
# Feds Accessing Location Data from Millions of People Through Private Brokers

## Description

**USA: Big Brother is tracking your location with the help of private data brokers.**

According to a recent report by the Electronic Frontier Foundation (EFF), data brokers harvest location data from mobile apps and then sell it to government agencies including state and local law enforcement, ICE, the FBI, the Department of Homeland Security and the Department of Defense.

Many of the apps on a mobile device track and record location data. These include navigation apps, social media apps, and weather apps, among many others. According to EFF, once a user gives an app permission to access location data, it typically has “free rein” to share it with just about anybody. Government agencies take advantage of these loose standards to purchase troves of location data relating to millions of individuals from data brokers.

> “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.”

There is a tangled web of companies buying and selling data in this multi-billion-dollar industry. According to the EFF report, it’s virtually impossible to determine which apps share data. But apparently, a lot of them do. Data broker Venntel, a subsidiary of Gravy Analytics, claims to collect location data from over 80,000 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.”

Venntel is one of the companies reportedly selling data to government agencies. According to EFF, current and former clients include the IRS, the DHS, along with its subsidiaries ICE and CBP, the DEA, and the FBI.

You might be tempted to blow off this clear violation of privacy, reasoning that it would be difficult to pick out a specific individual from a big batch of location data. But according to the report, “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. Users can also conduct searches for particular device identifiers allowing them to track a specific device. With this information, the users can track devices to specific workplaces, businesses and homes. Even if the data doesn’t include specific information such as names or phone numbers, it’s not “anonymous.” As one former employee told *Motherboard*, “you could definitely try and identify specific people.”

And as another EFF report pointed out, it’s virtually impossible to truly anonymize location data to begin with.

> Practically speaking, there is no way to deidentify individual location data. Information about where a person is and has been itself is usually enough to reidentify them. Someone who travels frequently between a given office building and a single-family home is probably unique in those habits and therefore identifiable from other readily identifiable sources. One widely cited study from 2013 even found that researchers could uniquely characterize 50 percent of people using only two *randomly* chosen time and location data points.

The Federal Procurement Database reveals that the DHS paid at least $2 million for location data products from Venntel. A heavily redacted document obtained from the FBI shows the agency paid $22,000 for a single license to the Venntel portal.

Venntel is just one of several companies in the location data game.

Once the feds get access to data, it becomes available to hundreds of state, local and federal agencies through fusion centers and the Information Sharing Environment (ISE). This creates the potential for the federal government to track the movement of millions of Americans with no warrant, no probable cause, and without the people even knowing it.

Fusion centers were sold as a tool to combat terrorism, but that is not how they are being used. The ACLU pointed to a bipartisan congressional report to demonstrate the true nature of government fusion centers: “They haven’t contributed anything meaningful to counterterrorism efforts. Instead, they have largely served as police surveillance and information sharing nodes for law enforcement efforts targeting the frequent subjects of police attention: Black and brown people, immigrants, dissidents, and the poor.”

Fusion centers operate within the broader ISE. According to its website, the ISE “provides analysts, operators, and investigators with information needed to enhance national security. These analysts, operators, and investigators…have mission needs to collaborate and share information with each other and with private sector partners and our foreign allies.” In other words, ISE serves as a conduit for the

sharing of information gathered without a warrant. Known ISE partners include the Office of Director of National Intelligence which oversees 17 federal agencies and organizations, including the NSA. ISE utilizes these partnerships to collect and share data on the millions of unwitting people they track.

*by Michael Maharrey*

**Category**

1. Crime-Justice-Terrorism-Corruption
2. Economy-Business-Fin/Invest
3. Freedom-Free speech-Resitance & H-rights
4. Main

**Date Created**
07/08/2022