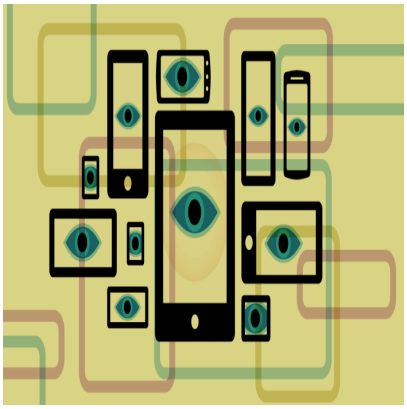


How the Federal Government Buys Our Cell Phone Location Data

Description

USA: Over the past few years, data brokers and federal military, intelligence, and law enforcement agencies have formed a vast, secretive partnership to surveil the movements of millions of people. Many of the mobile apps on our cell phones track our movements with great precision and frequency. Data brokers harvest our location data from the app developers, and then sell it to these agencies. Once in government hands, the data is used by the military to spy on people overseas, by ICE to monitor people in and around the U.S., and by criminal investigators like the FBI and Secret Service. This post will draw on recent research and reporting to explain how this surveillance partnership works, why is it alarming, and what can we do about it.

Where does the data come from?
Weather apps, navigation apps, coupon apps, and “family safety” apps often request location access in order to enable key features. But once an app has location access, it typically has free rein to share that access with just about anyone.

That’s where the location data broker industry comes in. 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.

One app developer received the following marketing email from data broker Safegraph:

SafeGraph can monetize between $1-$4 per user per year on exhaust data (across location, matches, segments, and other strategies) for US mobile users who have strong data records. We already partner with several GPS apps with great success, so I would definitely like to explore if a data partnership indeed makes sense.

But brokers are not limited to data from apps they partner with directly. The ad tech ecosystem provides ample opportunities for interested parties to skim from the torrents of personal information that are broadcast during advertising auctions. In a nutshell, advertising monetization companies (like

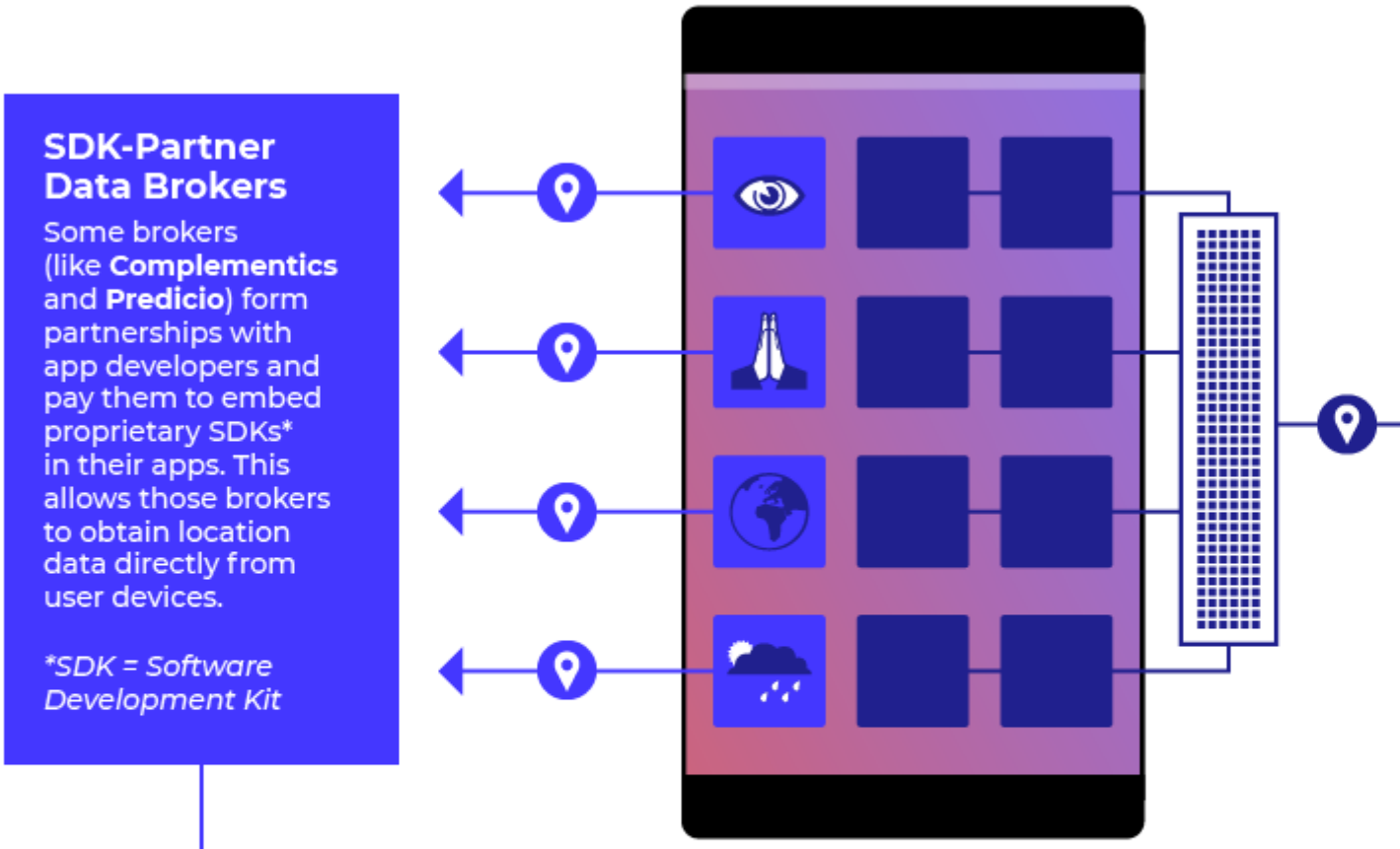
Google) partner with apps to serve ads. As part of the process, they collect data about users—including location, if available—and share that data with hundreds of different companies representing digital advertisers. Each of these companies uses that data to decide what ad space to bid on, which is a nasty enough practice on its own. But since these “bidstream” data flows are largely unregulated, the companies are also free to collect the data as it rushes past and store it for later use.

