



Inside Fog Data Science, the Secretive Company Selling Mass Surveillance to Local Police

This article is part of EFF's investigation of location data brokers and Fog Data Science. Be sure to check out our [issue page on Location Data Brokers](#).

A data broker has been selling raw location data about individual people to federal, state, and local law enforcement agencies, EFF has learned. This personal data isn't gathered from cell phone towers or tech giants like Google — it's obtained by the broker via thousands of different apps on Android and iOS app stores as part of the larger [location data marketplace](#).

The company, Fog Data Science, has claimed in [marketing materials](#) that it has “billions” of data points about “over 250 million” devices and that its data can be used to learn about where its subjects work, live, and associate. Fog sells access to this data via a web application, called [Fog Reveal](#), that lets customers point and click to access [detailed histories](#) of regular people's lives. This panoptic surveillance apparatus is offered to [state highway patrols](#), [local police departments](#), and [county sheriffs](#) across the country for [less than \\$10,000 per year](#).

[The records received by EFF](#) indicate that Fog has past or ongoing contractual relationships with at least 18 local, state, and federal law enforcement clients; [several other agencies](#) took advantage of free trials of Fog's service. EFF learned about Fog after filing more than 100 public records requests over several months for documents pertaining to government relationships with location data brokers. EFF also shared these records with [The Associated Press](#).

Troublingly, those records show that Fog and [some law enforcement did not believe](#) Fog's surveillance implicated people's Fourth Amendment rights and required authorities to get a warrant.

In this post, we use public records to describe how Fog's service works, where its data comes from, who is behind the company, and why the service threatens people's privacy and safety. In [a subsequent post](#), we will dive deeper into how it is used by law enforcement around the country and explore the legal issues with its business model.

How does the service work?

In [materials provided to law enforcement](#), Fog states that it has access to a "near real-time" database of billions of geolocation signals derived from smartphones. It sells subscriptions to a service, which the company usually billed as "Fog Reveal," that lets law enforcement look up location data in its database through a website. The smartphone signals in Fog's database include [latitude, longitude, timestamp, and a device ID](#). The company [can access historical data](#) reaching back to at least June 2017.

[Fog's materials](#) describe how users can run two different queries:

1. "Area searches": This feature allows law enforcement to draw one or more shapes on a map and specify a time range they would like to search. The service will show a list of all cell-phone location signals (including location, time, and device ID) within the specified area(s) during that time. The records EFF obtained do not say how large an area Fog's Area searches are capable of covering with a single query.
2. "Device searches": Law enforcement can specify one or more devices they've identified and a time range, and Fog Reveal will return a list of location signals associated with each device. Fog's materials describe this capability as providing a person's "[pattern of life](#)," which allows authorities to identify "[bed downs](#)," presumably meaning where people sleep, and "[other locations of interest](#)." In other words, Fog's service allows police to track people's movements over long periods of time.

Fog Reveal is typically licensed for a year at a time, and records show that over time the company has charged police agencies between [\\$6,000](#) – [\\$9,000](#) a year. That basic service tier typically includes 100 queries per month, though Fog sells additional monthly query allocations for [an additional fee](#). For example, in 2019, [the California Highway Patrol paid \\$7,500](#) for a year of access to Reveal plus \$2,400 for 500 more queries per month.

Fog states that it does not collect personally identifying information (for example, names or email addresses). But Fog allows police to track the location of a device over long stretches of time — several months with a single query — and Fog touts the use of its service for “pattern of life” analyses that reveal where the device owner sleeps, works, studies, worships, and associates. This can tie an “anonymous” device to a specific, named individual.

Together, the “area search” and the “device search” functions allow surveillance that is both broad and specific. An area search can be used to gather device IDs for everyone in an area, and device searches can be used to learn where those people live and work. As a result, using Fog Reveal, police can execute searches that are functionally equivalent to the geofence warrants that are commonly served to Google.

This service could be used to determine who was near the scene of a violent crime around the time it was committed. It also could be used to search for visitors to a Planned Parenthood or an immigration law office on a specific day or everyone who attended a protest against police violence.



Image from Fog’s marketing brochure, sent to North Dakota and Chino, CA, which appears to show a single location signal as viewed with Fog’s service.

The basics of Fog's services are laid out in [a marketing brochure](#) which was sent to several prospective customers. The brochure explains that Fog's "unique, proprietary and patented data platform" processes data from "hundreds of millions of mobile devices" and can deliver "both forensic and predictive analytics and near real-time insights on the daily movements of the people identified with those mobile devices[.]" The materials state that Fog's collection of people's location data is "[100% Opt-in. All users opt-in to location data collection](#)," though as we will discuss later, this claim is hard to take at face value.

