated location data can show which fellow attendees were present during these occasions.
- **Hidden locations:** Aggregated location data can reveal clusters in unusual or unlisted locations and tip off threat actors about the presence of a secret military base[7] or skunkworks project.
- **Hidden associations:** Aggregated location data can help uncover associations not previously known, perhaps indicating confidential talks with a corporate takeover target or a secret romantic relationship.

HOW INSIGHTS FROM SMARTPHONE LOCATION DATA CAN BE WEAPONIZED

The risks associated with weaponized smartphone location data are different for every individual. Below are some examples illustrating how location data can be misused by threat actors.

Physical tracking
After analyzing commercially available smartphone location data to get a handle on a famous actor's routine, a stalker stakes out the celebrity's favorite café during times of the week most likely to result in an encounter. The stalker eventually makes contact and takes intrusive videos that are shared online.

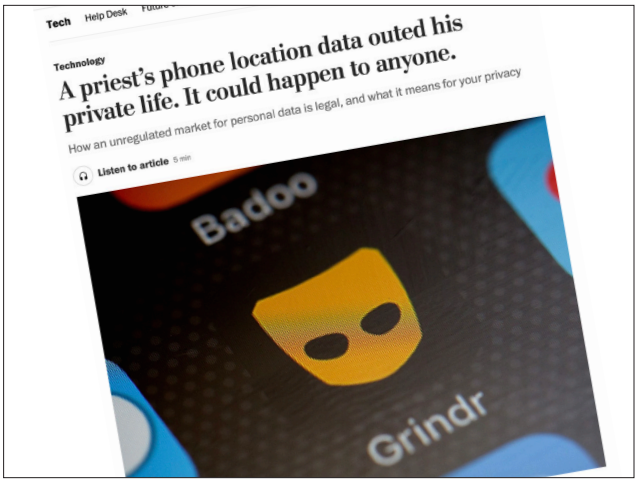
Public attacks
Tipped off by an informant with access to a location database licensed by a law enforcement agency, a tabloid learns that a politician sleeps at his aide's residence a few nights a week. The publication digs into the relationship and later goes public with the findings.

Blackmail
A criminal uses stolen credentials to a data broker's database to dig into a public figure's private life. After learning of the individual's recent visit to a drug rehab center, the criminal blackmails them into paying for silence.

Adapted strategy
A state-backed hacking group specializing in corporate espionage has infiltrated a cellular provider and learns of a secret meeting between the CEO of a rival foreign company and the head of another company, indicating a potential merger. Word flows back to a domestic competitor, which then pivots to reduce the impact of the merger.

Targeted hacking
A rogue hacker comes across a large dump of smartphone location data that's been leaked on the dark web. After learning that a high-net-worth individual gets coffee at the same shop every day, the hacker conducts a wireless attack from the parking lot and gains access to the target's banking credentials.

Given the secretive nature of smartphone location tracking by threat actors, concrete examples of this practice are not readily available or reported. However, a recent case may be a sign of things to come. In 2021, a Catholic priest was publicly outed[8] by a newsletter that used location data ultimately tied to Grindr. The publication was able to pinpoint which device belonged to the priest based on pings at his residence and other known locations, and then tracked that device to various gay bars.



HOW TO OPT OUT OF SMARTPHONE LOCATION TRACKING

When it comes to protecting location privacy, smartphone users have only a modicum of control. Short of not using any location-based apps, they can strictly manage app permissions to ensure that their location is only shared with trusted apps and only when the app is actively used, for example. This can limit location tracking through apps, but tracking through the cellular network is still possible. To counter this, users can turn off their device's location services and related radios when on the move. However, manipulating software settings is inconvenient and easy to forget to do consistently. On top of that, the operating system and any spyware on the device can continue to gather location data.

To make location privacy both convenient and highly assured, we at Privoro have developed Vault™. Vault serves as a portable Faraday enclosure delivering the highest levels of radio frequency attenuation to shield the device from cellular, WiFi, Bluetooth or GPS signals. By simply inserting their smartphone into Vault whenever traveling or otherwise needing to shield their location, users can achieve instant peace of mind that their location breadcrumbs won't be used against them.

PRIVORO®

SOURCES

1. Schlesinger, Jennifer, and Andrea Day, "How GPS can track you, even when you turn it off," CNBC, July 14, 2018.

2. Timberg, Craig, "For sale: Systems that can secretly track where cellphone users go around the globe," The Washington Post, August 24, 2014.

3. Gallagher, Ryan, "Chinese Hackers Compromised Telecom Firms, Researchers Say," Bloomberg, August 2, 2021.

4. Cox, Joseph, "How the U.S. Military Buys Location Data from Ordinary Apps," Motherboard, November 16, 2020.

5. Peterson, Andrea, "Ukraine's 1984 moment: Government using cellphones to track protesters," The Washington Post, January 21, 2014.

6. Thompson, Stuart A., and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy," The New York Times, December 19, 2019.

7. Tau, Byron, "The Ease of Tracking Mobile Phones of U.S. Soldiers in Hot Spots," The Wall Street Journal, April 26, 2021.

8. Cox, Joseph, "The Inevitable Weaponization of App Data Is Here," Motherboard, July 21, 2021.

PRIVORO®