Big Brother watching? Government agencies buying cell phone, internet data to track Americans

By Aaron Kliegman

Updated: September 28, 2022 - 11:05pm

Article Dig In

In a little noted trend, law enforcement agencies at every level of government are increasingly buying data from private, third-party data brokers on Americans' phone and internet activities in order to track them, often without a warrant.

While proponents say this practice provides critical help for investigations, critics argue it poses a serious violation of civil liberties that needs to be addressed through legislation.

One of the latest revelations about this controversial public-private partnership came from the Electronic Frontier Foundation, a nonprofit dedicated to "defending civil liberties in the digital world."

EFF recently obtained a trove of records through Freedom of Information Act requests on local and state police departments, as well as federal entities, purchasing a cellphone tracking tool that can monitor people's movements going back months in time.

The tool, Fog Reveal, is a product of the company Fog Data Science, which claims it has "billions" of data points about "over 250 million" devices that can be used to learn where people work, live, and associate.

Fog has past or ongoing contractual relationships with at least 18 local, state, and federal law enforcement clients, according to the documents reviewed by EEF.

Law enforcement has used the Fog data for a wide range of investigations, from the murder of a nurse in Arkansas to tracking the movements of a potential participant in the Jan. 6 Capitol riot, the Associated Press reported.

According to Fog, it's providing a helpful service so law enforcement agencies can better do their jobs.

"Local law enforcement is at the front lines of trafficking and missing persons cases, yet these departments are often behind in technology adoption," Matthew Broderick, a Fog managing partner, told the AP. "We fill a gap for underfunded and understaffed departments."

Others see the arrangement as a violation of Americans' civil liberties and the U.S. Constitution.

"Reporting and a recent investigation by EFF confirms that law enforcement across the country is regularly getting access to our private movements — with the ability to retrace our daily lives — often without a warrant," Aaron Mackey, senior staff attorney for EEF, told Just the News. "This is an end-run around the Fourth Amendment and permits broad surveillance that can sweep up anyone who happens to be near the scene of a crime."

Law enforcement agencies are getting much of this information from data brokers such as Fog, which harvest consumers' location data from app developers and then sell it to the agencies.

Specifically, various smartphone apps request location access in order to enable certain features. Once a person grants that access, the app is able to share it with other parties. Data brokers strike deals with the app developers — or with other data brokers — through various arrangements to obtain the information and sell it.

Many private entities, such as hedge funds and marketing firms, buy this location data for business purposes. However, other clients are from the government — namely federal, state, and local law enforcement, as well as military and intelligence agencies.

The government's interest in such data extends beyond phones to internet usage.

Multiple branches of the U.S. military have bought access to an internet monitoring tool that claims to cover over 90% of the world's internet traffic and can also provide access to people's email data, browsing history, and other information such as their sensitive internet cookies, according to documents reviewed by Vice last week.

The documents reveal the sale and use of a monitoring tool called Augury, which is developed by the cybersecurity firm Team Cymru and bundles a massive amount of data together and makes it available to government and corporate customers as a paid service.

Vice found that the U.S. Navy, Army, Cyber Command, and the Defense Counterintelligence and Security Agency have collectively paid at least $3.5 million to access Augury, allowing them to track internet usage and access large amounts of sensitive information.

In a letter last week to the inspectors general for the Justice, Defense, and Homeland Security departments, Sen. Ron Wyden (D-Ore.) wrote that a whistleblower contacted his office concerning the alleged warrantless use and purchase of this data from Augury by NCIS, a civilian law enforcement agency that's part of the Navy. According to Wyden, the whistleblower came to him after filing a complaint through the official reporting process with the Pentagon.

The purpose of Wyden's letter was to request the the agency watchdogs investigate the warrantless purchase of Americans' internet traffic data. Wyden expressed concern that by obtaining information from third-party data brokers and avoiding any judicial review process, government agencies were circumventing the Fourth Amendment's warrant requirements, which are meant to protect against unreasonable searches and seizures.

Last month, the House approved changes to next year's military budget requiring the Defense Department to disclose any purchases of smartphone or web browsing data that would normally require a warrant.

Government watchdogs have previously addressed the issue of warrants. Last year, for example, J. Russell George, inspector general of the Treasury Department, responded to an inquiry from Wyden and Sen. Elizabeth Warren (D-Mass.) about the IRS purchasing location data from data broker Venntel.

George wrote that IRS officials said they didn't need a warrant because "the information available had been voluntarily turned over through individual permissions" in the apps and devices they use.

The implication seems to be that when people allow location access and agree to all an app's terms, they also agree to potentially being surveilled by the government.

Among the largest government buyers of bulk location data is the Department of Homeland Security and several of its agencies, including Immigration and Customs Enforcement and Customs and Border Patrol.

DHS has paid millions of dollars in recent years to purchase, without warrants, cellphone location data from two companies to track the movements of both Americans and foreigners inside the U.S., at U.S. borders, and abroad, according to a report released by the American Civil Liberties Union in July.

Also in July, the Heritage Foundation filed a lawsuit against the Biden administration demanding the release of all documents related to DHS' contract with Babel Street, a Virginia-based data mining and surveillance company.

The contract concerns a Babel Street product capable of retrieving and copying data both from online sources and from apps running on the smartphones and other devices of billions of people worldwide.

In announcing its lawsuit, Heritage expressed concern about DHS working with private companies to monitor Americans' social media accounts and the prospect of government agencies searching and aggregating the data.

Other federal departments and agencies have partnered with data brokers. The FBI last year released its own contracts with Venntel, although they were heavily redacted. The documents showed the bureau paid $22,000 for a single license to the Venntel Portal.

For critics, legislation is necessary to ensure the government doesn't infringe on the rights of citizens.

"Law enforcement's exploitation of our private digital data is dangerous and unconstitutional," said Mackey. "This harmful surveillance is only possible because there is no federal law that ensures that everyone can control their private data. It's past time Congress acted to protect our private information from both private and government surveillance."

Some senators are reportedly pushing for legislation that would limit the ability of law enforcement agencies to buy data to track people's whereabouts without a warrant.

Many of the federal government purchases aren't meant to surveil Americans inside the U.S.

In one project, for example, researchers at Mississippi State University used a service provided by Babel Street to track movements around Russian missile test sites, including those of high-level diplomats. The U.S. Army funded the project.

The Iowa Air National Guard and U.S. Special Operations Command have also used information from data brokers for operations overseas.

Still, the potential for surveilling Americans has many prominent legal experts concerned.

"The only reason we permit private people to track you for business purposes is because we assume that it won't end up in government hands," renowned civil liberties lawyer Alan Dershowitz told the "Just the News, Not Noise" television show Tuesday. "If the government wanted to do the same thing, they'd need a warrant. I mentioned they tracked Mike Lindell He was hunting with his friends, and he was at Hardees — how did they find him? Did they buy data? Or did they have a GPS on him? Or did they track his cell phone? ...

"It's just too much Big Brother. And the connections now between private industry and the government is becoming one of the great issues of the 21st century: Google and Facebook and whether or not Google and Facebook have to take instructions from the government."