At the core of Fog's pitch is a series of claims about the breadth and depth of its location data. [It claims to process](#) over 250 million devices per month within the United States. (There are an [estimated 301 million mobile devices](#) nationally). [According to Fog](#), these devices generate 15 billion signals per day, or over 5 trillion per year.

Fog Data Science's proprietary platform has been architected with massive scale in mind and provides predictive analytics and near real-time insights on how people go about their daily lives. Currently, the platform processes:

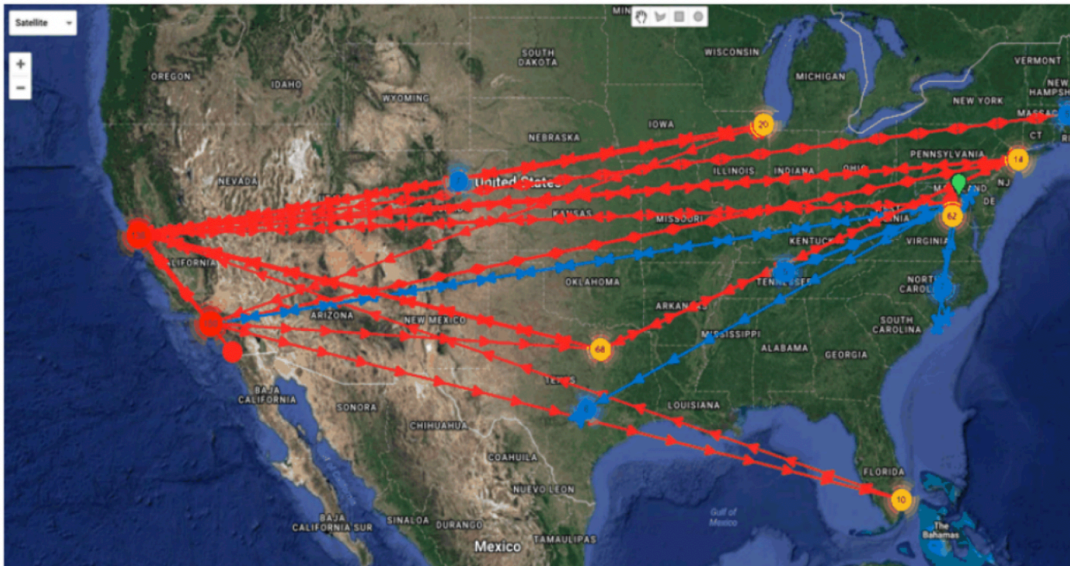
- 250 million devices each month
- 15 billion location signals each day
- 10 million fenced points of interest
- 1+ million daily events
- US and International Data

Excerpt from Fog's marketing brochure describing the properties of its dataset

EFF could not verify Fog's claims. But there is reason to be skeptical: Thanks to the nature of its data sources, it's likely that Fog can only access location data from users while they have apps open, or from a subset of users who have granted background location access to certain third-party apps. [Public records indicate](#) that some devices average several hundred pings per day in the dataset, while others are seen just a few times a day. Users who do not install many third-party apps, or who have opted out of tracking via Apple's App Tracking Transparency (ATT), may not be present in the dataset at all.

Additionally, [the records EFF reviewed](#) show that several of the agencies that worked with Fog have since [canceled their subscriptions](#), and [at least one said](#) they were not sure if they ever used Fog to successfully solve a case. Those

potential shortcomings are not a reason to underestimate Fog's invasiveness or its capability for unfettered dragnet monitoring. But it's important to understand its limits. Fog's data may be patchy and incomplete, with data about some people some of the time. But if we take Fog's claims at face value, it would mean that the company collects the location data of a majority of people in the United States on a monthly basis. This means Fog may have limits in its ability to locate any given person at a specific moment in time. But Fog's service may still be capable of identifying a significant portion of the hundreds of attendees at a protest or other sensitive location.



Example of "Pattern of Life Analysis"

[The brochure](#) gives some insight into how Fog intends for its service to be used. It lists a series of "use cases" from the dramatic ("Human Trafficking," "Terrorism Investigations," "Counter-Intelligence") to the more mundane ("Drug Investigations," "Soft Target Protection"). It seems to be aimed at both local law enforcement and at intelligence/homeland security agencies.

