

Tech tool offers police 'mass surveillance on a budget'

Associated Press | September 2, 2022

by Garance Burke and Jason Dearen

Local law enforcement agencies from suburban Southern California to rural North Carolina have been using an obscure cellphone tracking tool, at times without search warrants, that gives them the power to follow people's movements months back in time, according to public records and internal emails obtained by The Associated Press.

Police have used "Fog Reveal" to search hundreds of billions of records from 250 million mobile devices, and harnessed the data to create location analyses known among law enforcement as "patterns of life," according to thousands of pages of records about the company.

Sold by Virginia-based Fog Data Science LLC, Fog Reveal has been used since at least 2018 in criminal investigations ranging from the murder of a nurse in Arkansas to tracing the movements of a potential participant in the Jan. 6 insurrection at the Capitol. The tool is rarely, if ever, mentioned in court records, something that defense attorneys say makes it harder for them to properly defend their clients in cases in which the technology was used.

The company was developed by two former high-ranking Department of Homeland Security officials under former President George W. Bush. It relies on advertising identification numbers, which Fog officials say are culled from popular cellphone apps such as Waze, Starbucks and hundreds of others that target ads based on a person's movements and interests, according to police emails. That information is then sold to companies like Fog.

"It's sort of a mass surveillance program on a budget," said Bennett Cyphers, a special adviser at the Electronic Frontier Foundation, a digital privacy rights advocacy group.

The documents and emails were obtained by EFF through Freedom of Information Act requests. The group shared the files with The AP, which independently found that Fog sold its software in about 40 contracts to nearly two dozen agencies, according to GovSpend, a company that keeps tabs on government spending. The records and AP's reporting provide the first public account of the extensive use of Fog Reveal by local police, according to analysts and legal experts who scrutinize such technologies.

Federal oversight of companies like Fog is an evolving legal landscape. On Monday, the Federal Trade Commission sued a data broker called Kochava that, like Fog, provides its clients with advertising IDs that authorities say can easily be used to find where a mobile device user lives, which violates rules the commission enforces. And there are bills before Congress now that, if passed, would regulate the industry.

"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, said in an email. "We fill a gap for underfunded and understaffed departments."

Because of the secrecy surrounding Fog, however, there are scant details about its use and most law enforcement agencies won't discuss it, raising concerns among privacy advocates that it violates the Fourth Amendment to the U.S. Constitution, which protects against unreasonable search and seizure.

What distinguishes Fog Reveal from other cellphone location technologies used by police is that it follows the devices through their advertising IDs, unique numbers assigned to each device. These numbers do not contain the name of the phone's user, but can be traced to homes and workplaces to help police establish pattern-of-life analyses.

“The capability that it had for bringing up just anybody in an area whether they were in public or at home seemed to me to be a very clear violation of the Fourth Amendment,” said Davin Hall, a former crime data analysis supervisor for the Greensboro, North Carolina, Police Department. “I just feel angry and betrayed and lied to.”

Hall resigned in late 2020 after months of voicing concerns about the department’s use of Fog to police attorneys and the city council.

While Greensboro officials acknowledged Fog’s use and initially defended it, the police department said it allowed its subscription to expire earlier this year because it didn’t “independently benefit investigations.”

But federal, state and local police agencies around the U.S. continue to use Fog with very little public accountability. Local police agencies have been enticed by Fog’s affordable price: It can start as low as \$7,500 a year. And some departments that license it have shared access with other nearby law enforcement agencies, the emails show.

Police departments also like how quickly they can access detailed location information from Fog. Geofence warrants, which tap into GPS and other sources to track a device, are accessed by obtaining such data from companies, like Google or Apple. This requires police to obtain a warrant and ask the tech companies for the specific data they want, which can take days or weeks.

Using Fog’s data, which the company claims is anonymized, police can geofence an area or search by a specific device’s ad ID numbers, according to a user agreement obtained by AP. But, Fog maintains that “we have no way of linking signals back to a specific device or owner,” according to a sales representative who emailed the California Highway Patrol in 2018, after a lieutenant asked whether the tool could be legally used.

