Pentagon probes fitness-app use after map shows sensitive sites (Update)

January 29 2018

The concentration of activity at a military base or along a patrol route could be used by insurgent groups to plan attacks on personnel

The US military is reviewing how troops use fitness trackers and other devices, the Pentagon said Monday after an exercise-logging company

[published a map revealing potentially sensitive information](#) about US and allied forces in places including the Middle East.

The map, made by Strava Labs, shows the movements of its app users around the world, indicating the intensity of travel along a given path.

The company says it offers "a direct visualization of Strava's global network of athletes."

In large cities and well-known locations, the highlighted routes are hardly surprising, with dense urban areas lit up brightly compared to unpopulated areas or places without many app users.

In Iraq and Syria, much of the terrain is essentially dark, but viewers can easily spot beacons of activity in remote places where military bases are located, presumably indicating favorite jogging or walking routes.

Such activity in inaccessible desert compounds in the Middle East or around insurgent-held cities makes it clear the data are being gleaned from military users.

'Situational awareness'

"We are going to take a look at the Department-wide policy to ensure that we have operational security and force protection," Colonel Rob Manning, a Pentagon spokesman, told reporters.

"Recent data releases emphasize the need for situational awareness."

Strava's map highlights a series of well-known military bases in Iraq, in detail.

Similarly in Syria, areas that appear to be bases in the north—where US

troops are aiding local partners in the fight against the Islamic State group—are lit up brightly against an otherwise dark background.

The concentration of activity at a base or along a patrol route could be used by insurgent groups to plan attacks on military personnel.

Manning said the review would look at the use of all wearable electronics and smartphones.

Commanders already have the tools at their disposal to ensure "force protection," he added.

"DoD personnel are advised to emplace strict privacy settings on wireless technologies and applications, and such technologies are forbidden at specific DoD sites and during specific activities," he said, referring to the Department of Defense.

Manning said he was not aware of any request to Strava to take down its map.

'Security nightmare'

But the whole issue could have been fairly easily avoided.

According to Strava, "athletes with the Metro/heatmap opt-out privacy setting have all data excluded" from the mapping project.

Jeffrey Lewis, director of the Middlebury Institute of International Studies' East Asia Nonproliferation program, said the data revelations represent a "security nightmare" for governments around the world.

"Anyone with access to the data could make a pattern-of-life map for individual users, some of whom may be very interesting to foreign

intelligence services," he wrote in a column on the Daily Beast news site.

If anyone were to hack Strava, he said, they might be able to connect a particular user with a particular route.

"That's charming when it's a celebrity uploading a run. But what about a soldier?" he added, noting that an adversary could track a soldier as he or she moved from one assignment to the next.

Privacy tools

Strava referred queries to its blog posting last year in which it said "nothing is more important" than the safety of its users.

"Whether you are concerned about someone knowing where you are, where you ran or where you live, we've got the tools to help you take control," the company said.

"We work hard to make it easy for athletes to have access to the information and tools they need to control their privacy, whether you're using our mobile app or a GPS device."

Ned Price, a former CIA official who was seconded as a national security adviser to former president Barack Obama, said that "capable adversaries" had almost certainly been harvesting such data for years.

"Imagine how many similar data sources are out there we're ignorant of (because) it's not posted online," he wrote on Twitter.

© 2018 AFP