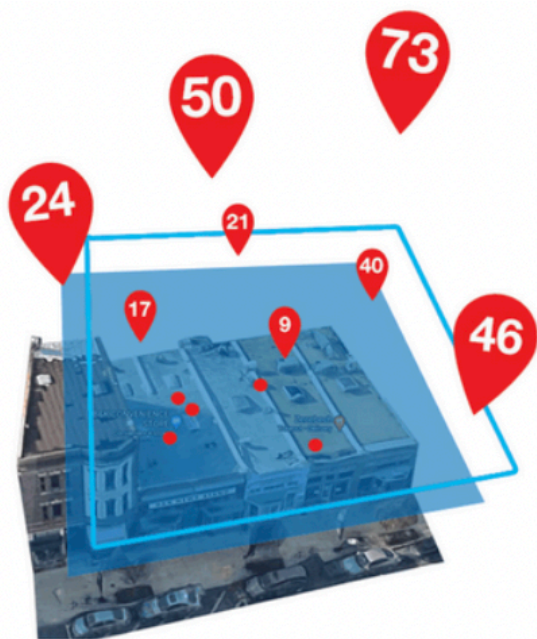
The language used in the document often invokes terms used by intelligence agencies. For example, [a core advertised feature](#) is the ability to run a "pattern of life analysis," which is what [intelligence analysts call](#) a profile of an individual's habits based on long-term behavioral data. Fog Reveal is also "[ideal for tipping and cueing](#)," which means using low-resolution, dragnet surveillance to decide where to perform more targeted, high-resolution monitoring. The brochure also includes a screenshot of Fog Reveal being used to monitor "a location at the US/Mexico border," and an alternate version of the brochure listed "Border Security/Tracking" as a possible use case. As we will discuss in our next post,

records show that Fog has worked with multiple DHS-affiliated fusion centers, where local and federal law enforcement agencies share resources and data.

In other materials, Fog emphasizes the convenience of its service. [An email titled “Solve crimes faster: Here’s how”](#) reads:

Find strong leads at your desk in minutes. Just type in a location, date and time, then watch app signals disclose what mobile devices were present at the crime scene. We’d love to help your department save time and money too. Let’s schedule a 10-minute demo next week.

Fog’s Reveal customers are given direct access to raw location data, [which can be exported from the web portal](#) into portable formats for processing elsewhere. Fog emphasizes that its license permits “[processing, analysis, and sub-licensing of location data](#),” potentially allowing law enforcement to share the data with private contractors. Fog routinely [encouraged](#) law enforcement agencies to share one license among multiple users, and [some customers used Fog to run queries](#) on behalf of other law enforcement agencies on request.



**Save weeks
of leg work
find strong
leads at
your desk
in minutes**

[Fog claims that it only sells its Reveal](#) service to law enforcement agencies. But Fog’s materials also advertise “[out-sourced analytic services](#)” for non law enforcement customers, including “private sector security clients.” [An email exchange](#) between Fog and Iowa police appears to corroborate this policy: Fog

says it will not grant private companies direct access to its database, but it will perform analysis on behalf of “law firms and investigative firms.” [According to a brochure](#), this analysis may include:

- Verifiable presence at a location on a specific date and time
- Likely locations for residences, places of business and frequent activities
- Links to other individuals, places and devices
- Patterns of activity correlating to certain events, times or alibis

In other words, Fog advertises that it can use its data to surveil the private lives of individuals on behalf of private companies. The records EFF has obtained do not provide any details about specific relationships Fog has with any private-sector clients.

Where does the data come from?

The kind of data that Fog sells to law enforcement originates from third-party apps on smartphones. Apps that have permission to collect a user’s location can share that data with third-party advertisers or data brokers in exchange for extra ad revenue or direct payouts. Downstream, data brokers collect data from many different apps, then link the different data streams to individual devices using [advertising identifiers](#). Data brokers often sell to other data brokers, obfuscating the sources of their data and the terms on which it was collected. Eventually, huge quantities of data can end up in the hands of actors with the power of state violence: police, intelligence agencies, and the military.

Over the past few years, journalists have uncovered several links between [private brokers of app-derived location data and the US government](#). Babel Street, best known for its open-source intelligence (OSINT) tools for analyzing social media and the like, sells location data as part of a secret add-on service called “Locate X.” Venntel, a subsidiary of marketing data company Gravy Analytics, has sold raw location data to several different US agencies, including ICE, Customs and Border Protection (CBP), and the FBI. And broker X-Mode [paid app developers around 3 cents per user per month](#) for access to location data, then sold it directly to defense contractors.

