How the U.S. Military Buys Location Data from Ordinary Apps

10.06.20

Location data

The U.S. military is buying the granular movement data of people around the world, harvested from innocuous-seeming apps, Motherboard has learned. The most popular app among a group Motherboard analyzed connected to this sort of data sale is a Muslim prayer and Quran app that has more than 98 million downloads worldwide. Others include a Muslim dating app, a popular Craigslist app, an app for following storms, and a "level" app that can be used to help, for example, install shelves in a bedroom.

Through public records, interviews with developers, and technical analysis, Motherboard uncovered two separate, parallel data streams that the U.S. military uses, or has used, to obtain location data. One relies on a company called Babel Street, which creates a product called Locate X. U.S. Special Operations Command (USSOCOM), a branch of the military tasked with counterterrorism, counterinsurgency, and special reconnaissance, bought access to Locate X to assist on overseas special forces operations. The other stream is through a company called X-Mode, which obtains location data directly from apps, then sells that data to contractors, and by extension, the military.

The news highlights the opaque location data industry and the fact that the U.S. military, which has infamously used other location data to target drone strikes, is purchasing access to sensitive data. Many of the users of apps involved in the data supply chain are Muslim, which is notable considering that the United States has waged a decades-long war on predominantly

Muslim terror groups in the Middle East, and hundreds of thousands of civilians have died during military intervention in Pakistan, Afghanistan, and Iraq. Motherboard does not know of any specific operations in which this type of app-based location data has been used by the U.S. military.

The apps sending data to X-Mode include Muslim Pro, an app that reminds users when to pray and what direction Mecca is in relation to the user's current location. The app has been downloaded over 50 million times on Android, according to the Google Play Store, and over 98 million in total across other platforms including iOS, according to Muslim Pro's website.

"The Most Popular Muslim App!," Muslim Pro's website reads. The app also includes passages and audio readings from the Quran. (After publication of this piece, Muslim Pro said it will no longer share data with X-Mode).

Another app that sent data to X-Mode was Muslim Mingle, a dating app that has been downloaded more than 100,000 times.

> ***Do you work at Babel Street, X-Mode, Venntel, or one of the apps mentioned in this piece? Did you used to, or know anything else about the location data industry? 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.***

Some app developers Motherboard spoke to were not aware who their users' location data ends up with, and even if a user examines an app's privacy policy, they may not ultimately realize how many different industries, companies, or government agencies are buying some of their most sensitive data. U.S. law enforcement purchase of such information has raised questions about authorities buying their way to location data that may ordinarily require a warrant to access. But the USSOCOM contract and

additional reporting is the first evidence that U.S. location data purchases have extended from law enforcement to military agencies.

USSOCOM bought access to Locate X, a location data product from a company called Babel Street, according to procurement records uncovered by Motherboard. A former Babel Street employee described to Motherboard how users of the product can draw a shape on a map, see all devices Babel Street has data on in that location, and then follow a specific device around to see where else it has been.

The Locate X data itself is anonymized, but the source said "we could absolutely deanonymize a person." Babel Street employees would "play with it, to be honest," the former employee added.

USSOCOM purchased the "additional software licenses" for Locate X and another product focused on text analysis called Babel X in April, according to the public records. The bundle of additional licenses cost around $90,600, the records show.

In a statement, Navy Cmdr. Tim Hawkins, a U.S. Special Operations Command spokesperson, confirmed the Locate X purchase, and added "Our access to the software is used to support Special Operations Forces mission requirements overseas. We strictly adhere to established procedures and policies for protecting the privacy, civil liberties, constitutional and legal rights of American citizens."

A Babel Street document available online says that "Within the technical specifications of the Locate X Data, Customer's use of the Locate X Data is not limited by the number of search queries." The document says the location data may not always be accurate.

Babel Street did not respond to multiple requests for comment.

In March, tech publication Protocol first reported that U.S. law enforcement agencies such as Customs and Border Protection (CBP) and Immigration and Customs Enforcement (ICE) were using Locate X. Motherboard then obtained an internal Secret Service document confirming the agency's use of the technology. Some government agencies, including CBP and the Internal Revenue Service (IRS), have also purchased access to location data from another vendor called Venntel.

"In my opinion, it is practically certain that foreign entities will try to leverage (and are almost certainly actively exploiting) similar sources of private platform user data. I think it would be naïve to assume otherwise," Mark Tallman, assistant professor at the Department of Emergency Management and Homeland Security at the Massachusetts Maritime Academy, told Motherboard in an email.

