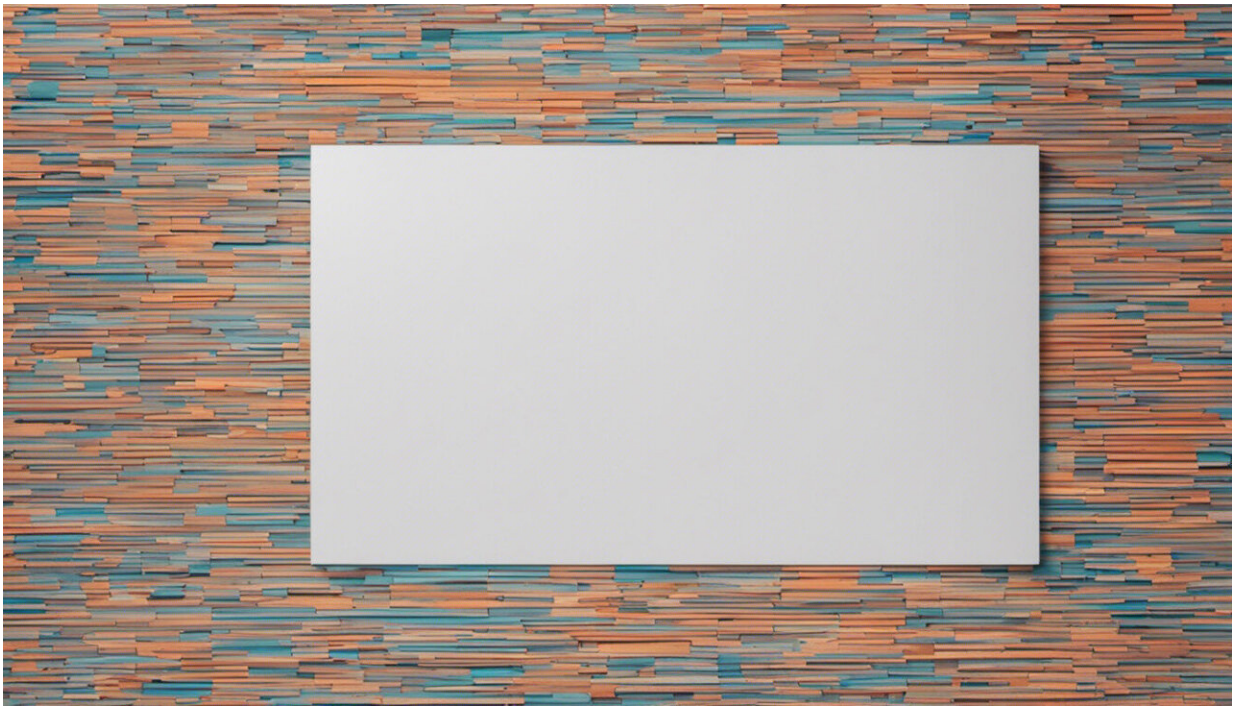
Change your phone settings so Apple, Google can't track your movements

January 14 2019, by Jen King



Credit: AI-generated image (disclaimer)

Technology companies have been pummeled by revelations about how poorly they protect their customers' personal information, including an in-depth New York Times report detailing the ability of smartphone apps to track users' locations. Some companies, most notably Apple, have begun promoting the fact that they sell products and services that

safeguard consumer privacy.

Smartphone users are never asked explicitly if they want to be tracked every moment of each day. But cellular companies, smartphone makers, app developers and social media companies all claim they have users' permission to conduct near-constant personal surveillance.

The underlying problem is that most people don't understand how tracking really works. The technology companies haven't helped teach their customers about it, either. In fact, they've intentionally obscured important details to build a multi-billion-dollar data economy based on an ethically questionable notion of informed consent.

How consumers are made to agree

Most companies disclose their data protection practices in a privacy policy; most software requires users to click a button saying they accept the terms before using the program.

But people don't always have a free choice. Instead, it's a "take-it-or-leave-it" agreement, in which a customer can use the service only if they agree.

Anyone who actually wants to understand what the policies say finds the details are buried in long legal documents unreadable by nearly everyone, perhaps except the lawyers who helped create them.

Often, these policies will begin with a blanket statement like "your privacy is important to us." However, the actual terms describe a different reality. It's usually not too far-fetched to say that the company can basically do whatever it wants with your personal information, as long as it has informed you about it.

U.S. federal law does not require that a company's privacy policy actually protect users' privacy. Nor are there any requirements that a company must inform consumers of its practices in clear, nonlegal language or provide consumers a notice in a user-friendly way.

Theoretically, users might be able to vote with their feet and find similar services from a company with better data-privacy practices. But take-it-or-leave-it agreements for technologically advanced tools limit the power of competition across nearly the entire technology industry.

