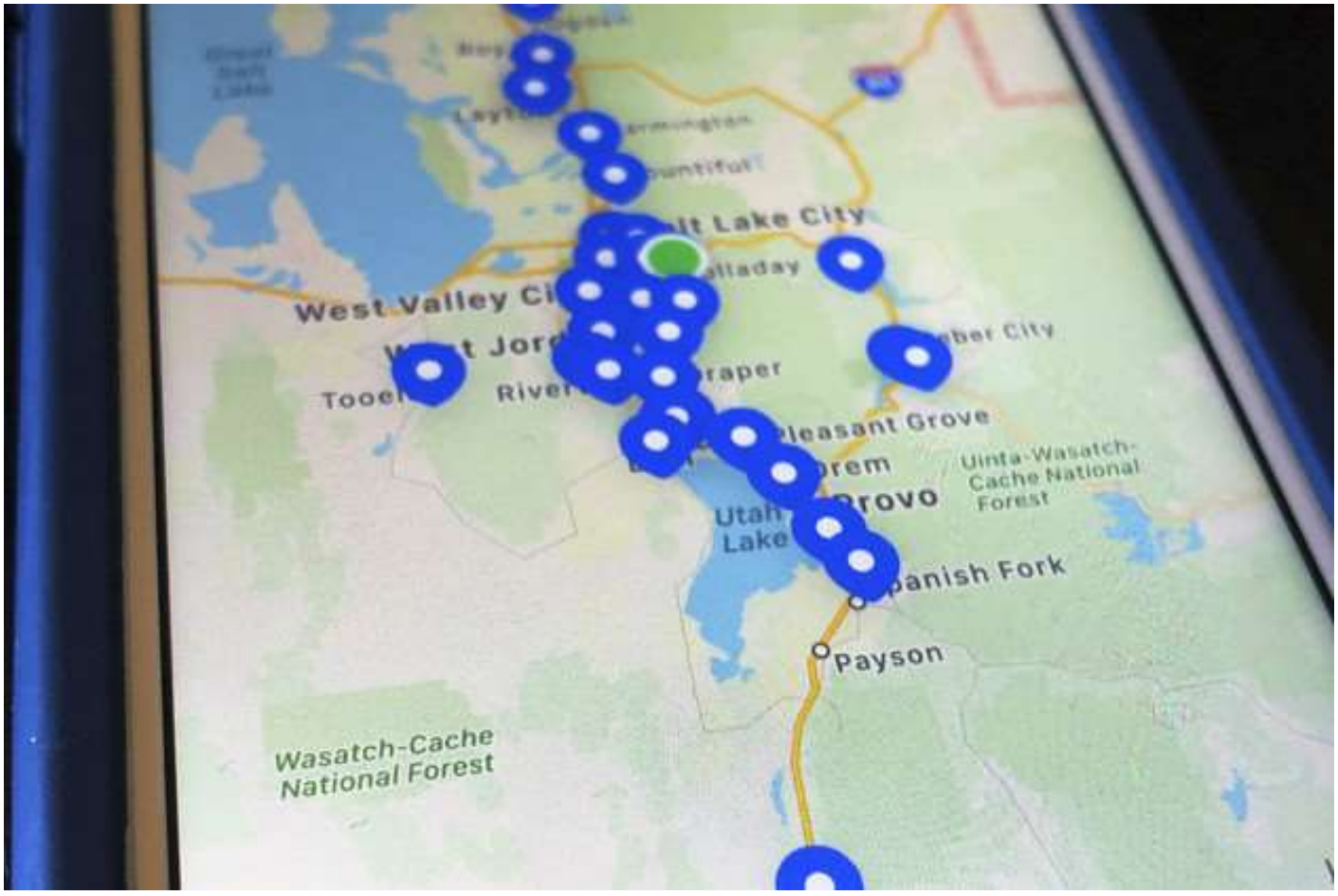
POLITICO

TECHNOLOGY

Homeland Security records show 'shocking' use of phone data, ACLU says

The civil liberties group released documents showing new details about how agencies had purchased information on people's movements throughout North America.