The data brokers covered in this post add another layer of misdirection to the mix. Some of them may gather data from apps or advertising exchanges directly, but others acquire data exclusively from other data brokers. For example, Babel Street reportedly purchases all of its data from Venntel. Venntel, in turn, acquires much of its data from its parent company, the marketing-oriented data broker Gravy Analytics. And Gravy Analytics has purchased access to data from the brokers Complementics, Predicio, and Mobilewalla. We have little information about where those companies get their data—but some of it may be coming from any of the dozens of other companies in the business of buying and selling location data.

If you’re looking for an answer to “which apps are sharing data?”, the answer is: “It’s almost impossible to know.” Reporting, technical analysis, and right-to-know requests through laws like GDPR have revealed relationships between a handful of apps and location data brokers. For example, we know that the apps Muslim Pro and Muslim Mingle sold data to X-Mode, and that navigation app developer Sygic sent data to Predicio (which sold it to Gravy Analytics and Venntel). However, this is just the tip of the iceberg. Each of the location brokers discussed in this post obtains data from hundreds or thousands of different sources. Venntel alone has claimed to gather data from “over 80,000” different apps. Because much of its data comes from other brokers, most of these apps likely have no direct relationship with Venntel. As a result, the developers of the apps fueling this industry likely have no idea where their users’ data ends up. Users, in turn, have little hope of understanding whether and how their data arrives in these data brokers’ hands.

Who sells location data?
Dozens of companies make billions of dollars selling location data on the private market. Most of the clients are the usual suspects in the data trade—marketing firms, hedge funds, real estate companies, and other data brokers. Thanks to lackluster regulation, both the ways personal data flows between private companies and the ways it’s used there are exceedingly difficult to trace. The companies involved usually insist that the data about where people live, sleep, gather, worship, and protest is used for strictly benign purposes, like deciding where to build a Starbucks or serving targeted ads.

But a handful of companies sell to a more action-oriented clientele: federal law enforcement, the military, intelligence agencies, and defense contractors. Over the past few years, a cadre of journalists have gradually uncovered details about the clandestine purchase of location data by agencies with the power to imprison or kill, and the intensely secretive companies who sell it.