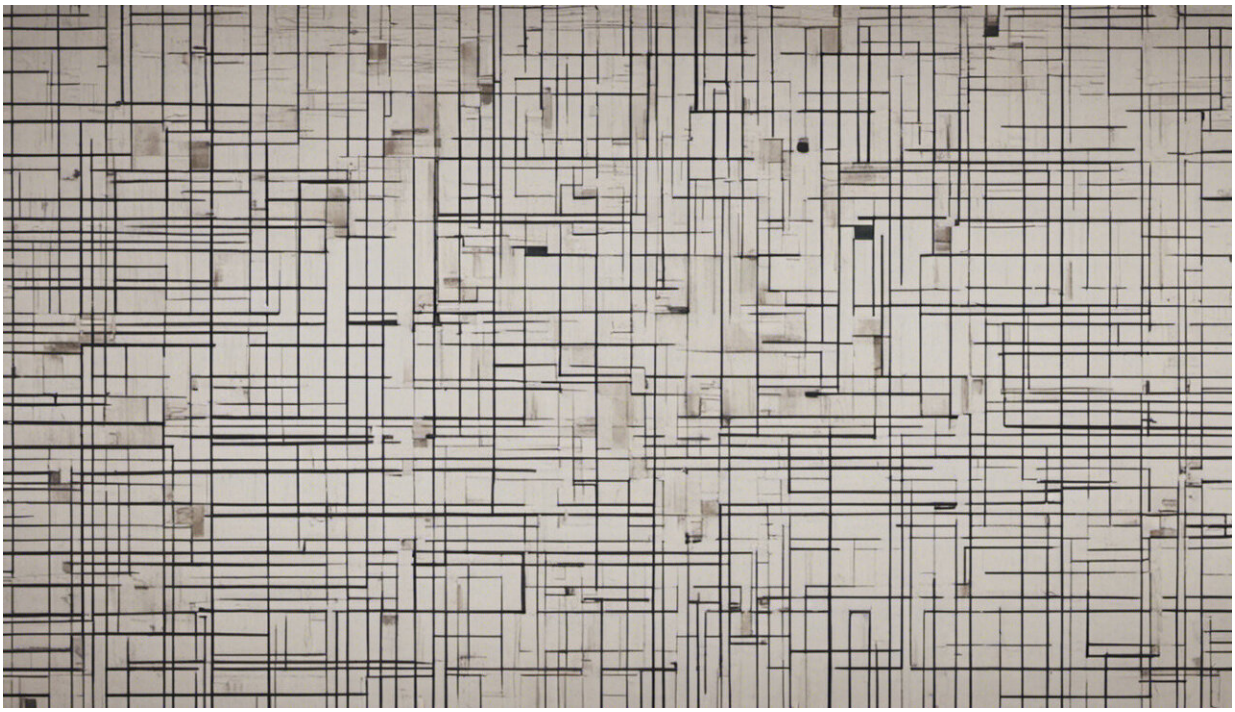
Data sold to third parties

There are a few situations where mobile platform companies like Apple and Google have let people exercise some control over data collection.

For example, both companies' mobile operating systems let users turn off location services, such as GPS tracking. Ideally, this should prevent most apps from collecting your location – but it doesn't always. Further, it does nothing if your mobile provider resells your phone's location information to third parties.

App makers are also able to persuade users not to turn off location services, again with take-it-or-leave-it notifications. When managing privileges for iOS apps, users get to choose whether the app can access the phone's location "always," "while using the app" or "never."

But changing the setting can trigger a discouraging message: "We need your location information to improve your experience," says one app. Users are not asked other important questions, like whether they approve of the app selling their location history to other companies.



Credit: AI-generated image (disclaimer)

And many users don't know that even when their name and contact information is removed from location data, even a modest location history can reveal their home addresses and the places they visit most, offering clues to their identities, medical conditions and personal relationships.

Why people don't opt out

Websites and apps make it difficult, and sometimes impossible, for most people to say no to aggressive surveillance and data collection practices. In my role as a scholar of human-computer interaction, one issue I study is the power of defaults.

When companies set a default in a system, such as "location services set to on," people are unlikely to change it, especially if they are unaware there are other options they could choose.

Further, when it is inconvenient to change the location services, as is the case on both iOS and Android systems today, it's even less likely that people will opt out of location collection – even when they dislike it.

Companies' take-it-or-leave-it privacy policies and default choices for users' privacy settings have created an environment where people are unaware that their lives are being subjected to minute-by-minute surveillance.

They're also mostly not aware that information that could identify them individually is resold to create ever-more-targeted advertising. Yet the companies can legally, if not ethically, claim that everyone agreed to it.

Overcoming the power of defaults

Privacy researchers know that people dislike these practices, and that many would stop using these services if they understood the extent of the data collection. If invasive surveillance is the price of using free services, many would rather pay or at least see companies held to stronger data collection regulations.

The companies know this too, which is why, I argue, they use a form of coercion to ensure participation.

Until the U.S. has regulations that, at a minimum, require companies to ask for explicit consent, individuals will need to know how to protect their privacy. Here are my three suggestions:

- Start by learning how to turn off location services on your iPhone

or Android device.

- Turn location on only when using an app that clearly needs location to function, such as a map.
- Avoid apps, such as Facebook Mobile, that dig deeply into your phone for as much personal information as possible; instead, use a browser with a private mode, like Firefox, instead.

Don't let default settings reveal more about you than you want.

Provided by The Conversation