In just three days in 2018, documents show that the CBP collected data from more than 113,000 locations from phones in the Southwestern United States — equivalent to more than 26 data points per minute — without obtaining a warrant. | Lindsay Whitehurst/AP Photo

By **ALFRED NG**

07/18/2022 07:00 AM EDT
Updated: 07/18/2022 03:30 PM EDT

The Trump administration's immigration enforcers used mobile location data to track people's movements on a larger scale than previously known, according to documents that raise new questions about federal agencies' efforts to get around restrictions on warrantless searches.

The data, harvested from apps on hundreds of millions of phones, allowed the Department of Homeland Security to obtain data on more than 336,000 location data points across North America, the documents show. Those data points may reference only a small portion of the information that CBP has obtained.

These data points came from all over the continent, including in major cities like Los Angeles, New York, Chicago, Denver, Toronto and Mexico City. This location data use continued into the Biden administration, as Customs and Border Protection renewed a contract for $20,000 that ended in September 2021.

The American Civil Liberties Union obtained the records from DHS through a lawsuit it filed in 2020. It provided the documents to POLITICO and separately released them to the public on Monday.

The documents highlight conversations and contracts between federal agencies and the surveillance companies Babel Street and Venntel. Venntel alone boasts that its database includes location information from more than 250 million devices. The documents also show agency staff having internal conversations about privacy concerns on using phone location data.

In just three days in 2018, the documents show that the CBP collected data from more than 113,000 locations from phones in the Southwestern United States — equivalent to more than 26 data points per minute — without obtaining a warrant.

The documents highlight the massive scale of location data that government agencies including CBP and ICE received, and how the agencies sought to take advantage of the mobile advertising industry's treasure trove of data.

"It was definitely a shocking amount," said Shreya Tewari, the Brennan fellow for the ACLU's Speech, Privacy and Technology Project. "It was a really detailed picture of how they can zero in on not only a specific geographic area, but also a time period, and how much they're collecting and how quickly."

DHS did not immediately respond to a request for comment.

"Despite claims by data brokers, no one who downloads an app thinks they are giving permission to waive their 4th Amendment rights and let the government follow their every move."

— Sen. Ron Wyden (D-Ore.)

The location data industry is an estimated $12 billion market, made up of hundreds of apps that collect location data, data brokers who trade that information among each other, and buyers who look to use that data for purposes such as advertising and law enforcement.

Because the U.S. has no federal privacy laws to rein the industry in, location data sales have gone largely unchecked for the past decade and allowed data brokers to sell millions of people's whereabouts to whoever's buying.

Location data has been sold in the past to help the U.S. military identify Muslim populations and was available on Planned Parenthood visitors. A blog also used location data to out a gay priest in 2021. In 2020, The Wall Street Journal revealed that federal agencies including DHS, ICE and CBP were using commercial location data for immigration enforcement. The documents published by the ACLU on Monday give a glimpse into just how much location data these agencies obtained, and how they viewed using that information.

"Venntel has a mobile location data intelligence platform that leverages the unclassified, commercially available mobile advertising ecosystem," a CBP official wrote in an email in March 2018.

Tracking on a major scale

The bulk of the location data that CBP obtained came from its contract with Venntel, a location data broker based in Virginia. Venntel is a subsidiary of Gravy Analytics, an advertising company that specializes in location data.

The data, which spanned from 2017 to 2019, contained more than 336,000 location data points that reached across North America. But in reality, the agency's data collection may go far beyond what the ACLU obtained through its FOIA requests, considering that CBP continued to use Venntel in 2021.

In the records, CBP highlighted that it used the location data for immigration enforcement, as well as human trafficking and narcotics investigations.

When Venntel first reached out to the federal agencies, it offered marketing material highlighting the extent of its data collection capabilities. In one email from February 2017 sent to ICE, the data broker boasted that it collected location data from more than 250 million mobile devices and processed more than 15 billion location data points a day.

CYBERSECURITY

'Lock it down right now': Abortion rights advocates prepare for a new wave of digital security threats

BY SAM SABIN

In another brochure, Venntel showed that its location data could be used to track devices traveling between Mexico and the U.S., and also trace a specific vehicle's route. The brochure page also indicated that Venntel's data was capable of identifying mobile devices that were at the deadly 2017 white supremacist riot in Charlottesville, Va.

