Surveillance is pervasive: Yes, you are being watched, even if no one is looking for you

July 25 2022, by Peter Krapp

Credit: Pixabay/CC0 Public Domain

The U.S. has the largest number of surveillance cameras per person in the world. Cameras are omnipresent on city streets and in hotels, restaurants, malls and offices. They're also used to screen passengers for

the Transportation Security Administration. And then there are smart doorbells and other home security cameras.

Most Americans are aware of video surveillance of public spaces. Likewise, most people know about online tracking—and want Congress to do something about it. But as a researcher who studies digital culture and secret communications, I believe that to understand how pervasive surveillance is, it's important to recognize how physical and digital tracking work together.

Databases can correlate location data from smartphones, the growing number of private cameras, license plate readers on police cruisers and toll roads, and facial recognition technology, so if law enforcement wants to track where you are and where you've been, they can. They need a warrant to use cellphone search equipment: Connecting your device to a mobile device forensic tool lets them extract and analyze all your data if they have a warrant.

However, private data brokers also track this kind of data and help surveil citizens—without a warrant. There is a large market for personal data, compiled from information people volunteer, information people unwittingly yield—for example, via mobile apps—and information that is stolen in data breaches. Among the customers for this largely unregulated data are federal, state and local law enforcement agencies.

How you are tracked

Whether or not you pass under the gaze of a surveillance camera or license plate reader, you are tracked by your mobile phone. GPS tells weather apps or maps your location, Wi-Fi uses your location, and cell-tower triangulation tracks your phone. Bluetooth can identify and track your smartphone, and not just for COVID-19 contact tracing, Apple's "Find My" service, or to connect headphones.

People volunteer their locations for ride-sharing or for games like Pokemon Go or Ingress, but apps can also collect and share location without your knowledge. Many late-model cars feature telematics that track locations—for example, OnStar or Bluelink. All this makes opting out impractical.

The same thing is true online. Most websites feature ad trackers and third-party cookies, which are stored in your browser whenever you visit a site. They identify you when you visit other sites so advertisers can follow you around. Some websites also use key logging, which monitors what you type into a page before hitting submit. Similarly, session recording monitors mouse movements, clicks, scrolling and typing, even if you don't click "submit."

Ad trackers know when you browsed where, which browser you used, and what your device's internet address is. Google and Facebook are among the main beneficiaries, but there are many data brokers slicing and dicing such information by religion, ethnicity, political affiliations, social media profiles, income and medical history for profit.

Big Brother in the 21st century

People may implicitly consent to some loss of privacy in the interest of perceived or real security—for example, in stadiums, on the road and at airports, or in return for cheaper online services. But these trade-offs benefit individuals far less than the companies aggregating data. Many Americans are suspicious of government censuses, yet they willingly share their jogging routines on apps like Strava, which has revealed sensitive and secret military data.

In the post-Roe v. Wade legal environment, there are concerns not only about period tracking apps but about correlating data on physical movements with online searches and phone data. Legislation like the

recent Texas Senate Bill 8 anti-abortion law invokes "private individual enforcement mechanisms," raising questions about who gets access to tracking data.

In 2019, the Missouri Department of Health stored data about the periods of patients at the state's lone Planned Parenthood clinic, correlated with state medical records. Communications metadata can reveal who you are in touch with, when you were where, and who else was there—whether they are in your contacts or not.

Location data from apps on hundreds of millions of phones lets the Department of Homeland Security track people. Health wearables pose similar risks, and medical experts note a lack of awareness about the security of data they collect. Note the resemblance of your Fitbit or smartwatch to ankle bracelets people wear during court-ordered monitoring.

The most pervasive user of tracking in the U.S. is Immigration and Customs Enforcement (ICE), which amassed a vast amount of information without judicial, legislative or public oversight. Georgetown University Law Center's Center on Privacy and Technology reported on how ICE searched the driver's license photographs of 32% of all adults in the U.S., tracked cars in cities home to 70% of adults, and updated address records for 74% of adults when those people activated new utility accounts.

No one is watching the watchers

Nobody expects to be invisible on streets, at borders, or in shopping centers. But who has access to all that surveillance data, and how long it is stored? There is no single U.S. privacy law at the federal level, and states cope with a regulatory patchwork; only five states—California, Colorado, Connecticut, Utah and Virginia—have privacy laws.

It is possible to limit location tracking on your phone, but not to avoid it completely. Data brokers are supposed to mask your personally identifiable data before selling it. But this "anonymization" is meaningless since individuals are easily identified by cross-referencing additional data sets. This makes it easy for bounty hunters and stalkers to abuse the system.

The biggest risk to most people arises when there is a data breach, which is happening more often—whether it is a leaky app or careless hotel chain, a DMV data sale or a compromised credit bureau, or indeed a data brokering middleman whose cloud storage is hacked.

This illicit flow of data not only puts fuzzy notions of privacy in peril, but may put your addresses and passport numbers, biometric data and social media profiles, credit card numbers and dating profiles, health and insurance information, and more on sale.

Provided by The Conversation