

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

By [Joseph Cox](#)

Global Research, November 17, 2020

[Vice](#) 16 November 2020

Region: [USA](#)

Theme: [Intelligence](#)

A Muslim prayer app with over 98 million downloads is one of the apps connected to a wide-ranging supply chain that sends ordinary people's personal data to brokers, contractors, and the military.

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 has killed [hundreds of thousands of civilians](#) during its military operations 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. 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 jfc Cox@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.

[Read complete article here.](#)

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Featured image is by Cathryn Virginia via Vice

The original source of this article is [Vice](#)
Copyright © [Joseph Cox](#), [Vice](#), 2020

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Joseph Cox](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca