Guess What? The Cops Can Buy Your Data Instead of Going to Court for It

A study by a Washington think tank notes that government agencies can work around legal limits by buying location and other data from outside brokers.

Rob Pegoraro

A new report offers a reminder you may resent: Government agencies don't need to bother getting a warrant for your data if they can just buy it.

Tech-policy types may not find much new in "Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers," released Thursday by the Center for Democracy & Technology. But its overall assessment—that data brokers continue to

provide law-enforcement and intelligence agencies with an efficient workaround to Fourth Amendment and other legal privacy protections—may upset many other Americans.

As this 51-page report observes in its introduction: "There is no clear limit on the potential availability of commercially acquired data that would typically require legal process to obtain."

Its authors—CDT staffers Sharon Bradford Franklin, Greg Nojeim, and Dhanaraj Thakur, plus human-rights lawyer and consultant Carey Shenkman—further note that this data procurement proceeds despite the Supreme Court's 2018 ruling in Carpenter v. United States that law-enforcement agencies must get a court warrant for a suspect's historical cell-site location information from wireless carriers.

For example, the report cites the FBI signing contracts with data broker Venntel to obtain location data for "pre-investigative activities" and Customs and Border Protection's deals with the same firm (remember that many legal rights don't apply at US borders).

But between vague app privacy policies, the fuzzier terms of data brokers, and deliberate opacity by government agencies about these transactions, the average citizen would struggle to learn how their data might have flowed from an app on their phone to a law-enforcement database.

(Unstated in CDT's report but worth pondering: Other governments can also buy this data, a point the Trump administration ignored while trying to call TikTok an instrument of Chinese spying.)

What to do about all this? CDT, a Washington-based nonprofit supported mostly by foundation and corporate donations, supports passage of The Fourth Amendment Is Not For Sale Act (S.1265), a bill from Sen. Ron Wyden

(D.-Ore.) that would ban these transactions. But the bill has gone nowhere since Wyden introduced it in April with bipartisan sponsorship led by Sen. Rand Paul (R.-Ky.).

Recommended by Our Editors

Need to Spoof Your Location? A VPN Can Help
So You've Been Pwned: What To Do When Your Private Data Goes Public
How to Turn Off Location Services and Stop Your iPhone Apps From Tracking You

CDT also endorses updating the Electronic Communications Privacy Act to address the role of data brokers. But Congress has yet to address even that 1986 law's grotesquely obsolete provisions allowing warrantless access to stored email—provisions that Google and other mail providers have quietly ignored for years, citing a circuit-court ruling invalidating them.

Should Congress continue to do nothing, you can do something by using the location-privacy features Apple and Google offer to cloak your location from your apps (and the advertising components in them). Both iOS and Android let you stop an app from checking your location in the background; last year's iOS 14 let iPhone users limit any app to knowing their approximate location, and Google's new Android 12 adds a similar control.

If you haven't checked out these options yet, now would be a great time to open your smartphone's Settings app.

Like What You're Reading?

Sign up for **Security Watch** newsletter for our top privacy and security stories delivered right to your inbox.