

JEREMY HSU SECURITY 01.29.18 07:14 PM

THE STRAVA HEAT MAP AND THE END OF SECRETS



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/BETTY IMAGES

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,

social network for athletes called Strava.

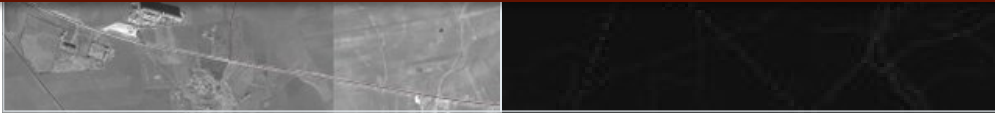
This past November, the San Francisco-based Strava announced a [huge update](#) to its global heat map of user activity that displays 1 billion activities—including running and cycling routes—undertaken by exercise enthusiasts wearing Fitbits or other wearable [fitness trackers](#). Some Strava users 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.





Nathan Ruser
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option).

medium.com/strava-engineer... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

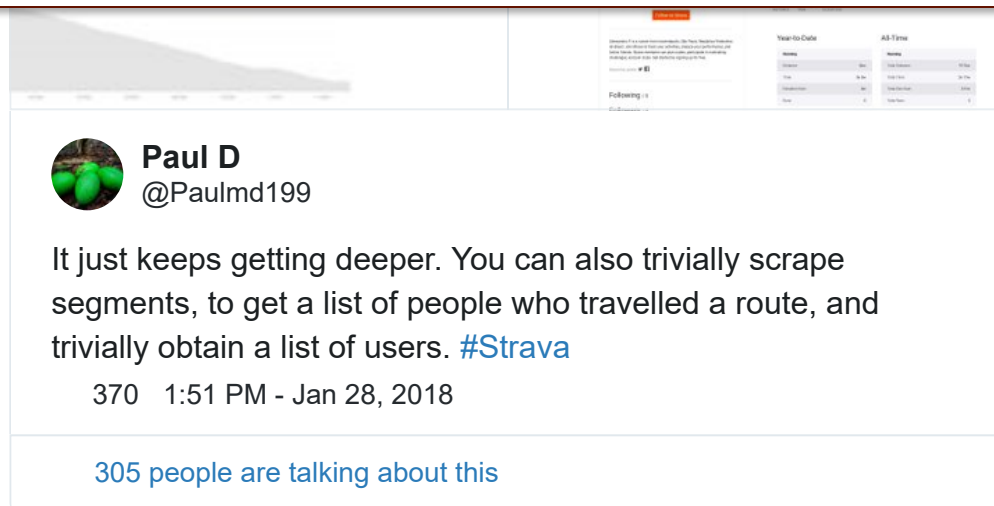
2,644 10:24 AM - Jan 27, 2018

2,374 people are talking about this

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.

1	James S.	30 Strava	4454	1.91	1	Gregory S.	47 Strava	1176	1.14
2	Laurence B.	21 Strava	2194	1.42	2	Luigi P.	42 Strava	1440	1.14
3	Chris J.	34 Strava	2129	1.45	3	Thomas T.	42 Strava	484	1.14
4	John S.	33 Strava	1428	1.42	4	Ross B.	41 Strava	734	1.14
5	John S.	33 Strava	4704	1.42	5	Luca M.	41 Strava	744	1.14
6	Mark H.	33 Strava	1734	1.42	6	Kyle S.	40 Strava	444	1.14
7	Michael C.	31 Strava	1444	1.42	7	A.S.	39 Strava	444	1.14
8	James W.	30 Strava	1174	1.42	8	Shady F.	38 Strava	474	1.14
9	Mark J.	30 Strava	1444	1.42	9	Mark	38 Strava	444	1.14
10	Paul M.	40 Strava	144	1.42	10	Mark C.	38 Strava	714	1.14
11	Paul M.	40 Strava	144	1.42	11	Thomas B.	38 Strava	444	1.14
12	John P.	40 Strava	1114	1.42	12	David L.	38 Strava	514	1.14



“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

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.

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,

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

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.

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

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.

