



Fact Sheet: Closing the Data Broker Loophole

The Problem

The government is circumventing clearly established Fourth Amendment rights by using taxpayer dollars to buy access to our private cell phone data.

In today's digital age, our Fourth Amendment rights are at significant risk. Owning a cell phone has become an essential part of living in our modern society, and most Americans carry theirs everywhere they go. To function, smartphones regularly connect with communications networks and geolocation services, creating detailed maps of individuals' daily movements. This cell phone location data can reveal our most sensitive activities and interactions: personal relationships, political and religious views, medical histories, and other intimate details about our lives.¹ Protecting this information from government surveillance can be especially important for government dissidents, marginalized communities, and those frequently confronted with undue police scrutiny.²

Normally, if law enforcement officers want to access your cell phone location data, they need a warrant. But a glaring loophole in current law allows law enforcement and government intelligence agencies to pay third party data brokers to gain access to your private, sensitive cell phone data — no warrant needed. The government often purchases the personal cell phone location data of American citizens from these brokers, who collect this data and offer it up to the highest bidder. This is the equivalent of police bypassing the requirement to get a warrant to search someone's apartment by simply handing their landlord an envelope of cash.

Numerous federal agencies, including those in the departments of Defense, Homeland Security, Justice, Treasury, and others, have made these data purchases and undermined the rights of tens of millions of Americans in the process.³

¹ Jennifer Valentino-DeVries et al., "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret," *New York Times*, December 10, 2018, <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html?module=inline>.

² Don Bell, "We Built a Surveillance State. What Now?" Project On Government Oversight, August 20, 2024, <https://www.pogo.org/analyses/we-built-a-surveillance-state-what-now>.

³ Letter from Paul M. Nakasone, General, U.S. Army Director, to Ron Wyden, Senator, about the National Security Agency's use of commercially available information, December 11, 2023, https://www.wyden.senate.gov/imo/media/doc/signed_wyden_letter_to_dni_re_nsa_purchase_of_domestic_metadata_a_and_ftc_order_on_data_brokers_with_attachments.pdf; Shreya Tewari and Fikayo Walter-Johnson, "New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data," ACLU, <https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data>; Joseph Cox, "The DEA Abruptly Cut Off Its App Location Data Contract," *Vice*, December 7, 2020, <https://www.vice.com/en/article/dea-venntel-location-data/>; Byron Tau, "IRS Used Cellphone Location Data to Try to Find Suspects," *Wall Street Journal*, June 19, 2020, <https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815>.

Some of the key architects of artificial intelligence (AI) have warned how the advent of AI dramatically heightens the risk of warrantless mass surveillance.⁴ Congress must act now to end warrantless location tracking and prevent the government from paying to bypass our Fourth Amendment protections.

The Solution

Adopt a clear and consistent standard that prevents the government from purchasing cell phone location and metadata to which they are not otherwise entitled as part of the reauthorization of Section 702 of FISA.

In 2024, a bipartisan majority in the U.S. House passed the Fourth Amendment Is Not For Sale Act. This Congress, several pieces of legislation that address the data broker loophole have support, such as the Government Surveillance Reform Act, SAFE Act (S.3893), and Protect Liberty and End Warrantless Surveillance Act.

Simply put, Congress must prohibit law enforcement and intelligence agencies from purchasing information that the government would otherwise need a warrant, court order, or subpoena to obtain.

Closing the data broker loophole would not prohibit law enforcement from accessing and using location data to apprehend a suspect in a criminal investigation or otherwise protecting the public's safety. It simply requires law enforcement to follow the Fourth Amendment, regardless of the means they are using to access our information.⁵

According to a 2023 YouGov poll, 80% of Americans agree government agencies should “obtain warrants before purchasing location information, internet records, and other sensitive data about people in the U.S. from data brokers.”

The government should not be able to buy its way around the Bill of Rights by purchasing the personal location data of millions of Americans from third party brokers. This bill would finally put a stop to a practice that is putting us at risk, circumventing clear privacy rules, and making unscrupulous data brokers rich. If we fail to establish these safeguards to protect our privacy in the age of big data and artificial intelligence, it will fundamentally harm Fourth Amendment rights and hamper the freedoms and activities they safeguard.

Contact

Don Bell, Policy Counsel, The Constitution Project at the Project On Government Oversight (POGO), at Donald.Bell@pogo.org.

⁴See Anthropic, “Statement from Dario Amodei on our discussions with the Department of War,” Press Release, February 26, 2026, <https://www.anthropic.com/news/statement-department-of-war>; Tara Deschamps, The Canadian Press, “AI surveillance risks among the technology’s most urgent problems: Hinton,” June 19, 2024, <https://financialpost.com/news/hinton-ai-surveillance-risks>.

⁵ Demand Progress Education Fund, “New Polling: As Mass Surveillance Debate Reaches Final Stages in Congress, Americans Demonstrate Overwhelming Support for Increased Privacy Protections,” Press Release, December 14, 2023, <https://demandprogresseducationfund.org/new-polling-as-mass-surveillance-debate-reaches-final-stages-in-congress-americans-demonstrate-overwhelming-support-for-increased-privacy-protections/>.