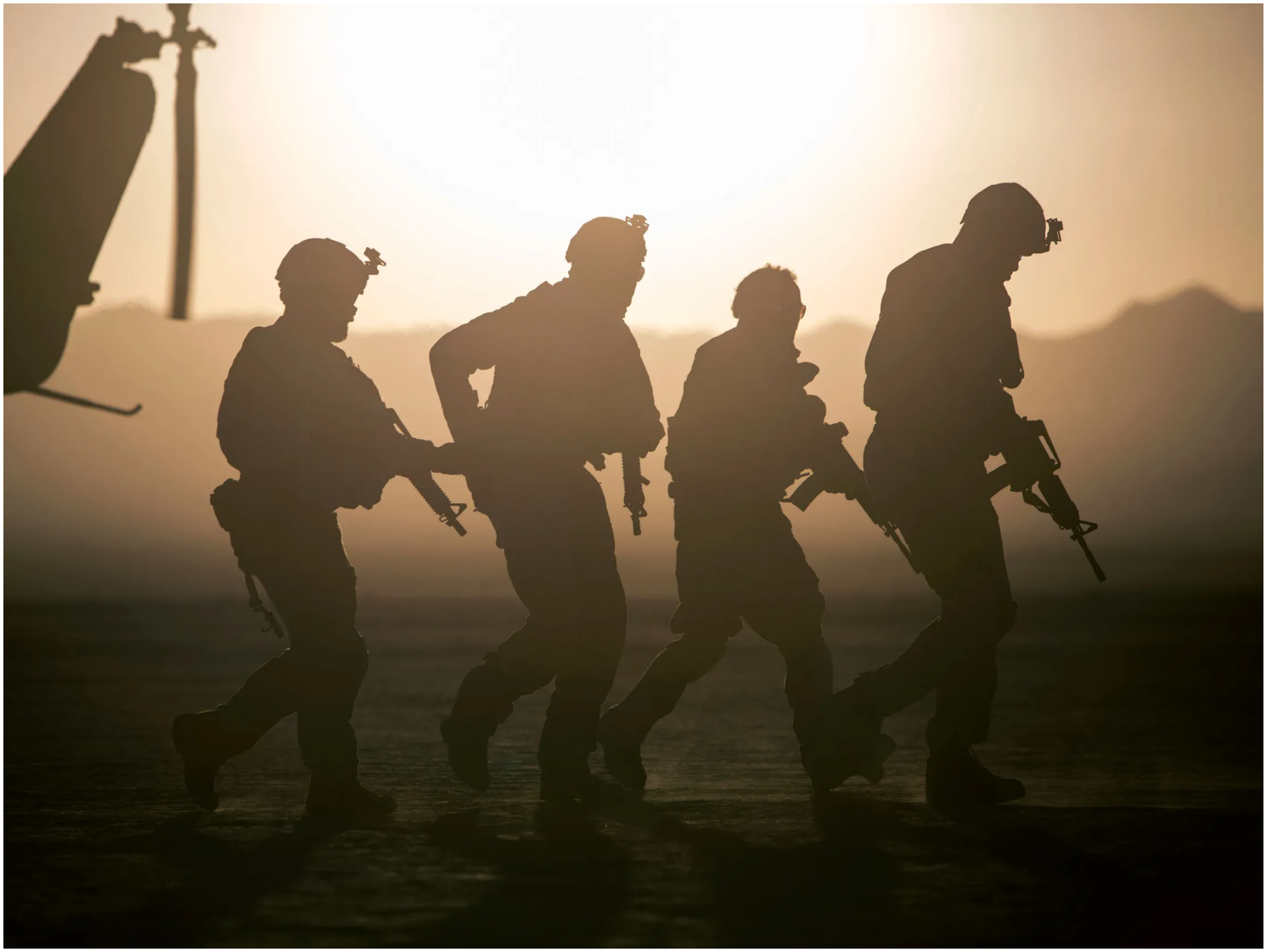
JEREMY HSU SECURITY JAN 29, 2018 7:14 PM

The Strava Heat Map and the End of Secrets

The US military is reexamining security policies after fitness tracker data shared on social media revealed bases and patrol routes



After fitness data service Strava revealed bases and patrol routes with an online "heat map," the US military is reexamining its security policies for the social media age. RAPHYE ALEXIUS/GETTY IMAGES

SAVE

A MODERN EQUIVALENT of the World War II era warning that "loose lips sink ships" may be "FFS don't share your Fitbit data on duty." Over the weekend, researchers and journalists raised the alarm about how anyone can identify secretive military bases and patrol routes based on public data shared by a "social network for athletes" called Strava.

This past November, the San Francisco-based Strava announced a huge update to its global heat map of user activity that displays 1 billion activities—including running and cycling routes—undertaken by exercise enthusiasts wearing Fitbits or other wearable fitness trackers. Some Strava users appear to work for certain militaries or various intelligence agencies, given that knowledgeable security experts quickly connected the dots between user activity and the known bases or locations of US military or intelligence operations. Certain analysts have suggested the data could reveal individual Strava users by name.

