

# Every Step You Take, Every Stop You Make: Your Phone Apps Are Tracking You (And Selling That Info)

They'll tell you they need your location to identify your favorite sports team or give you personalized weather reports or to warn you of traffic jams, but that isn't the only reason they want to track you. These companies want to collect your information and sell it.



[Daisy Luther](#) —

- 96shares
- [Share](#)
- [Tweet](#)
- [Plus](#)
- 

You're being watched constantly, at least if you have a [cell phone](#) with apps on them. A recently published report showed how seemingly innocuous apps were gathering information about

how a person goes about their day. They refresh constantly, collecting data about your location.

These companies are tracking every step you take, every stop you make, and then selling it to the highest bidder.

Now, before I get the predictable chorus of people telling me they'd never ever use a smartphone and that if they did have one they wouldn't enable location data on it, I can call BS (baloney sandwiches) on at least 44% of you because...well...Google tells me this. I get emails from Google every week telling me from what type of devices people access my website. I did not sign up to ask for this information – this is what Google does.

take our poll - story continues below



# • Who will cave first over the government shutdown?

So while many of you *are not* using a mobile device, many of you are.

## How the location apps are tracking every step you take

Everyone looks like dots on a map to the smartphone apps, but the information that can be put together is positively chilling. Here's what a day looks like for one of these "dots" on a map:

Yet another leaves a house in upstate New York at 7 a.m. and travels to a middle school 14 miles away, staying until late afternoon each school day. Only one person makes that trip: Lisa Magrin, a 46-year-old math teacher. Her smartphone goes with her.

An app on the device gathered her location information, which was then sold without her knowledge. It recorded her whereabouts as often as every two seconds, according to a database of more than a million phones in the New York area that was reviewed by The New York Times. While Ms. Magrin's identity was not disclosed in those records, **The Times was able to easily connect her to that dot.**

The app tracked her as she went to a Weight Watchers meeting and to her dermatologist's office for a minor procedure. It followed her hiking with her dog and staying at her ex-boyfriend's home, information she found disturbing.

“It’s the thought of people finding out those intimate details that you don’t want people to know,” said Ms. Magrin, who allowed The Times to review her location data. ([source](#))

Magrin was recorded more than 800 times making the trip to and from her place of work.

### **Have you enabled location services?**

If you have location information enabled on your phone, you’re being watched. There are more than 75 companies with apps that know where you live, where you work, where you go to the gym, and many other details about your personal routine.

According to the report by the NY Times, these apps are updating with your location 14,000 times per day, pinpointing your location within a few yards. And the businesses involved think it’s perfectly fine. “Many location companies say that **when phone users enable location services, their data is fair game.**”

About 75 companies have access to how [cell phone](#) users spend their time. This includes children who are often given phones these days so that parents can reach them at all times. This creepy tidbit was also discovered in the archives of data to which The Times was given access when once set of data showed the user of the phone going to the playground to school then back home.

**Location targeting is a massive, horrifying business, and it’s booming.**

The businesses involved track you, analyze your data, and either sell it or use it themselves. They claim that they have no interest in your identity – they're only looking at your patterns.

But those with access to the raw data — including employees or clients — could still identify a person without consent. They could follow someone they knew, by pinpointing a phone that regularly spent time at that person's home address. Or, working in reverse, they could attach a name to an anonymous dot, by seeing where the device spent nights and using public records to figure out who lived there. ([source](#))

One company, creepily called Reveal Mobile, has location-gathering code embedded into more than 500 apps, many of which provide local news.

Some estimates say that location targeting is going to be worth **\$21 billion** this year.

### **How they make money by tracking you**

The way they make money is simple – they track you and sell the information to people who want to advertise to you. Then, the people who bought your information use patterns discerned through tracking you to sell you things. The exception to this is Google, which physically tracks you so that they can sell ads to people who want to reach you as opposed to selling your information specifically.

The app developers can make money by directly selling their data, or by sharing it for location-based ads, which command a premium. Location data companies pay half a

cent to two cents per user per month, according to offer letters to app makers reviewed by The Times.

Targeted advertising is by far the most common use of the information.

Google and Facebook, which dominate the mobile ad market, also lead in location-based advertising. Both companies collect the data from their own apps. They say they don't sell it but keep it for themselves to personalize their services, sell targeted ads across the internet and track whether the ads lead to sales at brick-and-mortar stores. Google, which also receives precise location information from apps that use its ad services, said it modified that data to make it less exact.

Smaller companies compete for the rest of the market, including by selling data and analysis to financial institutions. This segment of the industry is small but growing, expected to reach about \$250 million a year by 2020, according to the market research firm Opimas.

[\(source\)](#)

The small companies are heading toward making 250 million. The small ones.

With that kind of money at stake, you know this is only going to become more prevalent.

**Here are just a few of the apps that are selling your information.**

As a reminder that nothing in this world is actually free, here are some of the “free” apps that may be tracking you right now, wherever you’re sitting down to read this article.

- [WeatherBug](#)
- [GasBuddy](#)
- [theScore](#)
- [The Weather Channel](#)
- Sense360
- Google
- Facebook

If you’re curious whether apps on your phone are tracking you and selling your information, [here’s a place you can plug in the name of your app and get a report](#). The only app on my phone with location enabled was Waze, which, thankfully doesn’t seem to be selling my information at this point in time.

