ACLU

NEWS & COMMENTARY

New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data

Thousands of previously unreleased records illustrate how government agencies sidestep our Fourth Amendment rights.

Shreya Tewari, Brennan Fellow, ACLU Speech, Privacy, and Technology Project

Fikayo Walter-Johnson, Paralegal, ACLU's Speech, Privacy, and Technology Project

Today, the ACLU published thousands of pages of previously unreleased records about how Customs and Border Protection, Immigration and Customs Enforcement, and other parts of the Department of Homeland Security are sidestepping our Fourth Amendment right against unreasonable government searches and seizures by buying access to, and using, huge volumes of people's cell phone location information quietly extracted from smartphone apps.

The records, which the ACLU obtained over the course of the last year through a Freedom of Information Act (FOIA) lawsuit, shed new light on the government's ability to obtain our most private information by simply opening the federal wallet. These documents are further proof that Congress needs to pass the Fourth Amendment Is Not For Sale Act, which would end law enforcement agencies' practice of buying their way around the Fourth Amendment's warrant requirement.

ICE's and CBP's warrantless purchase of access to people's sensitive location information was first reported by The Wall Street Journal in early 2020. After the news broke, we submitted a FOIA request to DHS, ICE, and CBP, and we sued to force the agencies to respond to the request in December 2020. Although the litigation is ongoing, we are now making public the records that CBP, ICE, the U.S. Secret Service, the U.S. Coast Guard, and several offices within DHS Headquarters have provided us to date.

The released records shine a light on the millions of taxpayer dollars DHS used to buy access to cell phone location information being aggregated and sold by two shadowy data brokers, Venntel and Babel Street. The documents expose those companies' — and the government's — attempts to rationalize this unfettered sale of massive quantities of data in the face of U.S. Supreme Court precedent protecting similar cell phone location data against warrantless government access.

Four years ago, in *Carpenter v. United States*, the Supreme Court ruled that the government needs a warrant to access a person's cellphone location history from cellular service providers because of the "privacies of life" those records can reveal. That case hinged on a request for one suspect's historical location information over a several-month period. In the documents we received over the past year, we found Venntel marketing materials sent to DHS explaining how the company collects more than 15 billion location points from over 250 million cell phones and other mobile devices *every day*.

With this data, law enforcement can "identify devices observed at places of interest," and "identify repeat visitors, frequented locations, pinpoint known associates, and discover pattern of life," according to a Venntel marketing brochure. The documents belabor how precise and illuminating this data is, allowing "pattern of life analysis to identify persons of interest." By searching through this massive trove of location information at their whim, government investigators can identify and track specific individuals or everyone in a particular area, learning details of our private activities and associations.

The government should not be allowed to purchase its way around

bedrock constitutional protections against unreasonable searches of our private information.

In the face of the obvious privacy implications of warrantless access to this information, these companies and agencies go to great lengths to rationalize their actions. Throughout the documents, the cell phone location information is variously characterized as mere "digital exhaust" and as containing no "PII" (personally identifying information) because it is associated with a cell phone's numerical identifier rather than a name — even though the entire purpose of this data is to be able to identify and track people. The records also assert that this data is "100 percent opt-in," that cell phone users "voluntarily" share the location information, and that it is collected with consent of the app user and "permission of the individual." Of course, that consent is a fiction: Many cell phone users don't realize how many apps on their phones are collecting GPS information, and certainly don't expect that data to be sold to the government in bulk.

In scattered emails, some DHS employees raised concerns, with internal briefing documents even acknowledging that "[l]egal, policy, and privacy reviews have not always kept pace with the new and evolving technologies." Indeed, in one internal email, a senior director of privacy compliance flagged that the DHS Office of Science & Technology appeared to have purchased access to Venntel even though a required Privacy Threshold Assessment was never approved. Several email threads highlight internal confusion in the agency's privacy office and potential oversight gaps in the use of this data — to the extent that all projects involving Venntel data were temporarily halted because of unanswered privacy and legal questions.

Nonetheless, DHS has pressed on with these bulk location data purchases. And the volume of people's sensitive location information obtained by the agency is staggering. Among the records released to us by CBP were seven spreadsheets containing a small subset of the raw location data purchased by the agency from Venntel. (Although the location coordinates for each spreadsheet entry are redacted, the date and time of each location point are not.) The 6,168 pages of location records we reviewed contain

approximately 336,000 location points obtained from people's phones. 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, meaning it is just a small subset of the total volume of people's location information available to the agency.

The documents also highlight particular privacy concerns for people living near our nation's borders. A 2018 DHS internal document proposed using the location data to identify patterns of illegal immigration, threatening to indiscriminately sweep in information about people going about their daily lives in border communities. There is also the potential for local law enforcement entities to gain access to this large mass of data in ways that they would not usually be able to. This is illustrated by a troubling request to DHS from a local police department in Cincinnati, seeking location data analytics pertaining to opioid overdoses in their jurisdiction.

DHS still owes us more documents, but whatever they show, it is already abundantly clear that law enforcement's practice of buying its way around the core protections of the Fourth Amendment must stop. There is bipartisan legislation in Congress right now that would do exactly that. The Fourth Amendment Is Not For Sale Act would require the government to secure a court order before obtaining Americans' data, such as location information from our smartphones, from data brokers. The principle here is simple: The government should not be allowed to purchase its way around bedrock constitutional protections against unreasonable searches of our private information. There is no end run around the Fourth Amendment.

Lawmakers must seize the opportunity to end this massive privacy invasion without delay. Each day without action only allows the government's covert trove of our personal information to grow.