SDK-Partner Data Brokers

Some brokers (like **Complementics** and **Predicio**) form partnerships with app developers and pay them to embed proprietary SDKs* in their apps. This allows those brokers to obtain location data directly from user devices.

**SDK = Software Development Kit*

Brokers That Sell Data to Governments

Though location data brokers most commonly sell to other private companies, there are some that specifically partner with military and law enforcement agencies.

Gravy Analytics

Venntel

Babel St

This chart illustrates the flow of location data from apps to agencies via two of the most prominent government-facing brokers: Venntel and Babel Street.

The vendor we know the most about is **Venntel**, a subsidiary of the commercial agency **Gravy Analytics**. Its current and former clients in the US government include, at a minimum, the IRS, the DHS and its subsidiaries ICE and CBP, the DEA, and the FBI. Gravy Analytics does not embed SDKs directly into apps; rather, it acquires all of its data indirectly through other data brokers.

Few data brokers reveal where their data comes from, and Venntel is no exception. But investigations and congressional testimony have revealed at least a few of Venntel's sources. In 2020, Martin Gundersen of NRK Beta filed requests under the GDPR's Right to Know in order to trace how data about his location made its way to Venntel. He installed two navigation apps from the company Sygic, as well as an app called Funny Weather, and granted them location permissions. Funny Weather sold his data to location broker Predicio, which then sold it to Gravy Analytics. The Sygic apps sold data to both Predicio and another firm, Complementics, which sent data to Gravy as well. All of the data ended up inside Venntel's database. In 2021, following a lengthy investigation by Sen. Ron Wyden, broker Mobilewalla revealed that it too had sold data to Venntel.

Gravy Analytics shares some information about its location-data practices on its website. Gravy claims it has access to "over 150 million" devices. It also states outright that it does not gather data from the bidstream. But government officials have told Congress that they believe Venntel's data is derived both from SDKs and from the bidstream, and there is other evidence to support that belief. One of Venntel's sources, Mobilewalla, has testified to Congress that it gathers and sells bidstream-based location data. Government contracts describe Venntel's dataset as containing data from "over 80,000 apps." Data brokers that rely solely on SDKs, like X-Mode, tend to maintain direct relationships with just a few hundred apps. Venntel's incredible app coverage makes it likely that at least a portion of its data has been siphoned from the bidstream.

Venntel's data is disaggregated and device-specific—making it easier for this data to point right to you. Motherboard reported that Venntel allows users to search for devices in a particular area, or to search for a particular device identifier to see where that device has been. It allows customers to track devices to specific workplaces, businesses, and homes. Although it may not include explicitly identifying information like names or phone numbers, this does not mean it is "anonymous." As one former employee told Motherboard, "you could definitely try and identify specific people."

Venntel has sold several annual licenses to its "Venntel Portal," a web app granting access to its database, at a price of around $20,000 for 12,000 queries. It has also sold direct access to all of its data from a region, updated daily and uploaded to a government-controlled server, for a more lavish $650,000 per year.

Babel Street is a government contractor that specializes in "open-source intelligence" (OSINT) services for law enforcement. Its flagship product, Babel X, scrapes and interprets text from social media and other websites and merges OSINT with data gathered from more traditional intelligence techniques. Babel Street is "widely used" by the military, intelligence agencies, private companies, and federal, state, and local law enforcement. It also sells access to app-derived location data through a service called "Locate X," as first reported by *Protocol* in March 2020.

Babel Street first registered Locate X with the U.S. Patent and Trademark Office in 2017. The service allows Babel's clients to query a database of app-derived location data. Locate X can be used to draw a digital fence around an address or area, pinpoint devices that were in that location, and see where else those devices went in prior months. Records obtained by Motherboard from DHS reveal that, according to a DHS official, "Babel Street basically re-hosts Venntel's data at a greater cost and with significant constraints on data access." Babel Street employees have also said Venntel is the ultimate source of most of the location data flowing to the federal government that we are aware of.