Enter Fog Data Science. Like the other companies, Fog buys data from the private market and packages it for use by law enforcement. Unlike most others, Fog seems to target smaller agencies. Venntel has sold a year’s worth of data to the Department of Homeland Security for more than \$650,000; meanwhile, Fog sold its service to the sheriff of Washington County, OH, for \$9,000 a year. While Venntel, Babel Street, and Anomaly 6 have made headlines for dealings with

three-letter federal agencies, public records show that Fog appears to have targeted its business at local, regional, and state law enforcement. That is, Fog sells its services to police agencies that most Americans are far more likely to interact with than federal law enforcement. [The records received by EFF](#) confirm past or ongoing contractual relationships with at least 18 state and local law enforcement clients; several other agencies took advantage of [free trials of Fog's service](#). [Notes from one agency's meeting](#) with Fog state that the company works with "50-60" agencies nationwide.

So where, exactly, does Fog's data come from? The short answer is that we don't know for sure. Several records explain that Fog's data is sourced from apps on smart phones and tied to mobile advertising identifiers, and one agency relayed that [Fog gathers data](#) from "over 700 apps." Fog officials have referred to a single "data provider" in emails and messages within Fog Reveal. [One such message](#) explained that the data provider "works with multiple sources to ensure adequate worldwide coverage," and that a "newly added source" was causing technical issues.

But when asked about which apps or companies originate its data, Fog has demurred. Some answers implied that Fog itself might not know. In July 2020, [Mark Massop responded to a point-blank question](#) from the Chino police that "Our data provider protects the sources of data that they purchase from." [Massop did say that at least two sources](#) were not included in Fog's dataset: Twitter and Facebook. Separately, [a Santa Clara County attorney wrote](#) that Fog gets information from "lots of smaller apps," but not Google or Facebook.

[Another document](#), shared in 2019 with the city of Anaheim, CA, says that Fog's portal uses "unstructured geo-spatial data emanating from open apps (Starbucks, Waze, etc.)" It's unclear whether this means that Fog actually receives data from the apps listed, or whether Starbucks and Waze are simply examples of "open apps" that could be sharing data. On Android, both [Starbucks](#) and [Waze](#) (which is owned by Google) have access to location permissions, and both apps use third-party advertising or analytics services. Waze was also mentioned in a presentation about Fog's capabilities to the Greensboro, NC police, according to Davin Hall, a former data analyst for the department interviewed by EFF. Per Hall, "Waze got brought up a lot" in the context of apps that could share data with Fog. "It got mentioned because it was a common one for people to have up while they were driving around, so it would be pinging regularly so that you could see the movement of the device actively," he said.

[The document](#) further claims that Fog’s competitors all buy their data from a single source, and that Fog has a unique and privileged relationship as an “associate” of that source.

[The use of app-based location data] for Law Enforcement and Intelligence Analysis purposes is limited to only a few carriers. Currently, these carriers purchase their source of data from an associate company of FOG Data Science. As non-associates, they are charged a much higher premium to purchase the data, thereby forcing higher prices for their products. [...]

Additionally, [FOG’s] direct access to, and association with, the database vendor allows it to offer low prices both per seat license and per additional query.

This implies that Fog’s data provider was, to its knowledge, the sole upstream source of app-based location data for all law enforcement and intelligence clients.

Links to Venntel

Other documents suggest that the “associate company” referenced in the Anaheim document — and the source of Fog’s data — is Venntel, perhaps the largest seller of location data to the government.

The most direct link comes from [an email exchange with the Iowa Department of Public Safety](#). In response to an Iowa intelligence analyst’s question about Fog’s data, a Fog representative said it would ask “our data partner” for assistance. Fog then forwarded the question (including a device identifier) to a representative of Venntel, who sent back a series of screenshots illustrating how the analyst should interpret the data.

There are other links between Fog and Venntel.