THE SUPPLY CHAIN

Some companies obtain app location data through bidstream data, which is information gathered from the real-time bidding that occurs when advertisers pay to insert their adverts into peoples' browsing sessions. Firms also often acquire the data from software development kits (SDKs).

Location data firm X-Mode, which is different than Babel Street, encourages app developers to incorporate its SDK, essentially a bundle of code, into their own apps. The SDK then collects the app users' location data and sends it to X-Mode; in return, X-Mode pays the app developers a fee based on how many users each app has. An app with 50,000 daily active users in the U.S., for example, will earn the developer $1,500 a month, according to X-Mode's website.

In a recent interview with CNN, X-Mode CEO Joshua Anton said the company tracks 25 million devices inside the United States every month,

and 40 million elsewhere, including in the European Union, Latin America, and the Asia-Pacific region. X-Mode previously told Motherboard that its SDK is embedded in around 400 apps.

In October the Australian Competition & Consumer Commission published a report about data transfers by smartphone apps. A section of that report included the endpoint—the URL some apps use—to send location data back to X-Mode. Developers of the Guardian app, which is designed to protect users from the transfer of location data, also published the endpoint. Motherboard then used that endpoint to discover which specific apps were sending location data to the broker.

Motherboard used network analysis software to observe both the Android and iOS versions of the Muslim Pro app sending granular location data to the X-Mode endpoint multiple times. Will Strafach, an iOS researcher and founder of Guardian, said he also saw the iOS version of Muslim Pro sending location data to X-Mode.

The data transfer also included the name of the wifi network the phone was currently collected to, a timestamp, and information about the phone such as its model, according to Motherboard's tests.

Muslim Pro did not respond to multiple requests for comment.

Other apps sending data to X-Mode included the "Accupedo" step counter app, which has been downloaded more than 5 million times according to the app's page on the Google Play Store; the "CPlus for Craigslist" app which lets users more easily search Craigslist, and has more than one million downloads; and "Global Storms," an app for following hurricanes, typhoons, and tropical storms. The app has been downloaded more than a million times.

As well as the prayer app, Motherboard also installed the Muslim Mingle dating app onto an Android phone and observed the app sending precise geolocation coordinates of the phone's current location and wifi network name to X-Mode multiple times. Vietnam-based Mingle, the developer behind the app as well as other dating apps such as Black Mingle which is marketed specifically towards Black people, did not respond to multiple requests for comment.

> *"It is safe to say from this context that the reasonable consumer—who is not a tech person—would not have military uses of their data in mind, even if they read the disclosures."*

Motherboard found another network of dating apps that look and operate nearly identically to Mingle, including sending location data to X-Mode. Motherboard installed another dating app, called Iran Social, on a test device and observed GPS coordinates being sent to the company. The network of apps also includes Turkey Social, Egypt Social, Colombia Social, and others focused on particular countries.

X-Mode then sells access to this sort of data to a wide range of different clients. Motherboard has previously shown that one of those clients includes a private intelligence firm whose goal is to use location data to track people down to their "doorstep." X-Mode has also demonstrated how its data can be used to follow where people in COVID-19 hotspots travelled to after potentially exposing one another to the coronavirus.

Those clients have also included U.S. military contractors, Motherboard found. Included in archived versions of the "Trusted Partners" section on its website, X-Mode lists Sierra Nevada Corporation and Systems & Technology

Research as customers. Sierra Nevada Corporation builds combat aircraft for the U.S. Air Force, and supports contractor Northrop Grumman in the development of cyber and electronic warfare capabilities for the U.S. Army. Systems & Technology Research works with the Army, Navy, and Air Force according to procurement records, and offers "data analytics" support to intelligence analysts, according to its website.

Senator Ron Wyden told Motherboard in a statement that X-Mode said it is selling location data harvested from U.S. phones to U.S. military customers.

"In a September call with my office, lawyers for the data broker X-Mode Social confirmed that the company is selling data collected from phones in the United States to U.S. military customers, via defense contractors. Citing non-disclosure agreements, the company refused to identify the specific defense contractors or the specific government agencies buying the data," the statement read.

X-Mode told Motherboard in an email that the company "does not work with Sierra Nevada or STR" but did not deny they were once customers. (As Motherboard has continued to report on the company and the office of Senator Ron Wyden has carried out its own investigation into the location data industry, X-Mode has removed multiple company names from the Trusted Partners page, including Sierra Nevada Corporation).

"X-Mode licenses its data panel to a small number of technology companies that may work with government military services, but our work with such contractors is international and primarily focused on three use cases: counter-terrorism, cybersecurity and predicting future COVID-19 hotspots," X-Mode added in its email to Motherboard.