Although Babel Street has many public-facing marketing materials, it has attempted to keep details about Locate X a secret. Terms of use provided by Babel Street to its clients ban using Locate X data as evidence, or even mentioning it in legal proceedings. Still, several buyers of Locate X have been reported publicly, including the Air National Guard, the U.S. Special Forces Command (SOCOM), CBP, ICE, and the Secret Service.

Anomaly 6 (or "A6") also sells app-derived location data to the government. Its existence was first reported by the *Wall Street Journal* in 2020.

A6 was founded by a pair of ex-Babel Street employees, Brendan Huff and Jeffrey Heinz. At Babel Street, the two men managed relationships with large government clients, including the Defense Department, the Justice Department, and the intelligence community. After striking off on their own, A6 allegedly began developing a product to compete with Babel Street's Locate X, and catering its services to a very similar clientele. In 2018, Babel Street sued the company and its founders, and the two companies eventually settled out of court.

A6 presents very little information about itself publicly. Its website comprises just a company logo and an email address on an animated background. It is not registered as a data broker in either California or Vermont. Not much is known about A6's data sources, either. The *Wall Street Journal* reported that it collects data via SDKs in "more than 500" mobile apps. According to a 2021 report by *Motherboard*, these SDKs are deployed by "partners" of the company, not A6 itself, creating a buffer between the company and its data sources. A6 claims its contracts with the government are "confidential" and it can't reveal which agencies it's working with. Public procurement records reveal at least one relationship: in September 2020, SOCOM division SOCAFRICA paid $589,000 for A6's services.

In April 2022, The Intercept and Tech Inquiry reported on presentations that A6 made in a meeting with Zignal Labs, a social media monitoring firm with access to Twitter's "firehose." A6 proposed a partnership between the two firms that would allow their clients to determine "who exactly sent certain tweets, where they sent them from, who they were with," and more. In order to demonstrate its capability, A6 performed a live demonstration: it tracked phones of Russian soldiers amassed on the Ukrainian border to show where they had come from, and it tracked 183 devices that had visited both the NSA and CIA headquarters to show where American intelligence personnel might be deployed. It followed one suspected intelligence officer around the United States, to an American airfield in Jordan, and then back to their home.

X-Mode is a location data broker which collects data directly from apps with its own SDK. X-mode began as the developer of a single app, "drunk mode," designed to help users avoid sending embarrassing texts after dark. But once the app started getting traction, the company decided its real value was in the data. It pivoted to develop an SDK that gathered location data from apps and funneled

it to X-Mode, which sold the data streams to nearly anyone who would pay. It's not clear whether X-Mode had direct relationships with any government clients, but it has sold data to several defense contractors that work directly with the U.S. military, including Systems & Technology Research and the Sierra Nevada Corporation. It has also sold to HYAS, a private intelligence firm that tracks "threat actors" suspected of being involved with cyberattacks "to their door" on behalf of law enforcement and private clients.

X-Mode developed an SDK that was embedded directly in apps. It paid developers directly for their data, at a rate of $0.03 per U.S. user per month, and $0.005 per international user. X-mode's direct-SDK model also made it possible to figure out exactly which apps shared data with the company by analyzing the apps themselves. That's why the company made headlines in 2020, when *Motherboard* revealed that dozens of apps that target at-risk groups – including two of the largest Islamic apps in the U.S., Muslim Pro and Salaat First – were monetizing location data with X-Mode. This visibility also made X-Mode more accountable for its behavior: both Apple and Google concluded that X-Mode violated their developer terms of service, and banned any apps using X-Mode's SDK from the App Store and the Play Store.

At one time, X-Mode boasted it had data from about 25 million active users in the U.S. and 40 million more worldwide, tracked through more than 400 different apps. After the crackdown by mobile platforms, the company was bought out and rebranded as Outlogic, and it adjusted its public image. But the company is still active in the location data market. Its new parent, Digital Envoy, sells "IP-based location" services, and describes its Outlogic subsidiary as "a provider of location data for the retail, real estate and financial markets." Digital Envoy also has deep ties to the U.S. government. The Intercept has reported that Digital Envoy contracts with the IRS enforcement division, the DHS Science and Technology Directorate (which has also contracted with Venntel), and the Pentagon's Defense Logistics Agency. It's unclear whether Outlogic's app-based location data is incorporated into any of those Digital Envoy relationships.