RELATED VIDEO

SECURITY

How to Lock Down Your Facebook Security and Privacy Settings

The only way to be truly secure on Facebook is to delete your account. But that's crazy talk! Here's how to lock

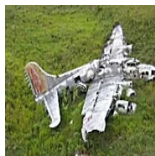
[VIEW COMMENTS](#)

MORE STORIES



HEYWISE

If You Can Name These Historical Figures Then Your IQ Is At Least 140



HISTORY 101

[Photos] WWII Ghost Bomber Lands With No One Inside, And All The Parachutes Still Packed



THEBROFESSIONAL.NET

(Photos) China's Military Super Military. It Looks like US Technology



PAST FACTORY

The F-15 Is No Match For This Plane



MORE SECURITY



SECURITY ROUNDUP

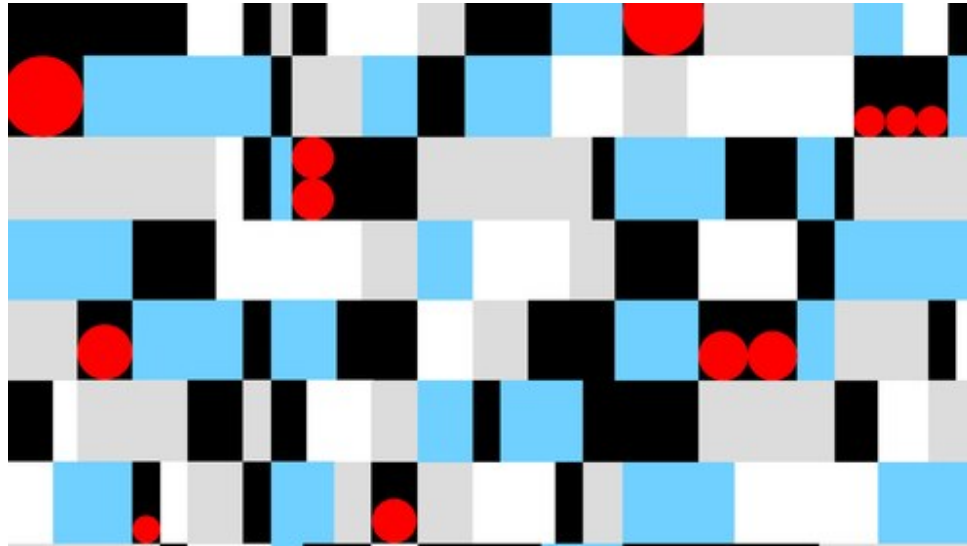
Amazon Won't Say How Many Customer Emails It Exposed

BRIAN BARRETT

PSA

Hey, Turn Off Siri on Your Lock Screen

LILY HAY NEWMAN



ROWHAMMER

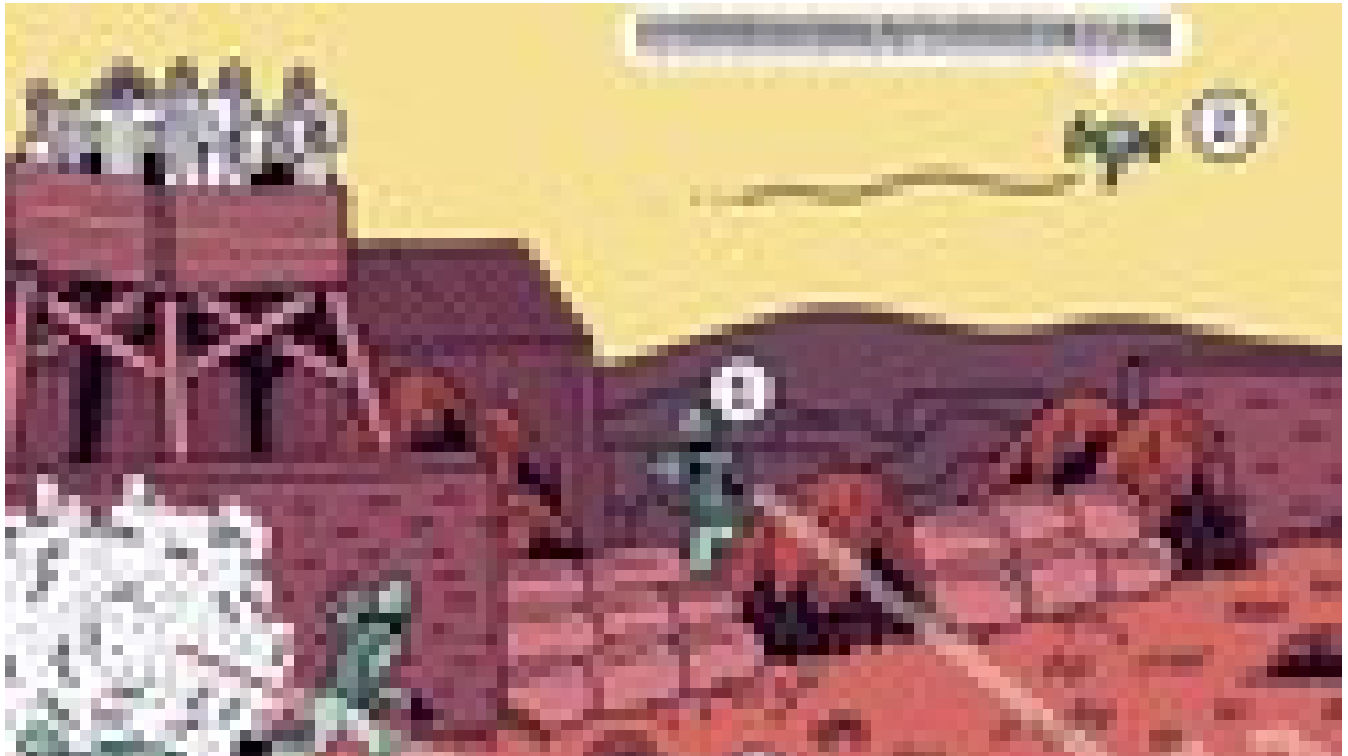
A Clever Data Hack Is More Dangerous Than Anyone Feared