### **Here’s how to protect your location privacy**

The Daily Mail explains how to protect your location privacy and get rid of anything that may be stored on your devices.

Even if you have ‘Location History’ off, Google often stores your precise location.

Here’s how to delete those markers and some best-effort practices that keep your location as private as possible.

But there’s no panacea, because simply connecting to the internet on any device flags an IP address that can be geographically mapped.

Smartphones also connect to cell towers, so your carrier knows your general location at all times.

### **To disable tracking on any device**

Fire up your browser and go to [myactivity.google.com](https://myactivity.google.com). You'll need to be logged into Google.

On the upper left drop-down menu, go to 'Activity Controls.' Turn off both 'Web & App Activity' and 'Location History.'

That should prevent precise location markers from being stored to your Google account.

Google will warn you that some of its services won't work as well with these settings off.

In particular, neither the Google Assistant, a digital concierge, nor the Google Home smart speaker will be particularly useful.

### **On iOS**

If you use Google Maps, adjust your location setting to 'While Using' the app. This will prevent the app from accessing your location when it's not active.

Go to Settings Privacy Location Services and from there select Google Maps to make the adjustment.

In the Safari web browser, consider using a search engine other than Google.



Under Settings Safari Search Engine, you can find other options like Bing or DuckDuckGo.

You can turn location off while browsing by going to Settings Privacy Location Services Safari Websites, and turn this to 'Never.'

This still won't prevent advertisers from knowing your rough location based on IP address on any website.

You can also turn Location Services off to the device almost completely from Settings Privacy Location Services.

Both Google Maps and Apple Maps will still work, but they won't know where you are on the map and won't be able to give you directions.

Emergency responders will still be able to find you if the need arises.

## **On Android**

Under the main settings icon click on 'Security & location.' Scroll down to the 'Privacy' heading. Tap 'Location.' You can toggle it off for the entire device.

Use 'App-level permissions' to turn off access to various apps.

Unlike the iPhone, there is no setting for 'While Using.'

You cannot turn off Google Play services, which supplies your location to other apps if you leave that service on.

Sign in as a 'guest' on your Android device by swiping down from top and tapping the downward-facing cursor, then again on the torso icon.

Be aware of which services you sign in on, like Chrome. You can also change search engines even in Chrome.

### **To delete past location tracking on any device**

On the page, [myactivity.google.com](https://myactivity.google.com), look for any entry that has a location pin icon beside the word 'details.'

Clicking on that pops up a window that includes a link that sometimes says 'From your current location.'

Clicking on it will open Google Maps, which will display where you were at the time.

You can delete it from this popup by clicking on the navigation icon with the three stacked dots and then 'Delete.'

Some items will be grouped in unexpected places, such as topic names, google.com, Search, or Maps.

You have to delete them item by item. You can wholesale delete all items in date ranges or by service, but will end up taking out more than just location markers. ([source](#))

According to The Daily Mail, Android has 1,200 apps with this kind location-sharing code while iOS has only 200.

**Think about the types of things that can be discovered about you.**

An app that constantly updates your location could find out a lot of intimate details. Here are a few examples of the invasive things that could be discovered:

- With whom you're spending time and where (read: who you're dating, having an affair with, best friends with)
- Where you get your food
- If you go to a psychiatrist or an oncologist
- If you attend AA or NA meetings
- How you're spending your work hours
- The route you regularly drive during your day
- How much exercise you get
- Whether you're walking or driving
- Where you live
- Where you work
- Where you spend your free time

Basically, every daily habit you have, someone knows if you use a cell phone with the location enabled. Every step you take, someone knows where that step is taking you. Every place you stop at for a period of time – someone knows that too.

**The thing is, people are giving their permission to be tracked.**

You know when you add something to your phone or computer and it forces you to grant permission for something that you don't really understand in a long disclaimer that hardly anyone actually reads? Then you click on the little checkmark saying "yeah, sure, whatever?"

That's the moment you gave one of these companies permission to track every move you make.

Companies that use location data say that people agree to share their information in exchange for customized services, rewards and discounts. Ms. Magrin, the teacher, noted that she liked that tracking technology let her record her jogging routes.

Brian Wong, chief executive of Kiip, a mobile ad firm that has also sold anonymous data from some of the apps it works with, says users give apps permission to use and share their data. "You are receiving these services for free because advertisers are helping monetize and pay for it," he said, adding, "You would have to be pretty oblivious if you are not aware that this is going on."

But it is easy to share information without realizing it. Of the 17 apps that The Times saw sending precise location data, just three on iOS and one on Android told users in a prompt during the permission process that the information could be used for advertising. Only one app, GasBuddy, which identifies nearby gas stations, indicated that data could also be shared to "analyze industry trends." ([source](#))

It's very true that nothing is free.

They'll tell you they need your location to identify your favorite sports team or give you personalized weather reports or to warn you of traffic jams, but that isn't the only reason they want to track you. These companies want to collect your information and sell it.

Repeat after me:

**NOTHING IS FREE.**

Article posted with permission from [Daisy Luther](#)