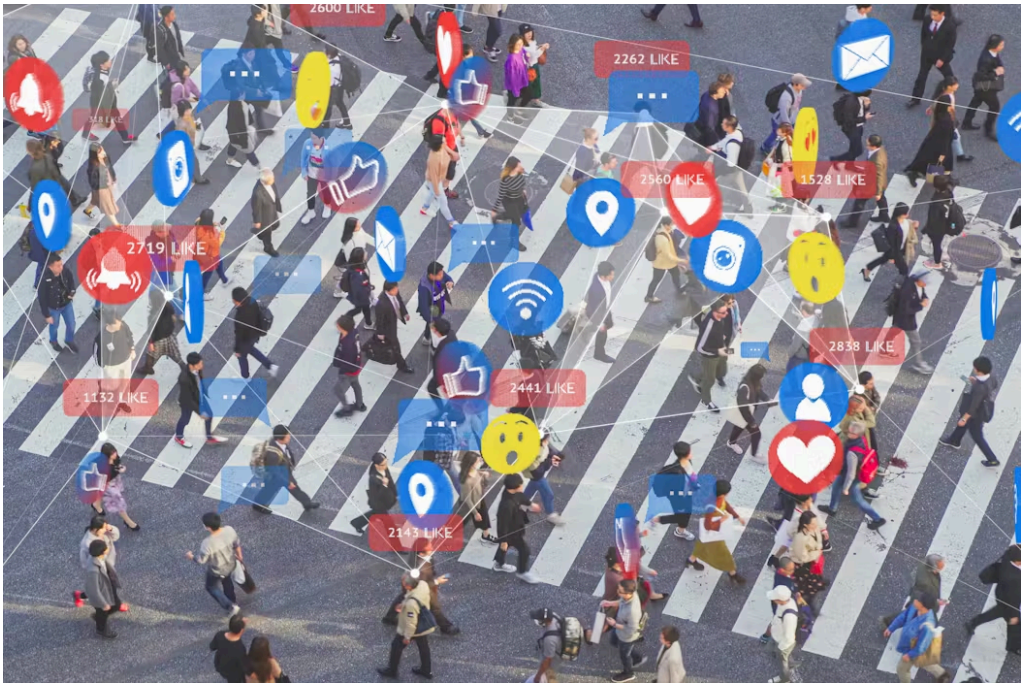
Yes, the government can track your location – but usually not by spying on you directly

Emilee Rader, Professor of Information, University of Wisconsin-Madison

Published: December 3, 2025 8:26am EDT



Where your smartphone has been is available for sale.

cofotoisme/iStock via Getty Images

If you use a mobile phone with location services turned on, it is likely that data about where you live and work, where you shop for groceries, where you go to church and see your doctor, and where you traveled to over the holidays is up for sale. And U.S. Immigration and Customs Enforcement is one of the customers.

The U.S. government doesn't need to collect data about people's locations itself, because your mobile phone is already doing it. While location data is sometimes collected as part of a mobile phone app's intended use, like for navigation or to get a weather forecast, more often locations are collected invisibly in the background.

I am a privacy researcher who studies how people understand and make decisions about data that is collected about them, and I research new ways to help consumers get back some control over their privacy. Unfortunately, once you give an app or webpage permission to collect location data, you no longer have control over how the data is used and shared, including who the data is shared with or sold to.

Why mobile phones collect location data

Mobile phones collect location data for two reasons: as a by-product of their normal operation, and because they are required to by law.

Mobile phones are constantly scanning for nearby cell towers so that when someone wants to place a call or send a text, their phone is already connected to the closest tower. This makes it faster to place a call or send a text.

To maintain quality of service, mobile phones often connect with multiple cell towers at the same time. The range of the radio signal from a cell tower can be thought of as a big bubble with the cell tower in the center. The location of a mobile phone can be calculated via triangulation based on the intersection of the bubbles surrounding each of the cell towers the phone is connected to.

In addition to cell tower triangulation, since 2001 mobile phone carriers have been required by law to provide latitude and longitude information for phones that have been used to call 911. This supports faster response times from emergency responders.

How location data ends up being shared

When people allow webpages and apps to access location data generated by their mobile phones, the software maker can share that data widely without asking for further permission. Sometimes the apps themselves do this directly through partnerships between the maker and data brokers.

More often, apps and webpages that contain advertisements share location data via a process called “real-time bidding,” which determines which ads are shown. This process involves third parties hired by advertisers, which place automated bids on the ad space to ensure that ads are shown to people who match the profile of interests the advertisers are looking for.

To identify the target audience for the ads, software embedded in the app or webpage shares information collected about the user, including their location, with the third parties placing the bids. These third parties are middlemen that can keep the data and do whatever they want with it, including selling the data to location data brokers, whether or not their bid wins the auction for the ad space.

What happens to the data once it is shared

The data acquired by location data brokers is sold widely, including to companies called location-based service providers that repackage it and sell access to tools that monitor people's locations. Some of these tools do things like provide roadside assistance. Others are used by police, government agencies and others to track down individuals.

In October 2025, news outlets reported that U.S. Immigration and Customs Enforcement had purchased a location surveillance tool from a company called Penlink that can track movements of specific mobile devices over time in a given location. Tools like this allow users to access location data from "hundreds of millions of mobile phones" without a warrant.

Why it matters

The invisible collection, sale and repackaging of location data is a problem because location data is extremely sensitive and cannot be made anonymous. The two most common locations a person visits are their home and where they work. From this information alone, it is trivially easy to determine a person's identity and match it with the other location data about them that these companies have acquired.

Also, most people don't realize that the location data they allowed apps and services to collect for one purpose, like navigation or weather, can reveal sensitive personal information about them that they may not want to be sold to a location data broker. For example, a research study I published about fitness tracker data found that even though people use location data to track their route while exercising, they didn't think about how that data could be used to infer their home address.

This lack of awareness means that people can't be expected to anticipate that data collected through the normal use of their mobile phones might be available to, for example, U.S. Immigration and Customs Enforcement.

More restrictions on how mobile phone carriers and apps are allowed to collect and share location data – and on how the government is allowed to obtain and use location information about people – could help protect your privacy. To date, Federal Trade Commission efforts to curb carriers' data sales have had mixed results in federal court, and only a few states are attempting to pass legislation to tackle the problem.

Emilee Rader receives funding from the National Science Foundation.