But the biggest danger may come from potential adversaries figuring out "patterns of life," by tracking and even identifying military or intelligence agency personnel as they go about their duties or head home after deployment. These digital footprints that echo the real-life steps of individuals underscore a greater challenge to governments and ordinary citizens alike: each person's connection to online services and personal devices makes it increasingly difficult to keep secrets.

All Your Base Are Belong to Us

The revelations began unspooling at a rapid pace after Nathan Ruser, a student studying international security at the Australian National University, began posting his findings via Twitter on Saturday afternoon. In a series of images, Ruser pointed out Strava user activities potentially related to US military forward operating bases in Afghanistan, Turkish military patrols in Syria, and a possible guard patrol in the Russian operating area of Syria.

Other researchers soon followed up with a dizzying array of international examples, based on cross-referencing Strava user activity with Google Maps and prior news reporting: a French military base in Niger, an Italian military base in Djibouti, and even CIA "black" sites. Several experts observed that the Strava heatmap seemed best at revealing the presence of mostly Western military and civilian operations in developing countries.

Many locations of military and intelligence agency bases pointed out by researchers and journalists had already been previously revealed through other public sources. But the bigger worry from an operations security standpoint was how Strava's activity data could be used to identify interesting individuals, and track them to other sensitive or secretive locations. Paul Dietrich, a researcher and activist, claimed to have used public data scraped from Strava's website to track a French soldier from overseas deployment all the way back home.

"This is the part that is perhaps most worrisome, that an individual's identity might be pullable from the data, either by combining with other information online or by hacking Strava—which just put a major bullseye on itself," says Peter Singer, strategist and senior fellow at New America, a think tank based in Washington, DC. "Knowing the person, their patterns of life, etc., again would compromise not just privacy but maybe security for individuals in US military, especially if in the Special Operations community."

Strava's data could even be used to follow individuals of interest as they rotated among military bases or intelligence community locations, according to Jeffrey Lewis, director of the East Asia Nonproliferation Program in the Middlebury Institute of International Studies at Monterey, California. In a sobering Daily Beast article,

Lewis laid out a scenario by which Chinese analysts could track a Taiwanese soldier based on his activities at a known missile base and thereby discover other previously unknown missile bases as the soldier's duties required him to rotate through those bases.

Taking Steps to Fix the Problem

The United States is clearly far from alone in dealing with such security challenges. Back in 2015, the People's Liberation Army Daily issued a stern warning to members of the Chinese military about the security risks posed by smart watches, fitness bands, and smart glasses, according to Quartz. But the Strava example shows that the United States may be at greater risk, with its relatively large footprint involving troops, intelligence personnel, diplomats, and contractors deployed overseas in sensitive areas or conflict zones.

The US military's Central Command has already begun reassessing its privacy policies for the troops after the Strava revelations, according to reporting by *The Washington Post* and others. Current US military service policies seem to allow for use of fitness trackers and other wearables with the caveat that local commanders have the discretion to tighten security. In fact, the US Army has previously promoted use of Fitbit trackers as part of a pilot fitness program.

Some of the security tightening may involve certain "no-go areas" or "leave-at-home policies" for personal smartphones and wearables, similar to what already exists in sensitive offices of the Pentagon and other installations, Singer says.

> 'People on their third or fourth deployment are going to lose their minds or their marriages if they can't use tech to simulate normalcy.'
>
> – LYNETTE NUSBACHER, MILITARY HISTORIAN

Certain military or intelligence facilities may also need upgrades to their security as a result of the Strava data reveal, says Lynette Nusbacher, a strategist and military historian based in the UK. She adds that militaries and other organizations will

require constant, up-to-date training for both their leadership and the rank-and-file, to ensure they're aware of the threat from modern geolocation technology.

The idea of banning wearable technologies outright may potentially make sense in certain cases: "A small minority of tier one special forces operators can go without toilet paper or soap or mobile phones for weeks," Nusbacher says. But she warns that imposing extreme restrictions more broadly could reduce the number of people willing to sign up for military or intelligence stints overseas.

"When I was deployed on operations in 1999 we expected one phone call a week and dial-up internet," Nusbacher says. "People on their third or fourth deployment are going to lose their minds or their marriages if they can't use tech to simulate normalcy."
Many analysts place the burden of responsibility on the US military and other organizations for the lapse, rather than on Strava. The latter does, after all, allow users to choose whether they share their data. "Strava offered a service," Nusbacher says. "It's not their fault that soldiers who needed better training and briefing turned that service into a vulnerability."

But Paul Scharre, senior fellow and director of the Technology and National Security Program at the Center for a New American Security, argues that technology companies do have certain responsibilities, especially after a problem of this magnitude has been identified.