LILY HAY NEWMAN

GRU

Russia's Elite Hackers May Have New Phishing Tricks

LILY HAY NEWMAN



SET TO STUN

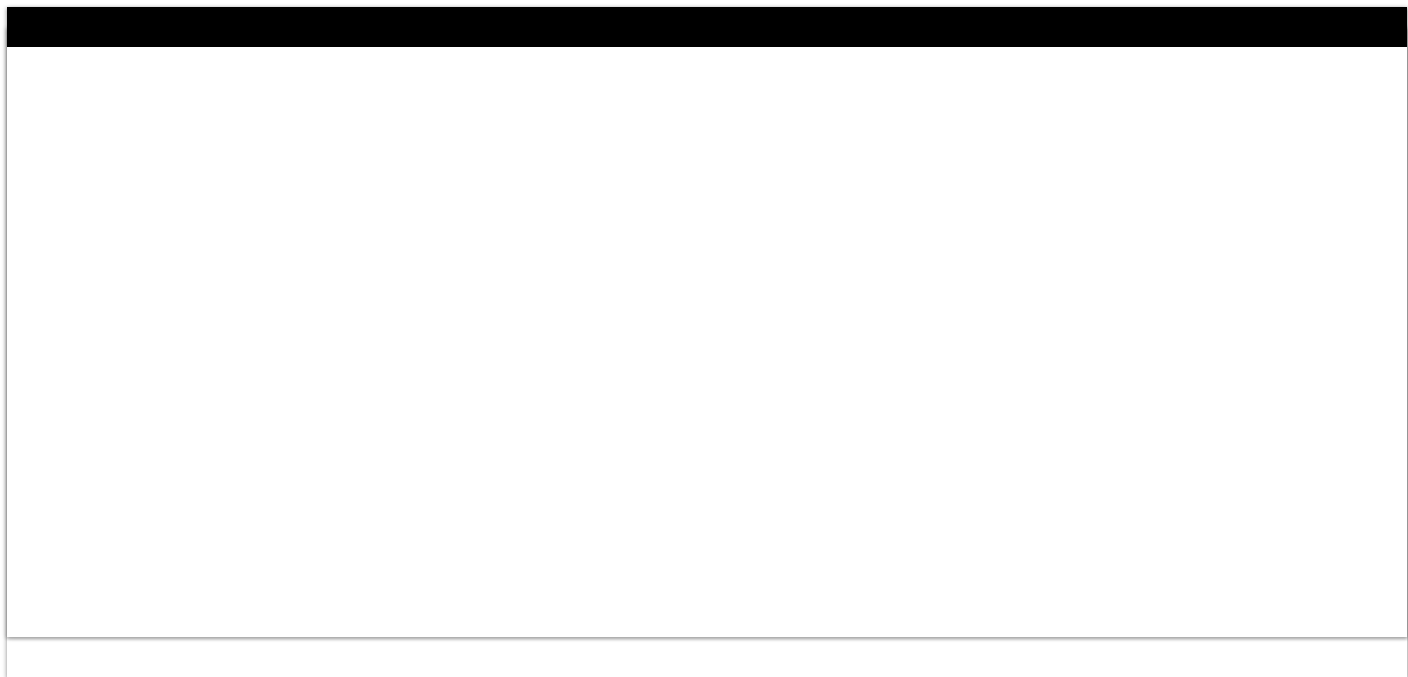
The Ingredients Powering the DOD's New Nonlethal Weapons

REBECCA HEILWEIL





LILY HAY NEWMAN



GET OUR NEWSLETTER

WIRED's biggest stories delivered to your inbox.

Enter your email

SUBMIT

FOLLOW US ON YOUTUBE

Don't miss out on WIRED's latest videos.



SUBSCRIBE	ADVERTISE
SITE MAP	PRESS CENTER
FAQ	ACCESSIBILITY HELP
CUSTOMER CARE	CONTACT US
SECUREDROP	T-SHIRT COLLECTION
NEWSLETTER	WIRED STAFF
JOBS	RSS

CNMN Collection

© 2018 Condé Nast. All rights reserved.