How is location data used?

While several contracts between data brokers and federal agencies are public records, very little is known about how those agencies actually use the services. Information has trickled out through government documents and anonymous sources.

Department of Homeland Security

Perhaps the most prominent federal buyer of bulk location data is the U.S. Department of Homeland Security (DHS), as well as its subsidiaries, Immigrations and Customs Enforcement (ICE) and Customs and Border Patrol (CBP). The Wall Street Journal reported that ICE used the data to help identify immigrants who were later arrested. CBP uses the information to "look for cellphone activity in unusual places," including unpopulated portions of the US-Mexico border. According to the report, government documents explicitly reference the use of location data to discover tunnels along the border. Motherboard reported that CBP purchases location data about people all around the United States, not just near the border. It conducts those searches without a court order, and it has refused to share its legal analysis of the practice with Congress.

The Federal Procurement Database shows that, in total, DHS has paid at least $2 million for location data products from Venntel. Recently released procurement records from DHS shed more light on one agency's practice. The records relate to a series of contracts between Venntel and a recently-shuttered research division of DHS, the Homeland Security Advanced Research Projects Agency (HSARPA). In 2018, the agency paid $100,000 for five licenses to the Venntel Portal. A few months later, HSARPA upgraded to a product called "Geographic Marketing Data – Western Hemisphere," forking over $650,000 for a year of access. This data was "delivered on a daily basis via S3 bucket"—that is, shipped directly to DHS in bulk. From context, it seems like the "Venntel Portal" product granted limited access to data hosted by Venntel, while the purchase of "Geographic Marketing Data" gave DHS direct access to all of Venntel's data for particular regions in near-real-time.

The HSARPA purchases were made as part of a program called the Data Analytics Engine (DA-E). In a Statement of Work, DHS explained that it needed data specifically for Central America and Mexico in order to support the project. Elsewhere, the government has boasted that ICE has used "big data architecture" from DA-E to generate "arrests, seizures, and new leads." ICE has maintained an ongoing relationship with Venntel in the years since, signing at least six contracts with the company since 2018.

Federal law enforcement

The FBI released its own contracts with Venntel in late 2021. The documents show that the FBI paid $22,000 for a single license to the Venntel Portal, but are otherwise heavily redacted. Another part of the Department of Justice, the Drug Enforcement Administration (DEA), committed $25,000 for a one-year license in early 2018, but Motherboard reported that the agency terminated its contract before the first month was up. According to the Wall Street Journal, the IRS tried to use Venntel's data to track individual suspects, but gave up when it couldn't locate its targets in the company's dataset. Some of Babel Street's law enforcement customers have had more success: Protocol reported that the U.S. Secret Service used Locate X to seize illegal credit card skimmers installed at gas pumps in 2018.

Military and intelligence agencies

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 (but of course, detailed movements of individuals are actually "personal characteristics").

Another customer of Locate X is the Iowa Air National Guard, as first reported by *Motherboard*. Specifically, the Des Moines-based 132d wing—which reportedly conducts "long-endurance coverage" and "dynamic execution of targets" with MQ-9 Reaper drones—purchased a 1-year license to Locate X for $35,000. The air base said the license would be used to "support federal mission requirements overseas," but did not elaborate further.

Anomaly 6 only has one confirmed federal client: the U.S. Special Operations Command, or SOCOM.

In 2020, SOCAFRICA – a division which focuses on the African continent – spent nearly $600,000 on a “commercial telemetry feed” from A6. In March 2021, SOCOM told *Vice* that the purpose of the contract was to “evaluate” the feasibility of using A6 services in an “overseas operating environment,” and that the government was no longer executing the contract. In September 2021, federal procurement records show that the U.S. Marines’ special operations command, MARSOC, executed another contract for $8,700 for “SME Support” from A6. (SME could stand for Subject Matter Expert, implying that A6 provided training or expertise.)

