12.22.17

How—And Why—Apple, Google, And Facebook Follow You Around In Real Life

Big tech companies and others are quietly amassing mountains of users' location data, in ways many don't realize and sometimes can't avoid.

[Photo: Arambar/Wikipedia]

BY DJ PANGBURN

LONG READ

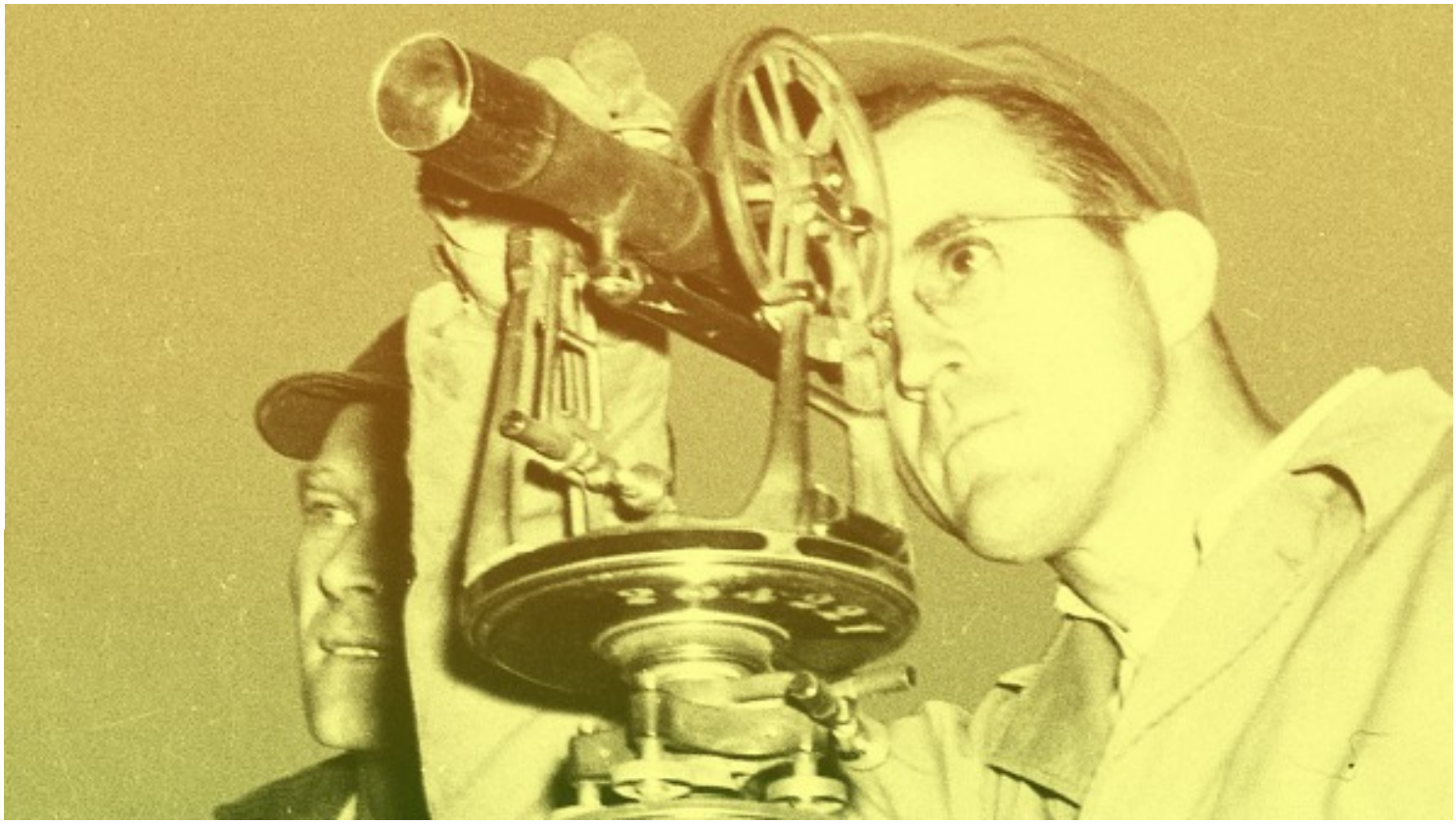
Even the most absent-minded smartphone user is probably aware that apps keep tabs on where they go. Many apps wouldn't work without location data. But few realize just how often that location tracking is happening—even when it's not necessary, even when their apps aren't being used, and, increasingly, even when a user isn't even carrying their phone. Tracking you across the map isn't always about improving user experience, of course, but rather about better understanding who you are and what kind of advertising to show you. If, for instance, a company knows that you've just stepped foot in one of their stores, they might start targeting you with ads touting a sale.

