THE WALL STREET JOURNAL.

FEDERAL AGENCIES USE CELLPHONE LOCATION DATA FOR IMMIGRATION ENFORCEMENT

Commercial database that maps movements of millions of cellphones is deployed by immigration and border authorities

By Byron Tau and Michelle Hackman
February 7, 2020

WASHINGTON – The Trump administration has bought access to a commercial database that maps the movements of millions of cellphones in America and is using it for immigration and border enforcement, according to people familiar with the matter and documents reviewed by The Wall Street Journal.

The location data is drawn from ordinary cellphone apps, including those for games, weather and e-commerce, for which the user has granted permission to log the phone's location.

The Department of Homeland Security has used the information to detect undocumented immigrants and others who may be entering the U.S. unlawfully, according to these people and documents.

U.S. Immigration and Customs Enforcement, a division of DHS, has used the data to help identify immigrants who were later arrested, these people said. U.S. Customs and Border Protection, another agency under DHS, uses the information to look for cellphone activity in unusual places, such as remote stretches of desert that straddle the Mexican border, the people said.

The federal government's use of such data for law enforcement purposes hasn't previously been reported.

Experts say the information amounts to one of the largest known troves of bulk data being deployed by law enforcement in the U.S. – and that the use appears to be on firm legal footing because the government buys access to it from a commercial vendor, just as a private company could, though its use hasn't been tested in court.

"This is a classic situation where creeping commercial surveillance in the private sector is now bleeding directly over into government," said Alan Butler, general counsel of the Electronic Privacy Information Center, a think tank that pushes for stronger privacy laws.

According to federal spending contracts, a division of DHS that creates experimental products began buying location data in 2017 from Venntel Inc. of Herndon, Va., a small company that shares several executives and patents with Gravy Analytics, a major player in the mobile-advertising world.

In 2018, ICE bought $190,000 worth of Venntel licenses. Last September, CBP bought $1.1 million in licenses for three kinds of software, including Venntel subscriptions for location data.

The Department of Homeland Security and its components acknowledged buying access to the data, but wouldn't discuss details about how they are using it in law-enforcement operations. People familiar with some of the efforts say it is used to generate investigative leads about possible illegal border crossings and for detecting or tracking migrant groups.

CBP has said it has privacy protections and limits on how it uses the location information. The agency says that it accesses only a small amount of the location data and that the data it does use is anonymized to protect the privacy of Americans.

"While CBP is being provided access to location information, it is important to note that such information doesn't include cellular phone tower data, is not ingested in bulk and doesn't include the individual user's identity," said a CBP spokesman. Tower data from cellphone companies, which can locate a specific phone, has been singled out by the Supreme Court for extra protection.

ICE initially was given access to the data for use by its criminal investigators who track human- and drug-smuggling organizations, according to people familiar with the activity. Subsequently, the data was shared with ICE's arm that carries out deportations, one of the people said.

"We do not discuss specific law-enforcement tactics or techniques, or discuss the existence or absence of specific law-enforcement-sensitive capabilities," said ICE spokesman Bryan Cox. Mr. Cox said the agency "generally" doesn't use location data for routine deportation operations.

The data was used to detect cellphones moving through what was later discovered to be a tunnel created by drug smugglers between the U.S. and Mexico that terminated in a closed Kentucky Fried Chicken outlet on the U.S. side near San Luis, Ariz., said people with knowledge of the operation.

The data tracking contributed to the 2018 arrest of the defunct restaurant's owner, Ivan Lopez, on conspiracy charges related to the construction of the tunnel, the people said. But police records of the incident make no mention of the use of data showing cellphones crossing the border in an unusual location, attributing the case instead to a routine traffic stop.

The San Luis police department "has always worked well with other entities," including federal law enforcement, said Lt. Marco Santana, a spokesman, who declined to comment further. A CBP spokesman declined to comment. Lawyers for Mr. Lopez, who pleaded guilty, declined to comment.

Contracting records show the federal government is buying the location data from Venntel. Venntel, in turn, purchased the information from private marketing companies that sell the location data of millions of cellphones to advertisers, people familiar with the matter say.

Venntel's president, Chris Gildea, said, "We are not able to comment on behalf of our customers, and any inquiries on this contract should be directed to DHS."

The company's website says that it "supports our national interests through technological innovation, data reliability and proven results." It says it offers defense-intelligence and national-security services.

Digital marketing, a multibillion-dollar industry, uses such data to deliver, for example, an ad for a restaurant or store to a nearby consumer who is scrolling through Facebook on a phone.

Divisions of DHS, ICE and CBP have purchased licenses to use Venntel's software as part of analytical programs for border security and other law-enforcement efforts, federal records show. Separate government documents make oblique references to such data being used to track, among other things, tunnels along the border.

The data is pseudonymised – meaning that each cellphone is represented by an alphanumeric advertising identifier that isn't linked to the name of the cellphone's owner. Cellphone users can change their identifier in their phone's settings menu or limit the apps that have access to their location.

Though anonymized, such mobile location data can be used to identify and track individuals based on their real-world behavior, the New York Times reported in December.

Marketing data is widely used by the government to gather intelligence abroad, say people familiar with the matter. But those contracts are frequently classified, so the extent to which intelligence agencies are buying such data cannot be determined.

In 2018, the Supreme Court issued a landmark ruling in the case Carpenter v. United States saying that geographic location data drawn from cellphones in the U.S. is a specially protected class of information because it reveals so much about Americans. The court put limits on law enforcement's ability to obtain such data directly from cellphone companies without court supervision.

But the federal government has essentially found a workaround by purchasing location data used by marketing firms rather than going to court on a case-by-case basis. Because location data is available through numerous commercial ad exchanges, government lawyers have approved the programs and concluded that the Carpenter ruling doesn't apply.

"In this case, the government is a commercial purchaser like anybody else. Carpenter is not relevant," said Paul Rosenzweig, a former DHS official who is a resident senior fellow at the R Street Institute, a conservative and libertarian think tank that promotes free markets. "The government is just buying a widget."