# US Homeland Security purchased “staggering” volumes of location data to illegally track citizens and immigrants

**Kevin Reed**
**20 July 2022**

The American Civil Liberties Union (ACLU) released on Monday previously unpublished records of bulk smartphone location data purchased by the Department of Homeland Security (DHS) from private contractors that it used illegally to track the movement of individuals across North America.

The documents were obtained by the ACLU through a Freedom of Information Act (FOIA) lawsuit filed in 2020. The records show that, during both the Trump and Biden administrations, the DHS was procuring huge volumes of people’s cell phone location tracking information from two data brokers—Venntel and Babel Street—in violation of the Fourth Amendment right against unreasonable searches and seizures.

The trove of records shows how the DHS departments, Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) and, also likely the US Secret Service and US Coast Guard, spent millions in government funds to make bulk location data purchases. An ACLU press release says, “the volume of people’s sensitive location information obtained by the agency is staggering.”

The ACLU has published a set of seven redacted spreadsheets provided by CBP that contain “a small subset of the raw location data purchased by the agency from Venntel.” The press release goes on to provide details, “For one three-day span in 2018, the records contain around 113,654 location points—more than 26 location points per minute. And that data appears to come from just one area in the Southwestern United States …”

Among the documents obtained are email communications between DHS staff and representatives of the data companies in which attempts are made to rationalize the “unfettered sale of massive quantities of data in the face of the US Supreme Court precedent protecting similar cell phone location data against warrantless government access,” the ACLU release says.

Shreya Tewari, the Brennan Fellow for ACLU’s Speech, Privacy, and Technology Project, said, “These records provide critical insight into the government’s attempts to wash its hands of any accountability in purchasing people’s sensitive location data when it would otherwise need a warrant.”

The ACLU shared the documents with Politico, which published its own analysis. Politico said that the records obtained in the FOIA lawsuit included location information which was “harvested from apps on hundreds of millions of phones” and enabled the DHS to pinpoint “more than 336,000 location data points across North America,” and that this data “may reference only a small portion of the information that CBP has obtained.”

Politico also revealed that the data points included locations in major cities like Los Angeles, New York, Chicago, Denver, Toronto and Mexico City. Politico also reported that the location data has been used by CBP during the Biden administration which “renewed a contract for $20,000 that ended in September 2021.”

Most of the data obtained by the ACLU comes from Venntel, a data broker located in the Washington DC area that is a subsidiary of Gravy Analytics. These companies specialize in gathering data which tracks the movement of individuals from one destination to another for the stated purposes of targeted marketing.

In making a sales pitch to the DHS departments, Venntel boasted that it had collected location data from

more than 250 million mobile devices and processed more than 15 billion location data points per day. On its website, Venntel promotes its services as “Innovative big data analytics for the world’s most challenging problems.”

According to an industry study, location data businesses include collectors, aggregators, marketplaces and location intelligence firms, and generate a combined $12 billion in annual revenue.

Location data is gathered by apps on smartphones and other mobile devices when they are given permission to do so by users. Permission-based location data gathering was implemented on Apple’s iOS in April 2021 and on Android devices in June 2022. Prior to these dates, app gathering of location data could be stopped, but users would need to either turn off location services entirely or for each app individually.

Apps have many reasons for needing to know a user’s location, such as how to provide directions to a retail location or serving up local weather conditions. However, when users enable location services for apps, either while using the app or as it is running in the background, they are not aware that this information is being bought and sold by powerful “big data” companies.

The ACLU revelations show that this information is being purchased from the data firms by the institutions of the national security state for the purposes of developing its police operations in violation of basic constitutional rights.

As reported in February 2020, the *Wall Street Journal* revealed at that time that the DHS under the Trump administration began purchasing phone location data from Venntel in 2017. It has taken more than two years since that time for Congress to launch an investigation into these practices, and the ACLU revelations are part of this legislative initiative. On Tuesday, the House Judiciary Committee held a hearing entitled “Digital Dragnets: Examining the Government's Access to Your Personal Data.” In April 2021, Senator Ron Wyden (Democrat-Oregon) introduced the “Fourth Amendment is Not For Sale Act” which states that government agencies cannot purchase the location data of Americans without a warrant.

The use of location data by police agencies is the tip of the iceberg of mass electronic surveillance of the public that has been ongoing and intensifying, beginning with the undemocratic provisions spelled out in the USA Patriot Act passed in the aftermath of the terror attacks of September 11, 2001.

Even after former NSA and CIA contractor and whistleblower Edward Snowden exposed details of the sophisticated techniques being used by the intelligence state to monitor the locations, activities and communications of everyone on the planet, all the assurances by Democrats and Republicans that these programs have been halted have turned out to be lies. The ongoing assault on privacy rights by state agencies, against both citizens and non-citizens alike, is a necessary part of the drive by US imperialism for war abroad and the destruction of democratic rights at home.