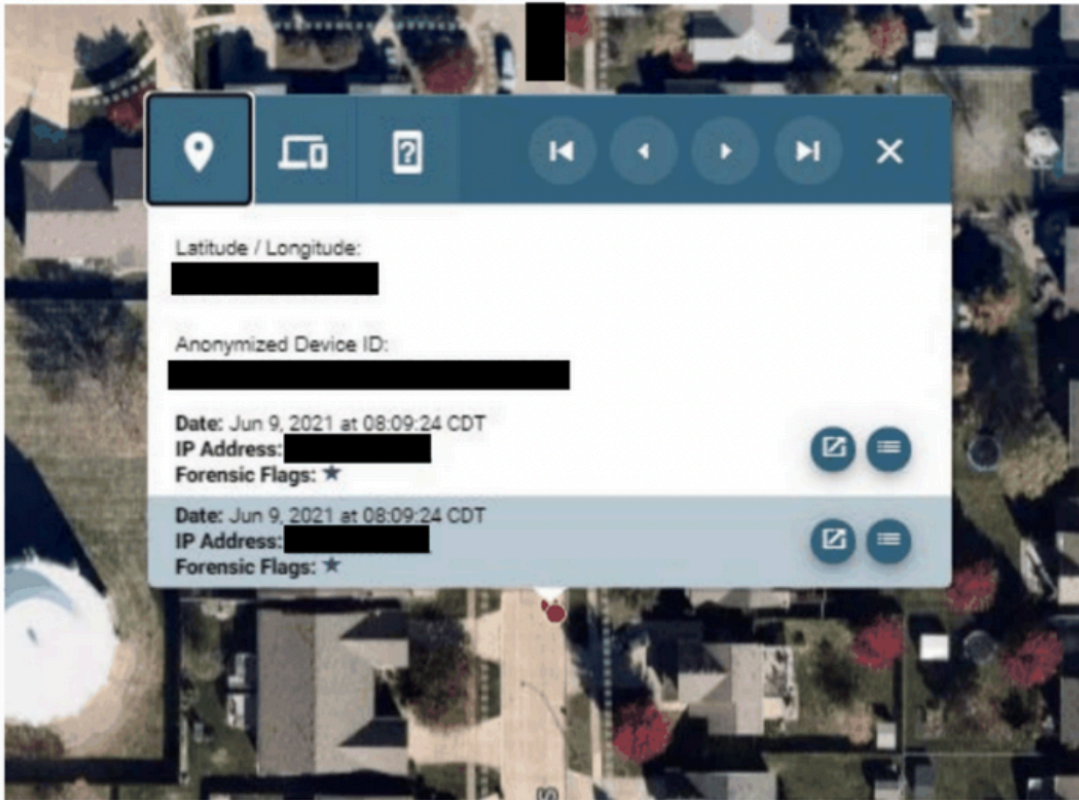
[The marketing materials](#) provided by Fog to multiple law enforcement agencies are nearly identical to [material that Venntel provided to DHS](#), according to records obtained by ACLU. The style, much of the language, and several of the graphics appear to be identical. It even appears that both companies use the same screenshot of a location in Santa Teresa, NM to illustrate their capabilities. Furthermore, both companies make identical claims about their data coverage,

including that they analyze “location signals from 250 million mobile devices in the U.S.” and “[15+ billion daily location signals](#).” These claims could be evidence that both companies have access to the same dataset.

Other records connect the two companies as well. One of the first records EFF received was a version of [Fog’s Software License Agreement](#) (SLA) from the Missouri State Highway Patrol. A piece of text in the header—edited to be hidden in the final document, but not deleted—reads “Venntel Analytics, Inc. Event Data Licensing Agreement.” .

Finally, [our investigation into the code hosted at fogreveal.com](#) turned up several literal links to Venntel. Many different URLs with the word “Venntel” in their path are referenced in the code. For example, when a Reveal user performs any geofenced device query, that query is submitted by sending a request to the url path “/Venntel/GetLocationData.”

This collection of evidence suggests that Venntel is Fog’s “associate,” that is, the source of its data. This conclusion would be consistent with Fog’s claim that its “associate” was the only source of data for other law-enforcement-facing location data brokers. [Previous reporting](#) has revealed that Venntel supplies data to other brokers, including Babel Street, which sells location data to the government through its secret “Locate X” service.



08:09:36 CDT back at the **Residential Location**.

EFF has redacted this screenshot to remove potentially identifiable information.

[Records released to EFF](#) also give us new information about how Venntel works. The screenshots appear to be taken from Venntel’s own web-based portal. It has [previously been reported](#) that Venntel lets users search for devices in a specific area, then perform deep dives on specific devices. This functionality parallels Fog Reveal’s “area search” and “device search” capabilities. To our knowledge, this is the first time the public has been able to see what Venntel’s user interface looks like. The interface is similar to Fog’s, though the visual style is slightly different. Venntel’s interface also appears to display more information than Fog’s does, including an IP address associated with each signal. You can read more about how Fog Reveal likely operates in [our deep dive into its code](#).