"Military service members, particularly in the special operations community, take operational security seriously: They would not have shared this data if they understood the consequences," Scharre says. "If Strava was serious about the negative consequences of this data being public, they would temporarily take the maps offline and work with the government to scrub sensitive data. I do not think it is acceptable for a company to release data that might imperil the lives of US service members."

In a statement, James Quarles, CEO of Strava, acknowledged that "members in the military, humanitarian workers and others living abroad may have shared their location in areas without other activity density and, in doing so, inadvertently increased awareness of sensitive locations. Many team members at Strava and in our community, including me, have family members in the armed forces. Please know that we are taking this matter seriously and understand our responsibility related to the data you share with us."

Quarles said that Strava was "committed to working with military and government officials to address potentially sensitive data." He added that the company was "reviewing features that were originally designed for athlete motivation and inspiration to ensure they cannot be compromised by people with bad intent," and was also working to simplify "privacy and safety features" for customers to more easily understand and control their data.

The Not-So-Bad and the Ugly

The heat map may contain a few bright spots, though. There is no evidence as of yet that certain countries or militant groups exploited the Strava heatmap along with other open-source intelligence to inflict real harm. “It’s a good thing this was reported now versus being exploited by an enemy later in a major war,” says Singer.

The Strava heatmap also represents the cumulative activity of users over several years up through September 2017. That means nobody can use it to track military patrols or analysts walking through CIA bases in real-time.

'I do not think it is acceptable for a company to release data that might imperil the lives of US service members.'

– PAUL SCHARRE, CENTER FOR A NEW AMERICAN SECURITY

Still, the Strava incident is just the latest and perhaps most spectacular example of how social media can compromise the operations security of even the most sensitive military and intelligence agencies. Analysts and journalists have previously tracked the locations of soldiers, such as Russian troops in Ukraine, based on selfies and other public data shared on social media. Back in 2007, Iraqi insurgents used geo-tagged photos shared on social media of US Army attack helicopters landing at an airbase to pinpoint and destroy four of the expensive war machines in a mortar attack.

Much of the public data needed to compromise certain aspects of military or intelligence operations was already out there and hiding in plain sight years ago, according to Gavin Sheridan, CEO of Vizlegal and a former journalist. In a lengthy Twitter thread, he explained how geotagging has made it relatively easy to detect Westerners—usually soldiers—in remote areas of the world, or even to compile lists of family members for individuals working at the CIA or the Pentagon.

But addressing the security risks highlighted by Strava will require much more than simply updating a few policies. A world dominated by the rise of social media, the growing availability of commercial satellite and drone imagery, and increasing usage of smartphones necessitates an entirely new cultural mentality.

“Too often we think secrets lie hidden, when now they are mostly out in the open,” says Singer. “Both militaries and the public need to come to grips with the fact that the era of secrets is arguably over.”

This story has been updated to include a statement from Strava CEO James Quarels.

TOPICS MILITARY SOCIAL MEDIA PRIVACY SECURITY SURVEILLANCE

Apple's Encryption Is Under Attack by a Mysterious Group

Plus: Sony confirms a breach of its networks, US federal agents get caught illegally using phone location data, and more.

ANDREW COUTS

Israel's Failure to Stop the Hamas Attack Shows the Danger of Too Much Surveillance

Hundreds dead, thousands wounded—Hamas' surprise attack on Israel shows the limits of even the most advanced and invasive surveillance dragnets as full-scale war erupts.

MATT BURGESS

They Supported Air Strike Victims. Then They Were Doxed and Arrested

Myanmar's military junta is increasing surveillance and violating basic human rights. The combination of physical and digital surveillance is reaching dangerous new levels.

MATT BURGESS

Rumors of a 'Global Day of Jihad' Have Unleashed a Dangerous Wave of Disinformation

The rapid spread of violent videos and photos, combined with a toxic stew of mis- and disinformation, now threatens to spill over into real-world violence.

DAVID GILBERT

A Powerful Tool US Spies Misused to Stalk Women Faces Its Potential Demise

Though often viewed as the “crown jewel” of the US intelligence community, fresh reports of abuse by NSA employees and chaos in the US Congress put the tool's future in jeopardy.

DELL CAMERON

They Cracked the Code to a Locked USB Drive Worth $235 Million in Bitcoin. Then It Got Weird

Stefan Thomas lost the password to an encrypted USB drive holding 7,002 bitcoins. One team of hackers believes they can unlock it—if they can get Thomas to let them.

ANDY GREENBERG

Okta’s Latest Security Breach Is Haunted by the Ghost of Incidents Past

A recent breach of authentication giant Okta has impacted nearly 200 of its clients. But repeated incidents and the company’s delayed disclosure have security experts calling foul.

LILY HAY NEWMAN

The 23andMe User Data Leak May Be Far Worse Than Believed

Plus: IT workers secretly funnel money to North Korea, a court in the US upholds keyword search warrants, and WhatsApp gets a passwordless upgrade on Android

ANDREW COUTS