Issue Brief: The Fourth Amendment Is Not For Sale Act

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. In order 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. Protecting this information from undue interference can be especially important for people of color, government dissidents, marginalized communities, and those frequently confronted with undue police scrutiny.

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 can (and often does) purchase the personal cell phone location data of American citizens from unregulated brokers who offer it up to the highest bidder, all without any court oversight. 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 the FBI, DHS, ICE, IRS, DEA, and the U.S. Military, have made these data purchases and undermined the rights of tens of millions of Americans in the process. Yet, we have no way of knowing whose data has been purchased or how that data has been used by the government. Congress must take action to end warrantless location tracking and prevent the government from paying to bypass our Fourth Amendment protections.

The Fourth Amendment is Not For Sale Act creates a clear and consistent standard and prevents the government from purchasing personal cell phone location data to which they are not otherwise entitled.

The Fourth Amendment is Not For Sale Act (S. 1265; H.R. 2738), recently introduced by Sen. Wyden (D-OR), Rep. Nadler (D-NY), and a bipartisan group of co-sponsors, closes the loophole that allows law enforcement entities to buy Americans’ personal location information from data brokers.
Specifically, the bill:

- Prevents law enforcement from circumventing the Fourth Amendment by simply buying personal cell phone data they aren’t otherwise entitled to access.
- Requires the government to get a court order to compel data brokers to disclose data.
- Bans police from buying data private companies obtained through deception or malicious hacking.

Importantly, this bill does not prohibit law enforcement from accessing and using location data to track down a suspect in a criminal investigation or otherwise protect the public’s safety. It simply holds law enforcement to the same legal standard, regardless of the means they are using to access our information.

**The bill has strong support from a bipartisan group of legislators, as well as a diverse coalition of 30 organizations spanning the ideological spectrum.**

The Fourth Amendment is Not For Sale Act has considerable support from lawmakers on both sides of the aisle. A broad coalition of civil liberties, civil rights, technology, and free speech groups have also endorsed the bill. This coalition includes:


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

**For more information, please contact Jake Laperruque, Senior Policy Counsel for the Constitution Project at the Project On Government Oversight (POGO), at jlaperruque@pogo.org or (973) 951-6344.**