Consent and Identifiability

In [marketing materials and emails](#), Fog has reassured prospective customers that its data is “100% opt-in” and that “no PII [personally-identifiable information] is ever collected.” But records obtained by EFF and the nature of precise,

individualized location data shows that the data is incredibly personal and can easily identify people.

First, Fog's assertion that the people in its database have "opted in" rests on a legal fiction [of consent](#) that [EFF](#), [courts](#), and [members of Congress](#) have repeatedly criticized because it fails to adequately protect people's privacy. Modern smartphones require user consent before allowing certain kinds of data, including location, to be shared with apps. However, phones do very little to limit how the data is used after that permission is obtained. As a result, every permission is an all-or-nothing proposition: when you let a weather app access your location in order to see a five-day forecast, you may also give it the ability to sell, share, and use that data for whatever other purposes it chooses. In the United States, often the only legal limits on an app's use of data are those it places on itself in a privacy policy. And these policies can be written so vaguely and permissively that there are, functionally, no limits at all.

In other words, even if a user consents to an app collecting location data, it is highly unlikely that they consent to that data winding up in Fog's hands and being used for law enforcement surveillance.

Fog's second claim, that its data contains no personally identifying information, is hard to square with common understandings of the identifiability of location data as well as with records showing Fog's role in identifying individuals.

Location data is understood to be "personally identifying" under many privacy laws. The [Colorado Privacy Act](#) specifically defines "identified individuals" as people who can be identified by reference to "specific geolocation data." [The California Privacy Rights Act](#) considers "precise geolocation data" associated with a device to be "sensitive personal information," which is given heightened protections over other kinds of personal information. These definitions exist because location data traces can often be tied back to individuals even in the absence of other PII. Academic researchers have shown [over](#) and [over again](#) that de-identified or "anonymized" location data [still poses privacy risks](#).

Fog's data can allow police to determine where a person sleeps, works, or worships; where they go to get lunch, or health care, or to unwind on a Friday night. Tying a location trace to a real identity is often more of a mild inconvenience than a serious barrier to police. Fog's own literature clarifies this: [in a PowerPoint presentation](#) shared with Chino, CA, it explains, "While there is no PII data provided, the ability to identify a location based on a device's signal strength can provide potential identifications when combined with other data that

agencies have access to.” After attending a meeting with Fog representatives, [a St. Louis County officer summarized](#): “There is no PI linked to the [device ID]. (But, if we are good at what we do, we should be able to figure out the owner).”

Furthermore, Fog’s [data is directly tied](#) to “hashed” advertising identifiers, and [multiple records show](#) how Fog has helped its customers use “device searches” to track devices with specific ad IDs. A phone’s ad ID is available to anyone with access to the device, and ad IDs shared widely among app developers, advertising companies, and data brokers of all stripes. Once an agency has access to a target’s ad ID, they can use Fog to search for a detailed history of that person’s movement.

[Emails between Fog and the California Highway Patrol](#) indicate that Fog did not believe the [Carpenter v. U.S.](#) decision—which held that law enforcement need a warrant to access cell site location information (CSLI)—applied to their service, and therefore no warrant was required to access the app-based location data that Fog sells. But as we have discussed, Fog’s data is acquired and sold without meaningful consent and can frequently be used to track individuals just as effectively as CSLI. We discuss the legal issues with Fog and what we know about how agencies have treated the law in [a subsequent post](#).

A perfect storm

The market for app-derived location data is massive. Dozens of companies actively buy and sell this data with assistance from thousands more. Many of them put raw data up for sale on the open market. And at least a handful of companies sell this kind of data to the federal government. Despite this, Fog Data Science is the only company EFF is aware of that sells individualized location data to state and local law enforcement in the United States.

Fog’s product represents a direct and uniquely modern threat to our privacy. Its business is only possible because of a cascade of decisions by tech platforms, app developers, lawmakers, and judges, all of whom have failed to adequately protect regular users. Apple and Google have designed their mobile operating systems to support third-party tracking, giving brokers like Fog essential tools like the ad identifier. Thousands of app developers have monetized their software by installing invasive tracking code on behalf of data brokers and ad tech. Congress has repeatedly failed to pass even basic privacy protections, allowing a multibillion dollar data broker industry to operate in the open. And courts have failed to clarify that a person’s Fourth Amendment rights aren’t diminished just because they’re carrying a smartphone that can transmit their location to apps and data brokers.