Another marketing brochure told CBP that "all users opt-in to location data collection," and that no personal data was ever collected. But in another email between Venntel and ICE, the data broker noted, "there are derived means by which identifiers and pertinent location can be assembled," meaning that this data could easily be linked to identify people despite not having any personal data tied to it.

"The way that they use the phrase 'opt-in,' they're talking about the fact that you have to give permission on your phone for an app to access location," the ACLU's Tewari said, "but it's very clear that when people are doing that, they're not expecting that that's going to be potentially creating this massive database of their entire location history that's available to the government at any time."

Contradictions

The records obtained by the ACLU highlight how these agencies knew that the advertising technology industry's location data collection was both a surveillance boon and a privacy concern.

In internal presentation documents, CBP highlighted the potential of adtech data, specifically with advertising IDs that are assigned to every device. The advertising industry relies on these mobile ad IDs to track what people have seen online, and learn about their patterns and behaviors.

"There are over 350 million mobile devices in the United States in use today, and that number is growing exponentially as more people purchase mobile devices every day. Therefore it is not uncommon to encounter individuals involved with illicit activity taking advantage of mobile technology to further their criminal goals," a contract between CBP and Venntel said.

But in the same presentations where CBP was highlighting the advantages of using advertising data, the agency was also showing its staff how to reset their

own advertising IDs on Android and iOS devices.

“These agencies seem fully aware that they are exploiting a massive privacy disaster in this country,” said Nathan Freed Wessler, the ACLU’s Speech, Privacy and Technology Project’s deputy director. “These agencies understand that the same data dumps that they are able to buy access to for whatever they want can also be bought by anyone else to try to target their agents.”

And in June 2019, DHS’ acting privacy officer ordered the agency to “stop all projects involving Venntel data” because of unanswered privacy and legal concerns. Venntel provided a privacy and legal review for DHS in September

2019, though its contents are redacted. In an October 2019 email included in the ACLU's document release, a DHS employee told Venntel that the agency was still waiting for the general counsel's review of the presentation. "DHS privacy and legal offices authorized the continued use of Venntel's data following this meeting," Gravy Analytics said in a statement on Monday.

Using the commercially available location data helped the agencies avoid requesting a warrant to track people, because they could just buy the data instead. But DHS' privacy officer in 2019 knew this was still a potential privacy concern, citing the Supreme Court ruling in *Carpenter v. United States*, which said police need warrants to access phone location data.

Location data's future

Despite the privacy concerns raised within the agency, other branches of DHS and law enforcement remain eager to use phone location data.

Records show that the Department of Justice also expressed interest in using data from Venntel, as did a police department in Cincinnati, Ohio, which sought to use the location data to address the opioid crisis.

And the agencies don't show any signs of slowing their use of location data. ICE signed another contract with Venntel in November, which is set to expire in June 2023.

Wessler called on the Biden administration to release an internal memo that the DHS uses to justify buying and using location data. The memo's existence was first reported by BuzzFeed News.

While proposed privacy laws seek to tackle location data collection, data sales to government agencies have a carveout in the latest draft of the American Data Privacy and Protection Act, H.R. 8152, a bill that would make it more difficult to collect and sell sensitive data, which includes location data.

In April 2021, Sen. Ron Wyden (D-Ore.) introduced the Fourth Amendment is Not For Sale Act, S. 1265, which looks to stop agencies from buying Americans'

data from data brokers without a warrant.

“Despite claims by data brokers, no one who downloads an app thinks they are giving permission to waive their 4th Amendment rights and let the government follow their every move,” Wyden said in an email. “The DHS inspector general has notified my office it has initiated an investigation of the department’s purchase of location data, which I’m looking forward to reviewing closely.”

CORRECTION: An earlier version of this article misstated the status of an ICE contract with Venntel, which ended in 2021. The story has also been updated with additional information about DHS’ review of privacy and legal concerns with the use of Venntel data.

FILED UNDER: PRIVACY, TECHNOLOGY, DEPARTMENT OF HOMELAND SECURITY, PHONES,