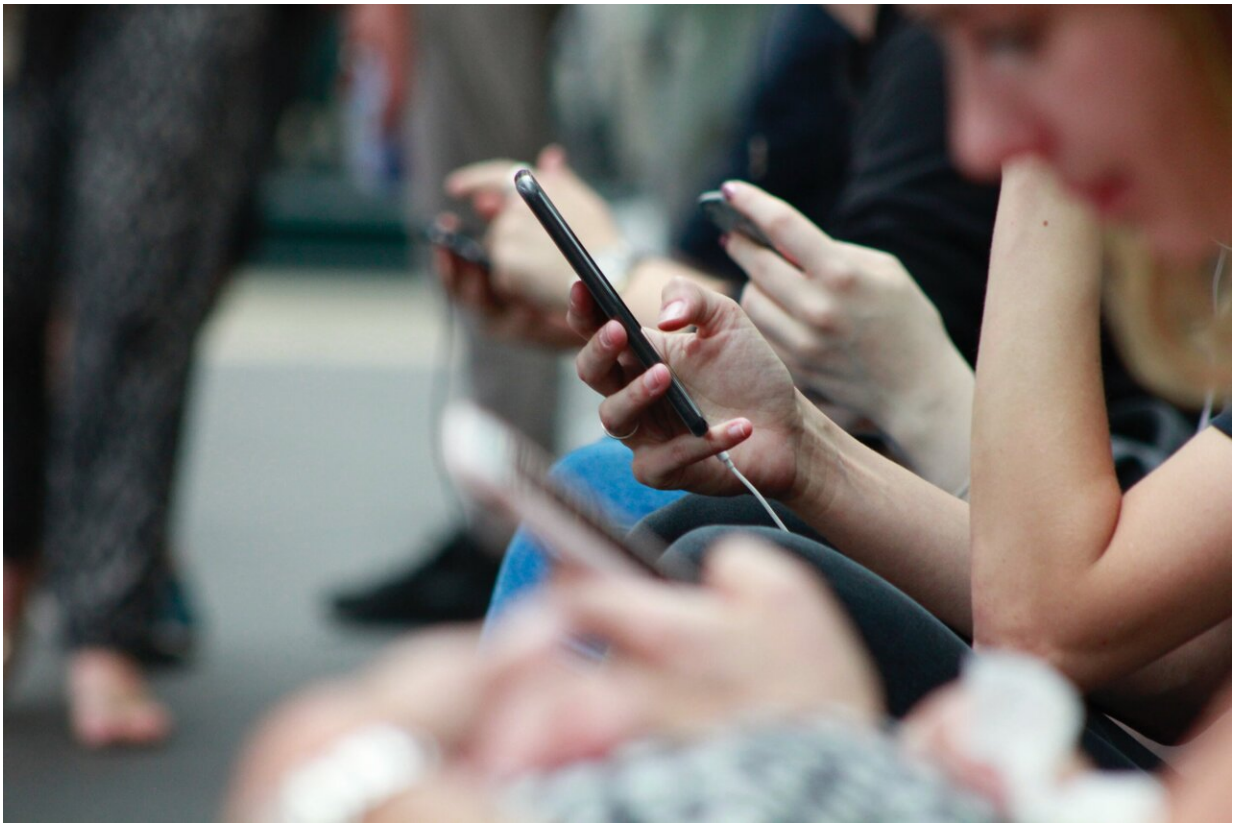
Is your mobile provider tracking your location? This new technology could stop it.

August 12 2021



Credit: Unsplash/CC0 Public Domain

Right now, there is a good chance your phone is tracking your location—even with GPS services turned off. That's because, to receive service, our phones reveal personal identifiers to cell towers owned by

major network operators. This has led to vast and largely unregulated data-harvesting industries based around selling users' location data to third parties without consent.

For the first time, researchers at the University of Southern California (USC) Viterbi School of Engineering and Princeton University have found a way to stop this privacy breach using existing cellular networks. The new system, presented at USENIX Security conference on Aug. 11, protects users' mobile privacy while providing normal mobile connectivity.

The new architecture, called "Pretty Good Phone Privacy" or PGPP, decouples phone connectivity from authentication and billing by anonymizing personal identifiers sent to cell towers. The software-based solution, described by the researchers as an "architecture change," does not alter cellular network hardware.

"We've unwittingly accepted that our phones are tracking devices in disguise, but until now we've had no other option—using mobile devices meant accepting this tracking," said study co-author Barath Raghavan, an assistant professor in computer science at USC. "We figured out how to decouple authentication from connectivity and ensure privacy while maintaining seamless connectivity, and it is all done in software."

Decoupling authentication and phone connectivity

Currently, for your phone to work, the network has to know your location and identify you as paying customer. As such, both your identity and location data are tracked by the device at all times. Data brokers and major operators have taken advantage of this system to profit off revealing sensitive user data—to date, in the United States, there are no federal laws restricting the use of location data.

"Today, whenever your phone is receiving or sending data, radio signals go from your phone to the cell tower, then into the network," said Raghavan. "The networks can scoop up all that data and sell it to companies or information-for-hire middlemen. Even if you stop apps tracking your location, the phone still talks to the tower, which means the carrier knows where you are. Until now, it seemed like a fundamental thing we could never get around."

But Raghavan, with study co-author Paul Schmitt who recently joined USC's Information Sciences Institute from Princeton University, found a way: They decoupled what's known as authentication—who you are—from your phone connectivity. The key finding: There is no reason why your personal identifier has to grant you network connectivity.

Their new system works by breaking the direct line of communication between the user's cellphone and the cell tower. Instead of sending a personally identifiable signal to the cell tower, it sends an anonymous "token." It does this by using a mobile virtual network operator, such as Cricket or Boost, as a proxy or intermediary.

"The key is—if you want to be anonymous, how do they know you're a paying customer?" said Raghavan. "In the protocol we developed, the user pays the bills, and gets a cryptographically signed token from the provider, which is anonymous. Now the identity in a specific location is separated from the fact that there is a phone at that location."

Restoring control

The duo, who have launched a startup called Invisv, prototyped and tested everything with real phones in the lab. Crucially, their approach adds almost zero latency and doesn't introduce new bottlenecks, avoiding performance and scalability problems of other anonymity networks. The service could handle tens of millions of users on a single server and

would be deployed seamlessly to customers through the network operator.

Since the system works by stopping a phone from identifying its user to the cell tower, all other location-based services—such as searching for the nearest gas station, or contact tracing—still work as usual. The researchers hope the technology will be accepted by major networks as default, particularly with mounting legal pressure to adopt new privacy measures.

"For the first time in human history, almost every single human being on the planet can be tracked in real-time," said Raghavan. "Until now, we had to just silently accept this loss of control over our own data—we believe this new measure will help to restore some of that control."

More information: Pretty Good Phone Privacy, arXiv:2009.09035 [cs.NI] arxiv.org/abs/2009.09035

Provided by University of Southern California