Despite such privacy assurances, the records show that law enforcement can use Fog's data as a clue to find identifying information. "There is no (personal information) linked to the (ad ID)," wrote a Missouri official about Fog in 2019. "But if we are good at what we do, we should be able to figure out the owner."

Fog's Broderick said in an email that the company does not have access to people's personal information, and draws from "commercially available data without restrictions to use," from data brokers "that legitimately purchase data from apps in accordance with their legal agreements." The company refused to share information about how many police agencies it works with.

"We are confident Law Enforcement has the responsible leadership, constraints, and political guidance at the municipal, state, and federal level to ensure that any law enforcement tool and method is appropriately used in accordance with the laws in their respective jurisdictions," Broderick said in the email.

"Search warrants are not required for the use of the public data," he added Thursday, saying that the data his product offers law enforcement is "lead data" and should not be used to establish probable cause.

Kevin Metcalf, a prosecutor in Washington County, Arkansas, said he has used Fog Reveal without a warrant, especially in "exigent circumstances." In these cases, the law provides a warrant exemption when a crime-in-process endangers people or an officer.

Metcalf also leads the National Child Protection Task Force, a nonprofit that combats child exploitation and trafficking. Fog is listed on its website as a task force sponsor and a company executive chairs the nonprofit's board. Metcalf said Fog has been invaluable to cracking missing children cases and homicides.

“We push the limits, but we do them in a way that we target the bad guys,” he said. “Time is of the essence in those situations. We can’t wait on the traditional search warrant route.”

Fog was used successfully in the murder case of 25-year-old nurse Sydney Sutherland, who had last been seen jogging near Newport, Arkansas, before she disappeared, Metcalf said.

Police had little evidence to go on when they found her phone in a ditch, so Metcalf said he shared his agency’s access to Fog with the U.S. Marshals Service to figure out which other devices had been nearby at the time she was killed. He said Fog helped lead authorities to arrest a farmer in Sutherland’s rape and murder in August 2020, but its use was not documented in court records reviewed by AP.

Cyphers, who led EFF’s public records work, said there hasn’t been any previous record of companies selling this kind of granular data directly to local law enforcement.

“We’re seeing counties with less than 100,000 people where the sheriff is using this extremely high tech, extremely invasive, secretive surveillance tool to chase down local crime,” Cyphers said.

One such customer is the sheriff’s office in rural Rockingham County, North Carolina, population 91,000 and just north of Greensboro, where Hall still lives. The county bought a one-year license for \$9,000 last year and recently renewed it.

“Rockingham County is tiny in terms of population. It never ceases to amaze me how small agencies will scoop up tools that they just absolutely don’t need, and nobody needs this one,” Hall said.

Sheriff’s spokesman Lt. Kevin Suthard confirmed the department recently renewed its license but declined to offer specifics about the use of Fog Reveal or how the office protects individuals’ rights.

“Because it would then be less effective as criminals could be cognizant that we have the device and adjust their commission of the crimes accordingly. Make sense?” Suthard said.

Fog has aggressively marketed its tool to police, even beta testing it with law enforcement, records show. The Dallas Police Department bought a Fog license in February after getting a free trial and “seeing a demonstration and hearing of success stories from the company,” Senior Cpl. Melinda Gutierrez, a department spokeswoman, said in an email.

Fog’s tool is accessed through a web portal. Investigators can enter a crime scene’s coordinates into the database, which brings back search results showing a device’s Fog ID, which is based on its unique ad ID number.

Police can see which device IDs were found near the location of the crime. Detectives or other officers can also search the location for IDs going forward from the time of the crime and back at least 180 days, according to the company’s user license agreement.

The emails and Fog’s Broderick contend the tool can actually search back years, however. Emails from a Fog representative to Florida and California law enforcement agencies said the tool’s data stretched back as far as June 2017. On Thursday Broderick, who had previously refused to address the question, said it “only has a three year reach back.”

While the data does not directly identify who owns a device, the company often gives law enforcement information it needs to connect it to addresses and other clues that help detectives figure out people’s identities, according to company representatives’ emails.

It is unclear how Fog makes these connections, but a company it refers to as its “data partner” called Venntel, Inc. has access to an even greater trove of users’ mobile data.

