STREET LEVEL SURVEILLANCE

REAL-TIME LOCATION TRACKING

Real-time mobile location tracking is one of the ways in which law enforcement is able to track the location of individuals across time. Many individuals carry cell phones and other mobile devices with them regularly, and these devices typically capture some location information as part of the functionality of their applications and the robust location tracking ecosystem associated with advertising. In the past few years, law enforcement has gained access to this information by purchasing it from data brokers, giving them access, often in real-time, to the locations of millions of individuals who have had nothing to do with crimes.

How it works

To advertise to you online, companies need to have some idea of who you are and what you like, and in order to do this, your behavior online — and, often, your location — need to be linked to you. This information is regularly collected, bought, and sold by advertisers and private companies. Weather apps, navigation apps, coupon apps, and "family safety" apps often request location access in order to enable key features. Once

access with just about anyone, including the police.

Data brokers entice app developers with cash-for-data deals, often paying per user for direct access to their device. Developers can add bits of code called "software development kits," or SDKs, from location brokers into their apps. Once installed, a broker's SDK is able to gather data whenever the app itself has access to it. Sometimes that means access to location data whenever the app is open. In other cases, it means "background" access to data whenever the phone is on, even if the app is closed.

In many cases, applications require individuals to grant "permission" to access and collect location and other data in order to use the application. This information is generally associated with your Ad-ID, a way of identifying you, your online behavior, and location across devices, applications, and websites.

This sensitive information is regularly sold and shared with entities that are not the original application, and law enforcement has begun buying this information from data brokers.

How Law Enforcement Use It

Real-time mobile location data is now being used by federal agencies and small, local police departments alike.

Military and foreign intelligence agencies have used location data in numerous instances. In one unclassified project, researchers at Mississippi State University used Locate X data to track movements around Russian missile test sites, including those of high-level diplomats. The U.S. Army funded the project and said it showed "good potential use" of the data in the future. It also said that the collection of cell phone data was consistent with Army policy as long as no "personal characteristics" of the phone's owner were collected; of course, detailed movements of individuals are actually "personal characteristics".

State and local law enforcement also now use purchased location data to track individuals who may or may not be involved in crimes. They are able to use this information by identifying a device of interest and following its location as it moves through time and space or they might specify an area of interest to try to identify all devices (and, by extension, individuals) within that area.

Law enforcement can use this data by first effectively "geofencing" an area — that is, drawing a virtual "fence" around a real-world area of interest — and then collecting

law enforcement deems to be of interest, including protests and sensitive locations like places of worship or reproductive health clinics.

Who Sells It

Location data can be purchased from a number of data brokers, which themselves either collect the information directly from applications via SDKs or from other data brokers and applications.

Fog Data Science is a data broker that specializes in selling location data to law enforcement agencies. Agencies claim that it is the only company that provides access to this type of information without requiring the purchase of other platforms or services.

Venntel, a subsidiary of the commercial agency Gravy Analytics, appears to provide the data on which Fog Data's services are built and it is the vendor about which we know the most. Venntel's current and former clients in the U.S. government include, at a minimum, the Internal Revenue Service (IRS), the Department of Homeland Security (DHS) and its subsidiaries Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), the Drug Enforcement Administrations (DEA), and the Federal Bureau of Investigation (FBI). Gravy Analytics does not embed SDKs directly into apps; rather, it acquires all of its data indirectly through other data brokers. Locate X and Veraset are other companies that sell location data to the government.

Cobwebs Technologies also integrates real-time mobile location data into its platform, which includes other intelligence analysis for police operations.

Threats Posed by It

The purchase and use of mobile location data undermines individual Fourth Amendment rights and circumvents regulations placed on the government's ability to track and collect information on us without reason.

The Fourth Amendment generally requires police to obtain a warrant from a court before they search a particular location or person. In 2018, the Supreme Court ruled in *Carpenter vs. United States* that under the Fourth Amendment, police must get a warrant before obtaining historical location data derived from cell carriers — known as "cell site location information," or CSLI. Historical CSLI, the court wrote, creates a

over years."

With access to location data from commercial data brokers, federal agencies can query data about the movements of millions or billions of identifiable people at once. They are not limited to data about a single area or slice of time. They can start from a single time and place, then look forwards or backwards at the location histories of hundreds of devices at once, learning where their owners live, work, and travel. Agencies can make extraordinarily broad queries that span entire states or countries, and filter the resulting data however they see fit. It appears that this kind of full-database access is what the DHS purchased in its 2018 deal with Venntel. This stretches the Fourth Amendment's particularity requirement far beyond the breaking point.

Fog's "device search" feature provides a chronicle of a person's life that is often even more detailed than the CSLI at issue in the important case Carpenter vs. United States. There, police requested CSLI about a specific individual. Carriers MetroPCS and Sprint provided the government with 12,898 data points spanning 127 days. In one case using Fog's data, Missouri officials acquired 47,394 signals spanning 163 days for a single phone.

As shown by records from Iowa Department of Public Safety and Broward County, Florida, Fog commonly helps customers perform device searches on known advertising IDs. Fog's "Reveal" feature can also be used to execute a dragnet search of large physical areas in what is the equivalent of a "geofence warrant." Geofence warrants allow police to request information from Google about every device that was in a particular area at a particular time. Similarly, police can use a Fog Reveal "area search" to identify all devices within a geofence and time frame, then perform a "pattern-of-life analysis" on each device to try to identify its owner. Courts have invalidated geofence warrants on the ground that they are too broad to be constitutional.

The Fourth Amendment prohibits unreasonable searches and seizures, and it requires particularity in warrants. If the federal government wants specific location data about a specific person, it must first get a warrant from a court based on probable cause of crime. If the federal government wants to set up a dragnet of the ongoing movements of millions of identifiable people for law enforcement purposes, too bad – that's a forbidden general search. The federal government cannot do an end-run around these basic Fourth Amendment rules through the stratagem of writing a check to location data brokers — and yet that is exactly what they're doing by purchasing mobile location data.

EFF's Work Related to It

EFF has been investigating the use of mobile phone location tracking by law enforcement.

In summer 2022, EFF published an investigation, together with the Associated Press, into Fog Data Science, which, prior to our report, had been an unknown player in the mobile location broker landscape.

EFF is continuing to work to advance common knowledge of law enforcement's use of mobile location data and supports legislation, like the Fourth Amendment is Not For Sale Act, which limits the ability of government agencies to purchase information on individuals.

Suggested Additional Reading

US v Ellis

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

Tech tool offers police 'mass surveillance on a budget' (Associated Press)

Carpenter v. United States decision (Supreme Court)

New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data (ACLU)

TECHNOLOGIES