Several app developers who work with X-Mode told Motherboard they did not know their users' location data was being sent to defense contractors.

"I was not aware that X-Mode was selling those data to some military contractors," Nicolas Dedouche, CEO at app development firm Mobzapp, told Motherboard in an email. Mobzapp made a screen sharing app for Android that sends location data to X-Mode and has been downloaded more than a million times. "I cannot be aware X-Mode is working with military contractors if they do not clearly mention it somewhere," he added.

"As an app developer I do care with whom I'm contracting with," Antoine Vianey, the developer behind the app "Bubble level" that has been downloaded more than ten million times, said. But they added "to be totally clear I missed the two you sent me!" referring to Sierra Nevada Corporation or Systems & Technology Research.

YanFlex, the developer behind the CPlus for Craigslist app, also did not appear to know that X-Mode works with military contractors. "I don't think what you described is true," they incorrectly wrote in an email when asked for comment.

Accupedo, the step tracking app, told Motherboard in an email that "We do not speak publicly about the relationships we have with our partners. If you are interested in our relationship with X-Mode, you can contact them directly."

"We are comfortable with how X-Mode uses location data," Neil Kelly, president and chief developer of Kelly Technology, which makes the Global Storms app, told Motherboard in an email.

"I cannot be aware X-Mode is working with military

contractors if they do not clearly mention it somewhere."

On its website, X-Mode describes its "best practices" in how it obtains consent from app users to gather their location data. As well as the operating system level permission to access location data, and a privacy policy, X-Mode says it also "provide[s] our publisher partners with recommended language both to ease their privacy navigation and to have brand consistency with the way we present our data collection and sharing to users across our panel."

The Bubble level terms of service pop-up that appears when a user first opens the app says the software may collect anonymous location data "to power tailored ads, location-based analytics, attribution and other civic, market and scientific research about traffic and crowds." The Global Storms app provided a similar dialogue in Motherboard's tests. The disclaimers themselves do not explicitly say the data will be sent to military contractors or a private intelligence firm. Some app privacy policies as well as X-Mode's own policy says the company may use location data "for disease prevention and research, security, anti-crime and law enforcement."

"I don’t know how many provide consent," Kelly said of the Global Storms app's users.

But some apps that are harvesting location data on behalf of X-Mode are essentially hiding the data transfer. Muslim Pro does not mention X-Mode in its privacy policy, and did not provide any sort of pop-up when installing or opening the app that explained the transfer of location data in detail. The privacy policy does say Muslim Pro works with Tutela and Quadrant, two other location data companies, however. Motherboard did observe data

transfer to Tutela.

The Muslim Mingle app provided no pop-up disclosure in Motherboard's tests, nor does the app's privacy policy mention X-Mode at all. Iran Social, one of the apps in the second network of dating apps that used much of the same code, also had the same lack of disclosures around the sale of location data.

After Motherboard's tests and being approached for comment, Mingle added a new opt-in dialogue box that does say the Muslim Mingle app collects location data. Innovate Dating, the company behind Iran Social, did the same.

X-Mode clarified in an email to Motherboard that its partner apps are contractually obligated to follow relevant data protection laws and obtain consent, rather than there being a technical mechanism in place that stops collection without informed consent.

"We require all apps on our platform to follow all applicable privacy and data protection laws and platform guidelines (e.g., Google/Android and Apple/OS). Our app partners are contractually obligated to comply with these requirements. These requirements include obtaining all required consents and permissions (including applicable opt-ins and providing means to opt-out) from end-users for any data collection and use," X-Mode wrote in an email. "We provide our app partners with consent management tools to help them comply with these requirements, and we audit our publisher's apps for conformance. When we learn of any alleged issue of nonconformance by an app on our platform, we take this seriously, and we investigate thoroughly and remediate as necessary," it added.

When shown some of the apps' lackluster privacy disclosures, Chris Hoofnagle, faculty director at the Berkeley Center for Law & Technology, told

Motherboard in an email "The question to ask is whether a reasonable consumer of these services would foresee of these uses and agree to them if explicitly asked. It is safe to say from this context that the reasonable consumer—who is not a tech person—would not have military uses of their data in mind, even if they read the disclosures."

Sierra Nevada Corporation was behind a widely discredited report that used location data to conclude that a disruptive event happened at the Wuhan Institute of Virology in October 2019.

Neither Sierra Nevada Corporation or Systems & Technology Research responded to multiple requests for comment.

Clarification: A sentence about civilian casualties has been updated to note that hundreds of thousands of civilians have died during the U.S.'s military interventions in the Middle East.