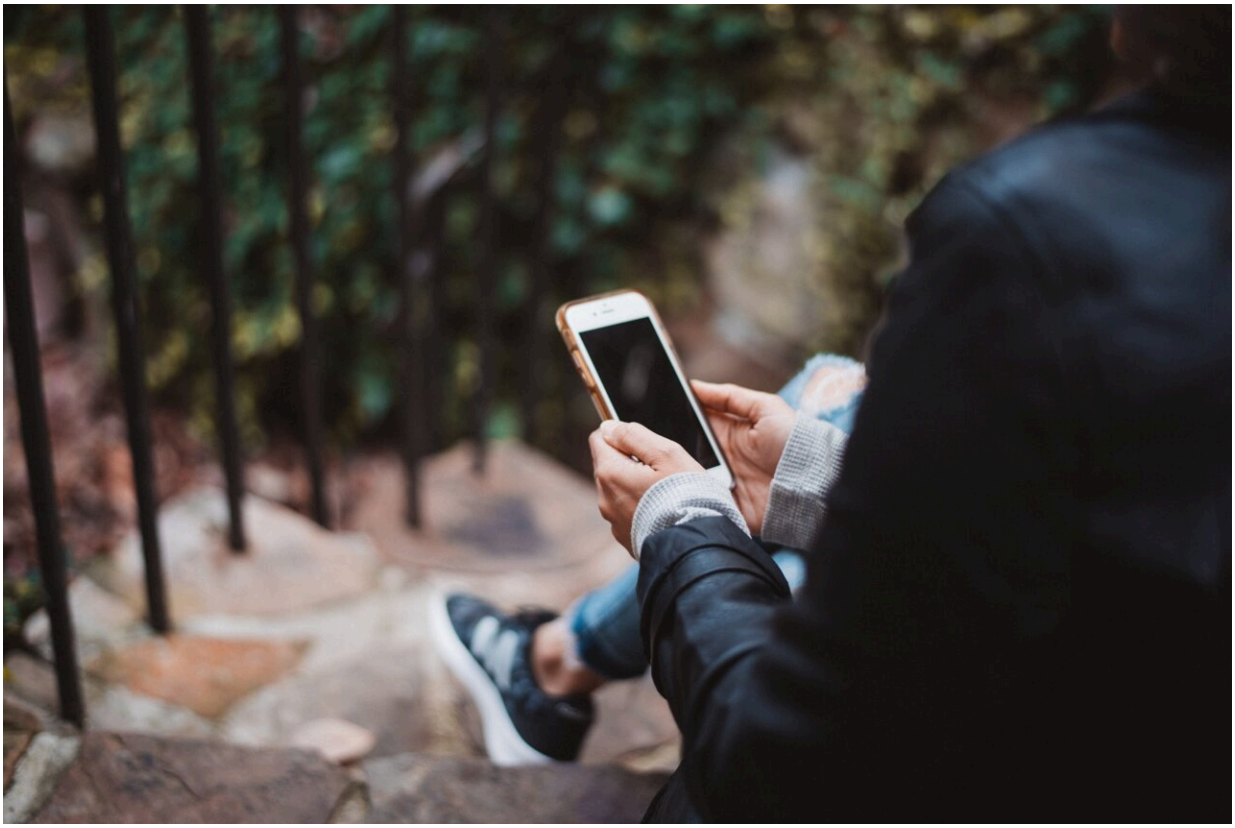
From call records to sensors, your phone reveals more about you than you think

August 31 2022, by Susan Landau



Credit: Unsplash/CC0 Public Domain

The Federal Trade Commission filed suit against Kochava Inc. on Aug. 29, 2022, accusing the data broker of selling geolocation data from hundreds of millions of mobile devices. Consumers are often unaware

that their location data is being sold and that their past movements can be tracked, according to the commission.

The FTC's suit specified that Kochava's data can be used to track consumers to sensitive locations, including "to identify which consumers' mobile devices visited reproductive health clinics."

When the U.S. Supreme Court overturned Roe v. Wade on June 24, 2022, many people seeking abortion care found themselves in legal jeopardy. Numerous state laws criminalizing abortion thrust the perilous state of personal privacy into the spotlight. As a cybersecurity and privacy researcher, I've seen how readily people's movements and activities can be tracked.

If people want to travel incognito to an abortion clinic, according to well-meaning advice, they need to plan their trip the way a CIA operative might—and get a burner phone. Unfortunately, that still wouldn't be good enough to guarantee privacy.