Venntel is a large broker that has supplied location data to agencies such as Immigration and Customs Enforcement and the FBI. The Department of Homeland Security's watchdog is auditing how the offices under its control have used commercial data. That comes after some Democratic lawmakers asked it to investigate U.S. Customs and Border Protection's use of Venntel data to track people without a search warrant in 2020. The company also has faced congressional inquiries about privacy concerns tied to federal law enforcement agencies' use of its data.

Venntel and Fog work closely together to aid police detectives during investigations, emails show. Their marketing brochures are nearly identical, too, and Venntel staff has recommended Fog to law enforcement, according to the emails. Venntel said "the confidential nature of our business relationships" prevented it from responding to AP's specific questions, and Fog would not comment on the relationship.

While Fog says in its marketing materials that it collects data from thousands of apps, like Starbucks and Waze, companies are not always aware of who is using their data. Venntel and Fog can collect billions of data points filled with detailed information because many apps embed invisible tracking software that follows users' behavior. This software also lets the apps sell customized ads that are targeted to a person's current location. In turn, data brokers' software can Hoover up personal data that can be used for other purposes.

Prior to publication, Fog's Broderick refused to say how the company got data from Starbucks and Waze. But on Thursday, he said he did not know how data aggregators collected the information Fog Reveal draws from, or the specific apps from which the data was drawn.

For their part, Starbucks and Waze denied any relationship to Fog. Starbucks said it had not given permission to its business partners to share customer information with Fog.

“Starbucks has not approved Ad ID data generated by our app to be used in this way by Fog Data Science LLC. In our review to date, we have no relationship with this company,” said Megan Adams, a Starbucks spokesperson.

“We have never had a relationship with Fog Data Science, have not worked with them in any capacity, and have not shared information with them,” a Waze spokesperson said.

Fog Data Science LLC is headquartered in a nondescript brick building in Leesburg, Virginia. It also has related entities in New Jersey, Ohio and Texas.

It was founded in 2016 by Robert Liscouski, who led the Department of Homeland Security’s National Cyber Security Division in the George W. Bush administration. His colleague, Broderick, is a former U.S. Marine brigadier general who ran DHS’ tech hub, the Homeland Security Operations Center, during Hurricane Katrina in 2005. A House bipartisan committee report cited Broderick among others for failing to coordinate a swift federal response to the deadly hurricane. Broderick resigned from DHS shortly thereafter.

In marketing materials, Fog also has touted its ability to offer police “predictive analytics,” a buzzword often used to describe high-tech policing tools that purport to predict crime hotspots. Liscouski and another Fog official have worked at companies focused on predictive analytics, machine learning and software platforms supporting artificial intelligence.

“It is capable of delivering both forensic and predictive analytics and near real-time insights on the daily movements of the people identified with those mobile devices,” reads an email announcing a Fog training last year for members of the National Fusion Center Association, which represents a network of intelligence-sharing partnerships created after the Sept. 11 attacks.

Fog's Broderick said the company had not invested in predictive applications, and provided no details about any uses the tool had for predicting crime.

Despite privacy advocates' concerns about warrantless surveillance, Fog Reveal has caught on with local and state police forces. It's been used in a number of high-profile criminal cases, including one that was the subject of the television program "48 Hours."

In 2017, a world-renowned exotic snake breeder was found dead, lying in a pool of blood in his reptile breeding facility in rural Missouri. Police initially thought the breeder, Ben Renick, might have died from a poisonous snake bite. But the evidence soon pointed to murder.

During its investigation, emails show the Missouri State Highway Patrol used Fog's portal to search for cellphones at Renick's home and breeding facility and zeroed in on a mobile device. Working with Fog, investigators used the data to identify the phone owner's identity: it was the Renicks' babysitter.

Police were able to log the babysitter's whereabouts over time to create a pattern of life analysis.

It turned out to be a dead-end lead. Renick's wife, Lynlee, later was charged and convicted of the murder.

Prosecutors did not cite Fog in a list of other tools they used in the investigation, according to trial exhibits examined by the AP.