Fog Reveal can be used to harm vulnerable people and suppress civil liberties. Fog's area searches can let police perform dragnet surveillance on attendees of peaceful protests, religious services, or political rallies. Some of Fog's customers already have a history of doing so by other means: [an investigation by ACLU](#) revealed how California Highway Patrol used helicopters with high-tech surveillance cameras to capture zoomed-in video of attendees at peaceful demonstrations against police violence.

Fog's service is especially dangerous in the wake of the Supreme Court's *Dobbs* decision. Many states have criminalized abortion, giving state and local police license to unleash their surveillance powers against people seeking reproductive healthcare as well as the professionals that provide it. Fog Reveal lets an officer sitting at a desk draw geofences around abortion clinics anywhere in the world, then track all devices seen visiting them.

Finally, Fog's service is ripe for abuse. [The records we received](#) indicated that some agencies required warrants to use Fog in some circumstances but did not show that law enforcement placed any limits on individual officers' use of the technology, nor that they conducted routine oversight or auditing. It is possible that officers with access to Fog Reveal could misuse it for personal ends, just like some have misused other investigative tools [in the past](#). In June, [news broke](#) that a US Marshal is being charged for allegedly using a different geolocation surveillance service in 2018 that was then sold by a prison payphone company — Securus — to track “people he had personal relationships with as well as their spouses.” (The US Marshals have previously contracted with Fog as well.) It's possible that officers could similarly misuse Fog to surveil people they know.

How to protect yourself

The good news, if any, is that it is relatively straightforward to protect yourself from Fog's surveillance. Fog relies on data gathered by code embedded in third-party apps. That means you can cut off its supply by revoking location permissions to any apps that you do not completely trust. Furthermore, turning off location services at the operating system level should prevent Fog and other app-based data brokers from accessing your location data at all. (This does not always prevent location data from being gathered by other actors, like your cellular carrier. You can read more about avoiding a range of threats to privacy in one of EFF's [Surveillance Self-Defense guides](#).)

There is no evidence that Google Maps, Apple, or Facebook provide data to Fog, and [emails from Fog representatives](#) and its customers state that Fog does not

gather data from Google or Facebook. While there are other reasons to restrict Google's access to your location, it does not appear as though data shared exclusively with one of these map providers will end up in Fog's database.

Finally, evidence suggests that Fog's service relies on using advertising identifiers to link data together, so simply disabling your ad ID may stymie Fog's attempts to track you. [One email suggests](#) that Apple's App Tracking Transparency initiative — which made ad ID access opt-in and resulted in a drastic decrease in the number of devices sharing that information — made services like Fog less useful to law enforcement. And former police analyst Davin Hall told EFF that the company wanted to keep its existence secret so that more people would leave their ad IDs enabled.

You can reset or disable your ad ID by following the instructions [here](#).

Fog and its customers have spent years trying to remain in the shadows. Its service cannot function properly otherwise. Exposed to the light of day, Fog's product becomes clear: an all-seeing eye that invades millions of Americans' privacy without warrant or accountability.

Read more about Fog Data Science:

- *Press release: [Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation](#)*
- *[What is Fog Data Science? Why is the Surveillance Company so Dangerous?](#)*
- *[How Law Enforcement Around the Country Buys Cell Phone Location Data Wholesale](#)*
- *[Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data](#)*
- *[Fog Data Science Puts our Fourth Amendment Rights up for Sale](#)*
- *[How Ad Tech Became Cop Spy Tech](#)*

Discover more. Join our email list for EFF news, events, campaigns, and ways to support digital freedom.

POSTAL CODE (OPTIONAL)

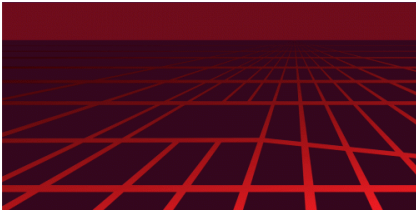
EMAIL ADDRESS *

SIGN UP NOW



I would like to join EFF's email list for EFF news, events, campaigns, and ways to support digital freedom.

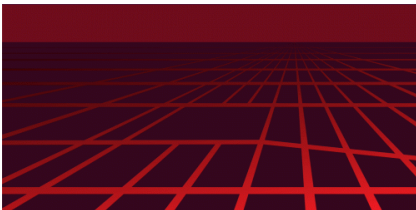
RELATED UPDATES



PRESS RELEASE | AUGUST 4, 2026

Mobile Ad Software Encourages Location Data Sharing, EFF Report Finds

SAN FRANCISCO – Some software development kits (SDKs) provided by advertising companies to help developers monetize their apps are automatically feeding users' location data into systems that location data brokers use to track people, an Electronic Frontier Foundation (EFF) [report found](#). EFF began investigating the location-sharing practices of various...



