Military Unit That Conducts Drone Strikes Bought Location Data From Ordinary Apps

Joseph Cox ⋮ 7-9 minutes

Image: U.S. Air National Guard

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

A division of the Iowa Air National Guard that carries out overseas intelligence missions, performs reconnaissance, and conducts strikes with Reaper drones recently bought access to location data harvested from ordinary apps installed on peoples' smartphones, Motherboard has found. The tool, called Locate X, lets users search by a specific area and see which devices were present in that location at a particular point in time.

The news shows the continued use of commercial location data by the armed forces. The Iowa National Guard declined to say what it was using the data for. The news also comes as lawmakers demand answers from military and intelligence chiefs on purchases of location data. Motherboard previously reported how a Muslim-focused prayer app provided data to a company called X-Mode whose customers include military contractors, and that Special Operations Command (SOCOM) also bought access to Locate X.

> *Are you a government user of location data? Or do you work at a location data company? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.*

The specific part of the military that bought the Locate X product in the new contract was the 132d Wing of the Iowa Air National Guard, based out of Des Moines, Iowa, public procurement records show. The contract was for just over $35,000, and includes "Premium data feed—Locate X—1 year subscription," according to the records.

The 132d Wing is made of various units that are tasked with gathering intelligence, executing targets, providing medical assistance, and cyberspace operations.

"The mission of the 132d Wing Operations Group is to deploy worldwide and execute directed long-endurance coverage of targets while providing intelligence, surveillance, and reconnaissance as well as dynamic execution of targets," the division's website reads. The Drone Databook, a research

document written by Dan Gettinger from the Center for the Study of the Drone at Bard College, says the 132d Wing Operations Group flies MQ-9 Reaper drones.

The 132d Wing used to fly F-16s, but converted to exclusively flying drones in 2014. That move proved controversial, with some Iowans protesting outside the base. "It brings war directly, physically to Des Moines," Gilbert Landolt, then-president of the Des Moines Veterans for Peace, told the *Des Moines Register* in 2014.

The primary mission of another part of the 132d Wing, the Intelligence Group, is to provide "intelligence, surveillance, and reconnaissance (ISR) products, applications, capabilities, and resources, to include cyber and geospatial forces and expertise," according to the 132d website.

The 132d Wing has also manned COVID-19 test sites in Iowa and helped contact tracing efforts during the pandemic.

"The Iowa National Guard did request the purchase of the software Locate X," Major Katherine Headley, director of public affairs at the Iowa National Guard, told Motherboard in an email. Headley declined to say exactly how the Iowa Air National Guard will use the data.

"This product will be used to support our federal mission requirements overseas. In regards to its use, we plan to strictly adhere to all policies and procedures along with federal and constitutional laws," the statement added.

Locate X is made by a company called Babel Street. As *Protocol* first reported in March last year, Locate X uses location data from apps installed on peoples' phones. Locate X clients included Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), and the Secret Service, *Protocol* reported. Motherboard later obtained a Secret Service document confirming the agency had bought access to Locate X.

Babel Street did not respond to a request for comment.

According to a Department of Homeland Security document, Babel Street "re-hosts" location data obtained by Venntel, another government contractor. Venntel sells a similar location data product to various law enforcement agencies, including ICE, the IRS, and CBP, that the company builds by collating information from ordinary apps.

In the internal Department of Homeland Security document discussing the purchase of Venntel data obtained by Motherboard through a Freedom of Information Act (FOIA) request, an official writes that "Babel Street basically re-hosts Venntel's data at a greater cost and with significant constraints on data access." Venntel, meanwhile, "offers broad and uncontrolled access to the underlying dataset," the document adds. Motherboard has previously shown with an internal CBP document that Venntel's dataset is "global," and this DHS document adds that it "brings together 80,000 mobile applications into a single source."

Although Venntel's data is pseudonymized, a former Venntel worker previously told Motherboard that "If you search a certain house, you're only going to get three of four different signals out of there. I think from that standpoint, you could definitely try and identify specific people." Now with the revelation that Babel Street's dataset is based on Venntel's, the issue of deanonyimation may also apply to Locate X.

This shows that the pipeline of location data from apps, through contractors, and eventually to government agencies is controlled to a higher degree by Venntel than previously known. Apps that end up providing data to Venntel may also be ultimately providing it to Babel Street and the Locate X product too.

Venntel did not respond to a request for comment.

Motherboard and Norwegian media organization NRK previously showed how a company called Predicio was connected to the supply chain of data to Venntel. Using a leaked Predicio dataset of real peoples' locations as well as a technical analysis of apps, Motherboard also found multiple apps providing data to Predicio, including Salaat First (Prayer Times), a Muslim-focused app which has been downloaded more than 10 million times from the Google Play Store. Salaat First collected and sold this information likely without the informed consent of many users, as the app did not present its privacy policy to users inside the app itself. After Motherboard's report, Google banned Predicio from the Play Store.

In February, over a dozen lawmakers led by Representative Mark Pocan including Ilhan Omar, Alexandria Ocasio-Cortez, and Rashida Tlaib, demanded an investigation into how the U.S. military has purchased and used location data.

"This disclosure raises serious concern that such information is advancing systematic, warrantless surveillance of the Muslim-American community contrary to the privacy protections guaranteed in the U.S. Constitution," the letter read. The letter came in response to Motherboard's Muslim Pro investigation.

A memo obtained by the office of Senator Ron Wyden from the Defense Intelligence Agency (DIA) said DIA staff had been granted permission to query a set of U.S. commercial location data without a warrant five times within the past two and a half years, *The New York Times* reported. *The Wall Street Journal* reported this data came from a National Geospatial-Intelligence Agency program that obtains the data directly from the apps.

Subscribe to our cybersecurity podcast CYBER, here.

ORIGINAL REPORTING ON EVERYTHING THAT MATTERS IN YOUR INBOX.