It's hard to dispute the value of a good sale, but location tracking raises all sorts of privacy concerns. (Not to mention that using the GPS will drain your smartphone's battery faster.) Should app makers know where we live, where our children go to school, where we go to get away from it all? And if so, how much should they tell us about it?

Those complicated questions help explain why the biggest tech companies, including Apple, Amazon, Facebook, Google, Twitter, and Verizon, filed a pro-privacy amicus brief in last month's Supreme Court case Carpenter v. United States, in which they argued that police should have a warrant before accessing cell phone location data. After all, if we thought the police could easily access our data, we might start asking more questions about what our phones know about us, and become less comfortable with using these companies' products.

But location tracking is quietly, sometimes surreptitiously, baked into the web's modern data collection regime. According to a recent study by French research organization Exodus Privacy and Yale University's Privacy Lab, more than three in four Android apps contain at least one third-party "tracker," which uses various techniques to glean personal information, including location and in-app behavior, to better target users for advertisements and services. (In 2016, the FTC sued InMobi, a company that described itself as "the world's largest independent mobile advertising company" because it tracked consumers' location even if they denied permission.)

The t ers found by the Yale researchers include some of the most popular apps on the Google Play Store, including Tinder, Spotify, Uber, and OKC . Many of these apps rely on a service owned by Google, Crashlytics, that primarily tracks app crash reports, but can also provide the ability to "get i ght into your users, what they're doing, and inject live social content to delight them." The researchers didn't study iOS apps, but they warned that the p em may also exist on Apple's App Store, noting that many of the tracker companies used on Android apps also distribute apps via Apple.



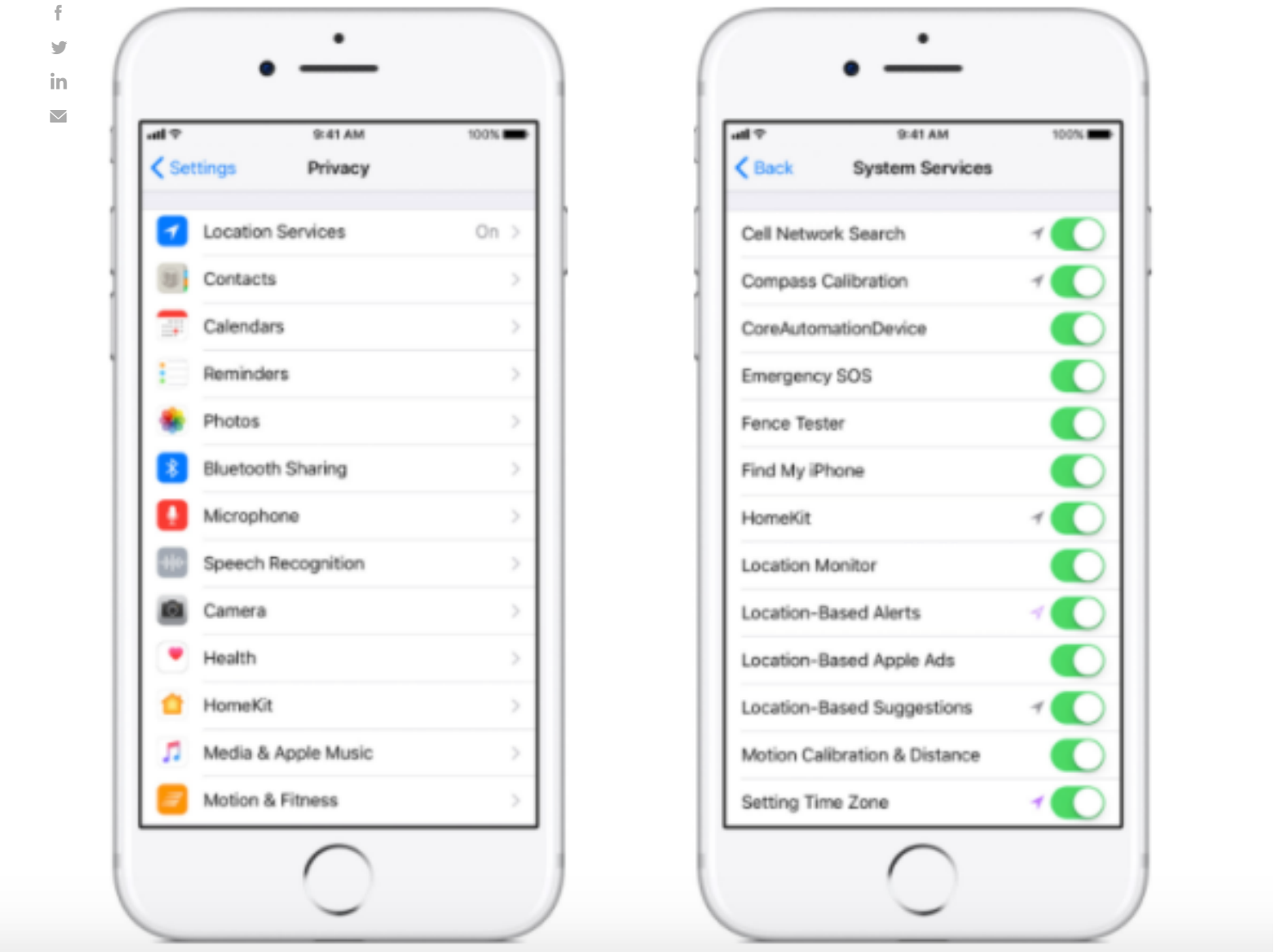
[Photo: Flickr user U.S. Department of Energy]

Even so-called anonymized location data—without our real-life name attached to it—can help paint a detailed portrait of a user and their habits, or even crack open their entire identity. Like the National Security Agency, which gathers billions of records a day on people's cell-phone locations across the globe, developers realize there is a lot to be gleaned from users' frequented locations and movement patterns. For app developers and ad targeters, this locational awareness is "the stuff of the future," as one data scientist put it to me recently. Here's how three of the largest companies are gathering your location, and what, if anything, you can do about it.

APPLE: "A BETTER USER EXPERIENCE" AND TARGETED ADS

The company has been lauded by some for its emphasis on privacy. As Apple chief executive Tim Cook says in a letter at the company's privacy webpage, "When we do ask to use your data, it's to provide you with a better user experience."

But Apple's handling of location data has faced criticism before. In 2011, Apple was found to be storing location data on users' phones in an unencrypted file; it subsequently encrypted that kind of data on the device, on the cloud, and in transit. And in a class-action lawsuit filed in 2014, plaintiff Chen Ma was concerned that, among other things, users were given "no meaningful" way to switch off Location Services without "substantially compromising" key parts of the iPhone's functionality.



Privacy and location services in iOS 11 (Settings > Privacy > Location Services > System Services).

Apple still collects a lot of location data, though it says it doesn't share this data directly with advertisers: Like Facebook and Google, it only makes your data available to them by putting you in an "anonymized" targeting group. iPhone users can turn off "Location-based Apple ads," thanks to a small radio button deep inside the settings app (Settings > Privacy > Location Services > System Services; even with that off, however, Apple still builds an ad targeting profile on you based on keyboard language settings, device type, App Store searches and Apple News articles you read, though some of that tracking can be limited under Settings > Privacy > Advertising.)

If Location Services is on, some location data collection can't be turned off at all. With Location Services enabled, according to Apple, "your device will periodically send the geo-tagged locations of nearby Wi-Fi hotspots and cell towers to Apple to augment Apple's crowd-sourced database of Wi-Fi hotspot and cell tower locations." If you're moving in a vehicle, "a GPS-enabled iOS device will also periodically send GPS locations and travel speed information to Apple to be used for building up Apple's crowd-sourced road-traffic database." (This "crowd-sourced location data" is "anonymous and encrypted," Apple adds. "It doesn't personally identify you.")

All of this location data is owned by Apple. At the very bottom of another page, Apple clarifies that by enabling Location Services for your devices, "you agree and consent to the transmission, collection, maintenance, processing, and use of your location data and location search queries by Apple, its partners, and licensees to provide and improve location-based and road traffic-based products and services." Most users have little choice here: As Chen Ma pointed out in her lawsuit, many apps simply can't function without activating location services in some form.

On iOS, navigate to Settings, then scroll down and tap on Privacy, then tap on Location Services. Users can disable location tracking wholesale by toggling the slider to off, or can control which specific apps have access to location and when. In iOS 11, users can choose to allow an app to track their location either "Never" or only while using the app.

GOOGLE: AN ARSENAL OF TOOLS TRACKS YOU ONLINE AND OFFLINE

Like Facebook and others, Google is working to insert itself even further into our daily transactions, and location data is critical to that. Google's fleet of apps—Gmail, Chrome, Gchat, and of course Maps—collect location data with user permission; other apps in the Android ecosystem also gather location data, sometimes without permission (see above). Like many other data companies, Google also follows users across the internet with web cookies that track IP addresses, which, as the *Guardian* reported last year, allows the service to make pretty informed guesses on user locations and habits.

The tech giant also uses what is known as "implicit location information," which is when Google interprets a search for a specific location ("Empire State buildi estaurants nearby," for instance) as evidence the person will be visiting the building; then targets related ads at the user based on this inform on.

In Ma Google announced a new program aimed at tracking users' offline locations and behavior too, using data gathered from third-parties. (The comp says it has access to about 70% of U.S. credit and debit card transactions through partnerships with data companies.) After a user clicks on a merchant's digital ad, Google can determine if that person purchased something in that merchant's bricks-and-mortar store; that could help persuade merchants to spend more on ads. At the time, Google said it would "match transactions back to Google ads in a secure and privacy-safe way, and only report on aggregated and anonymized store sales to protect your customer data."

Google has also managed to collect user locations in more surreptitious ways. As *Quartz* reported last month, Google collected the physical addresses of nearby cell towers with which Android users' phones were communicating for everyday text, call and app usage. Gathering data from several cell towers effectively allows Google to triangulate a user's cell signal, and thus determine an approximate location—even when users have location services turned off or have removed their SIM card. Google told *Quartz* that this data was not stored, and that it would end the data collection.

To disable location tracking on an Android device, go to Settings, scroll down and tap Location, then switch the slider to the off position. However, as with iOS apps (above), this will turn off all location tracking so that apps like Google Maps or even Uber or Lyft won't work. To control location tracking with more granularity, go into each app through the App Manager and turn off location tracking. Android Users can also view and delete their device's location history. All users of Google services can also see their location data through the company's Timeline page, and can opt out of having some of their activities logged and opt out of being shown some ads.

Related: The Popular Design Tool That's Actually A Privacy Nightmare

FACEBOOK CAN ALSO TELL WHERE YOU SHOP OFFLINE

As with other smartphone apps, Facebook, Messenger, WhatsApp, and Instagram also attempt to capture your location across devices and throughout the course of the day, from your early-morning reading habits, to a Spotify playlist during your commute, to your social media browsing at night. Like Google, Facebook wants to help advertisers know if their ads led you to visit the advertisers' brick-and-mortar store, and to help "retarget" ads at you if you have. You don't need to be online, or with your device either: Facebook, like Google and other large data gatherers, are also determined to link not just your online locations and data, but your offline location data too.

As of September, advertisers can use Facebook data as well as custom data provided by the advertiser, like a list of in-store purchases, to target ads at users. "This feature allows businesses to re-engage in-store audiences with more relevant and compelling campaigns, as well as create lookalike audiences," Facebook said in a statement. An apparel brand could "choose to exclude in-store customers, for example, when running a promotion available only for new customers."

To turn off location tracking for Facebook, see its explainer, and check your privacy settings to choose how the platform targets ads at you. Note that you can't stop someone like a friend from tagging your location or your Facebook profile in a location-tagged photo. It's also worth mentioning that if you upload a photo to Facebook, unless you've disabled location tracking, the photo will include geotags that provide Facebook with location data on where the photo was taken. To see your check-in locations, from your profile, hover your mouse over "More" and click "Check-ins." Users can also download their Facebook data to see login locations.

In general, it's also a good idea to routinely clear your browser of cookies and trackers that Facebook and other companies use to track you in digital and physical space.

Related: Here's How To Track The Smartphone Apps That Are Tracking You

HOW WHATSAPP AND INSTAGRAM FEED FACEBOOK'S LOCATION DATABASE

Some apps are less obvious about their location tracking. Take WhatsApp, the popular Facebook-owned messaging app that lets users communicate with encryption via Wi-Fi instead of on their cellular data plans. On the surface, it would seem that WhatsApp wouldn't require location data. But I recently noticed that location services were enabled on my iPhone's WhatsApp app. Based on my frequency of usage, this means that WhatsApp was pretty much always tracking my location for the last seven months, and feeding that data into the internal profile Facebook uses to track me. Facebook uses Instagram data in a similar way.

In November 2016, after protests and pressure from privacy regulators in Europe over Facebook's decision to combine WhatsApp data with Facebook data, the social media platform temporarily paused its data sharing program for European users. In May, the European Commission fined Facebook $122 million for misleading WhatsApp users about its data sharing with Facebook.