DEEPLINKS BLOG BY LENA COHEN, HUDSON HONGO |
MARCH 5, 2026

The Government Uses Targeted Advertising to Track Your Location. Here's What We Need to Do.

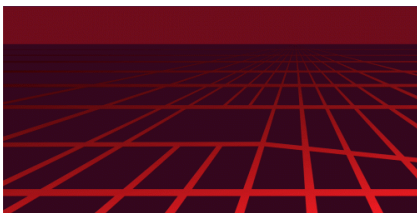
The online advertising industry has built a massive surveillance machine, and the government can co-opt it to spy on us.



DEEPLINKS BLOG BY MARIO TRUJILLO, HAYLEY TSUKAYAMA
| JUNE 24, 2025

Why Are Hundreds of Data Brokers Not Registering with States?

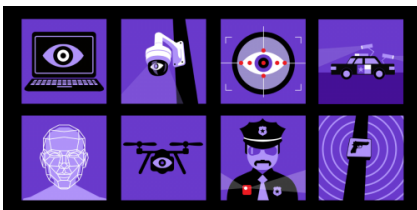
Hundreds of data brokers have not registered with state consumer protection agencies. A new analysis by Privacy Rights Clearinghouse (PRC) and the Electronic Frontier Foundation (EFF) reveals that many data brokers registered in one state aren't registered in others.



DEEPLINKS BLOG BY RINDALA ALAJAJI | APRIL 15, 2025

Privacy on the Map: How States Are Fighting Location Surveillance

Location data is highly sensitive, and without proper protections, it can be used to harm those who are already vulnerable. The digital trail we leave behind can reveal far more than we think, and without laws in place to protect us, we are all at risk.



DEEPLINKS BLOG BY MARIO TRUJILLO, BERYL LIPTON |
JANUARY 6, 2025

EFF Goes to Court to Uncover Police Surveillance Tech in California

The private company Pen-Link sued the San Joaquin Sheriff's Office to block the agency from disclosing to EFF the unredacted contracts between them, claiming the information is a trade secret. We are going to court to make sure the public gets access to these records.



DEEPLINKS BLOG BY LISA FEMIA | DECEMBER 4, 2024

Location Tracking Tools Endanger Abortion Access. Lawmakers Must Act Now.

EFF wrote recently about Locate X, a deeply troubling location tracking tool that allows users to see the precise whereabouts of individuals based on the locations of their smartphone devices. Developed and sold by the data surveillance company Babel Street, Locate X collects smartphone location data from a variety...



DEEPLINKS BLOG BY THORIN KLOSOWSKI | JULY 29, 2024

Senators Expose Car Companies' Terrible Data Privacy Practices

In a letter to the Federal Trade Commission (FTC) last week, Senators Ron Wyden and Edward Markey urged the FTC to investigate several car companies caught selling and sharing customer information without clear consent. Alongside details previously gathered from reporting by The New York Times, the letter also...



DEEPLINKS BLOG BY CATALINA SANCHEZ | JUNE 4, 2024

Car Makers Shouldn't Be Selling Our Driving History to Data Brokers and Insurance Companies

You accelerated multiple times on your way to Yosemite for the weekend. You braked when driving to a doctor appointment. If your car has internet capabilities, GPS tracking or OnStar, your car knows your driving history. And now we know: your car insurance carrier might know it, too. In a recent *New...*



DEEPLINKS BLOG BY KAREN GULLO | MARCH 15, 2024

Location Data Tracks Abortion Clinic Visits. Here's What to Know

Our concerns about the selling and misuse of location data for those seeking reproductive and gender healthcare are escalating amid a recent wave of cases and incidents demonstrating that the digital trail we leave is being used by anti-abortion activists. The good news is some states and tech companies...



DEEPLINKS BLOG BY ADAM SCHWARTZ | FEBRUARY 27, 2024

Sen. Wyden Exposes Data Brokers Selling Location Data to Anti-Abortion Groups That Target Abortion Seekers

This post was written by Jack Beck, an EFF legal intern In a recent letter to the FTC and SEC, Sen. Ron Wyden (OR) details new information on data broker Near, which sold the location data of people seeking reproductive healthcare to anti-abortion groups. Near enabled these groups to send...