Using a maps app to plan a route, sending terms to a search engine and chatting online are ways that people actively share their personal data. But mobile devices share far more data than just what their users say or type. They share information with the network about whom people contacted, when they did so, how long the communication lasted and what type of device was used. The devices must do so in order to connect a phone call or send an email.

Who's talking to whom

When NSA whistleblower Edward Snowden disclosed that the National Security Agency was collecting Americans' telephone call metadata—the Call Detail Records—in bulk in order to track terrorists, there was a great deal of public consternation. The public was rightly concerned

about loss of privacy.

Researchers at Stanford later showed that call detail records plus publicly available information could reveal sensitive information, such as whether someone had a heart problem and their arrhythmia monitoring device was malfunctioning or whether they were considering opening a marijuana dispensary. Often you don't have to listen in to know what someone is thinking or planning. Call detail records—who called whom and when—can give it all away.

The transmission information in internet-based communications—IP-packet headers—can reveal even more than call detail records do. When you make an encrypted voice call over the internet—a Voice over IP call—the contents may be encrypted but information in the packet header can nonetheless sometimes divulge some of the words you're speaking.

A pocket full of sensors

That's not the only information given away by your communications device. Smartphones are computers, and they have many sensors. For your phone to properly display information, it has a gyroscope and an accelerometer; to preserve battery life, it has a power sensor; to provide directions, a magnetometer.

Just as communications metadata can be used to track what you're doing, these sensors can be used for other purposes. You might shut off GPS to prevent apps from tracking your location, but data from a phone's gyroscope, accelerometer and magnetometer can also track where you're going.

This sensor data could be attractive to businesses. For example, Facebook has a patent that relies on the different wireless networks near

a user to determine when two people might have been close together frequently—at a conference, riding a commuter bus—as a basis for providing an introduction. Creepy? You bet. As someone who rode the New York City subways as a young girl, the last thing I want is my phone introducing me to someone who has repeatedly stood too close to me in a subway car.

Uber knows that people really want a ride when their battery power is low. Is the company checking for that data and charging more? Uber claims not, but the possibility is there.

And it's not just apps that get access to this data trove. Data brokers get this information from the apps, then compile it with other data and provide it to companies and governments to use for their own purposes. Doing so can circumvent legal protections that require law enforcement to go to court before they obtain this information.

Beyond consent

There's not a whole lot users can do to protect themselves. Communications metadata and device telemetry—information from the phone sensors—are used to send, deliver and display content. Not including them is usually not possible. And unlike the search terms or map locations you consciously provide, metadata and telemetry are sent without you even seeing it.

Providing consent isn't plausible. There's too much of this data, and it's too complicated to decide each case. Each application you use—video, chat, web surfing, email—uses metadata and telemetry differently. Providing truly informed consent that you know what information you're providing and for what use is effectively impossible.

If you use your mobile phone for anything other than a paperweight,

your visit to the cannabis dispensary and your personality—how extroverted you are or whether you're likely to be on the outs with family since the 2016 election—can be learned from metadata and telemetry and shared.

That's true even for a burner phone bought with cash, at least if you plan on turning the phone on. Do so while carrying your regular phone and you'll have given away that the two phones are associated—and perhaps even that they belong to you. As few as four location points can identify a user, another way your burner phone can reveal your identity. If you're driving with someone else, they'd have to be equally careful or their phone would identify them—and you. Metadata and telemetry information reveals a remarkable amount about you. But you don't get to decide who gets that data, or what they do with it.

The reality of technological life

There are some constitutional guarantees to anonymity. For example, the Supreme Court held that the right to associate, guaranteed by the First Amendment, is the right to associate privately, without providing membership lists to the state. But with smartphones, that's a right that's effectively impractical to exercise. it's nearly impossible to function without a mobile phone. Paper maps and public payphones have virtually disappeared. If you want to do anything—travel from here to there, make an appointment, order takeout or check the weather—you all but need a smartphone to do so.

It's not just people who might be seeking abortions whose privacy is at risk from this data that phones shed. It could be your kid applying for a job: For instance, the company could check location data to see if they are participating in political protests. Or it could be you, when the gyroscope, accelerometer and magnetometer data gives away that you and your co-worker went to the same hotel room at night.

There's a way to solve this chilling scenario, and that's for laws or regulations to require that the data you provide to send and receive communications—TikTok, SnapChat, YouTube—is used just for that, and nothing else. That helps the people going for abortions—and all the rest of us as well.

Provided by The Conversation