Finally, the Defense Intelligence Agency (DIA) has confirmed that it, too, works with location data brokers. In a January 2021 memo to Senator Ron Wyden, DIA stated that it “provides funding to another agency” that purchases location data from smartphones on its behalf. The data is global in scope, including devices inside and outside the United States, though the DIA said it segregates U.S. data points into a separate database as it arrives. The U.S. location database can only be queried after a “specific process” involving approval from multiple government agencies, and the DIA stated that permission had been granted five times in the previous two and a half years. The DIA claimed it needs a warrant to access the information. It’s unclear which data broker or brokers the DIA has worked with.

Is it legal for the federal government to buy our location data?

In a word, “no.” 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.

The U.S. Supreme Court’s ruling on cell-site location information, or CSLI, is instructive. CSLI is generated as cell phones interact with cell towers. It’s collected passively, all the time, from every phone that has cell service. It is less granular than GPS-based location data, and thus cannot locate devices as accurately. The only companies that can access it directly are the phone carriers themselves. In 2018, the Supreme Court ruled in *Carpenter v. United States* that CSLI is protected by the Fourth Amendment. It also held that the government can’t demand CSLI from telecom companies without a court-approved warrant. Since 2018, all major U.S. carriers have publicly committed to stop selling raw CSLI to anyone. Police do commonly obtain warrants for CSLI pertaining to active investigations.

Courts also are beginning to crack down on “geofence warrants” for GPS data from large companies like Apple and Google. These warrants seek all the phones present in a particular time and place. As EFF has explained, they are general searches that violate the Fourth Amendment’s particularity requirement. One was struck down by a federal district court earlier this year in *United States v. Chatrie* . Federal purchase of location data about millions of people raises similar Fourth Amendment concerns.

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. As Anomaly 6 reportedly demonstrated, 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.

In 2021, the Center for Democracy and Technology published a comprehensive report on the legal framework underpinning the government's purchasing of location data. It concluded that when law enforcement and intelligence agencies purchase personal data about Americans, "they are evading Fourth Amendment safeguards as recognized by the Supreme Court." EFF agrees. The Fourth Amendment should not be for sale. Sensitive data about our movements should not be collected and sold in the first place, and it certainly shouldn't be made available to government agencies without a particularized warrant.

Finally, transparency laws in Vermont and California require certain kinds of data brokers, including those that process location data, to register with the state. Of the companies discussed above, X-Mode, Gravy Analytics, and Venntel are registered in California, but Babel Street and Anomaly 6 are not. These laws need better enforcement.

What can we do?

Congress must ban federal government purchase of sensitive location information. The issue is straightforward: government agencies should not be able to buy any personal data that normally requires a warrant.

But legislatures should not stop there. Personal data is only available to government because it's already amassed on the private market. We need to regulate the collection and sale of personal data by requiring meaningful consent. And we should ban online behavioral advertising, the industry which built many of the tracking technologies that enable this kind of mass surveillance.

The developers of mobile operating systems also have power to shut down this insidious data market. For years, both Apple and Google have explicitly supported third-party tracking with technology like the advertising identifier. They must reverse course. They also must crack down on alternative methods of tracking like fingerprinting, which will make it much more difficult for brokers to track users. Furthermore, OS developers should require apps to disclose which SDKs they pack into their apps and whom they share particular kinds of data with. Both Apple and Google have made strides towards data-sharing transparency, giving users a better idea of how particular apps access sensitive permissions. However, users remain almost entirely in the dark about how each app may share and sell their data.

Fortunately, you can also take steps towards preventing your location data from winding up in the hands of data brokers and the federal government. As a first step, you can disable your advertising identifier. This removes the most ubiquitous tool that data brokers use to link data from different sources to your device. You can also look at the apps on your phone and turn off any unnecessary permissions granted to third-party apps. Data brokers often obtain information via apps, and any app with location permission is a potential vector. Revoke permissions that apps do not absolutely need, especially location access, and uninstall apps that you do not trust.

By Bennett Cyphers

Category

1. Crime-Justice-Terrorism-Corruption
2. Freedom-Free speech-Resitance & H-rights
3. Main
4. NWO-Deep State-Dictatorship-Tyrrany
5. Science-Tech-AI-Medical & Gen. Research

Date Created
06/16/2022