But Missouri officials seemed pleased with Fog's capabilities, even though it didn't directly lead to an arrest. "It was interesting to see that the system did pick up a device that was absolutely in the area that day. Too bad it did not belong to a suspect!" a Missouri State Highway Patrol analyst wrote in an email to Fog.

In another high-profile criminal probe, records show the FBI asked state intelligence officials in Iowa for help with Fog as it investigated potential participants in the events at the U.S. Capitol on Jan. 6.

“Not definitive but still waiting to talk things over with a FOG rep,” wrote Justin Parker, deputy director of the Iowa Department of Public Safety, in an email to an FBI official in September 2021. It was unclear from the emails if Fog’s data factored into an arrest. Iowa officials did not respond and the FBI declined to comment.

Metcalf, the Arkansas prosecutor, has argued against congressional efforts to require search warrants when using technologies like Fog Reveal.

He believes Americans have given up any reasonable expectation of privacy when they use free apps and likens EFF’s objections to tech like Fog to a “cult of privacy.”

“I think people are going to have to make a decision on whether we want all this free technology, we want all this free stuff, we want all the selfies,” he said. “But we can’t have that and at the same time say, ‘I’m a private person, so you can’t look at any of that.’ That just seems crazy.”

Although he is not an official Fog employee, Metcalf said he would step in to lead training sessions including the tool for federal prosecutors, federal agencies and police, including the Chicago Police Department, the emails show.

That kind of hands-on service and word-of-mouth marketing in tight-knit law enforcement circles seems to have helped increase Fog’s popularity.

The Maryland State Police is among the many agencies that have had contracts for Fog Reveal, and records show investigators believed it had a lot of potential.

"Companies have receptors all over. Malls, shopping centers, etc. They're all around you," wrote Sgt. John Bedell of the Criminal Enforcement Division, in an email to a colleague. The agency purchased a year of access to Fog in 2018.

"Picture getting a suspect's phone then in the extraction being able to see everywhere they'd been in the last 18 months plotted on a map you filter by date ranges," wrote Bedell. "The success lies in the secrecy."

Elena Russo, a spokesperson for the agency, confirmed it had a Fog license previously but that it had lapsed. "Unfortunately, it was not helpful in solving any crimes," she wrote in an email.

Still, as more local policing agencies sign up for Fog, some elected officials said they have been left in the dark. Several officials said there wasn't enough information to grasp what services Fog actually provides.

"Who is this company? What are the track records? What are the privacy protections?" asked Anaheim council member Jose Moreno, remembering his confusion about Fog during a 2020 council meeting. "That night our chief had very little information for us."

In Anaheim, the Fog license was paid for by a federal "Urban Area Security Initiative," DHS grants that help localities fund efforts to prevent terrorism. A police spokesman said the department has not used it.

Defense attorneys worry there are few legal restrictions on law enforcement's use of location data.

It's a gap police agencies exploit, and often don't disclose in court, said Michael Price, litigation director of the National Association of Criminal Defense Lawyers' Fourth Amendment Center.

"(Fog) is exceedingly rare to see in the wild because the cops often don't get warrants," said Price.

“Even if you do ask for (information) sometimes they say ‘We don’t know what you are talking about.’”

Privacy advocates worry Fog’s location tracking could be put to other novel uses, like keeping tabs on people who seek abortions in states where it is now illegal. These concerns were heightened when [a Nebraska woman was charged in August](#) with helping her teenage daughter end a pregnancy after investigators got hold of their Facebook messages.

Government’s use of location data is still being weighed by the courts, too. In 2018, the Supreme Court ruled that police generally need a warrant to look at records that reveal where cellphone users have been.

Nearly two years after walking off the crime data supervisor job with the Greensboro police force, Hall still worries about police surveillance in neighboring communities.

“Anyone with that login information can do as many searches as they want,” Hall said. “I don’t believe the police have earned the trust to use that, and I don’t believe it should be legal.”

AP National Writer Allen G. Breed contributed from Greensboro, North Carolina. Dearen reported from New York and Burke reported from San Francisco.

This reporting was produced in collaboration with researchers Janine Graham, Nicole Waddick and Jane Yang as well as the University of California, Berkeley’s Human Rights Center Investigations Lab and School of Law.

<https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef>