Strava's fitness heatmaps are a 'potential catastrophe'

You can run (or bike), but you can't hide from big-data irresponsibility.

V. Blue | 02.02.18
@violetblue

V. Blue
@violetblue
February 2nd, 2018

In this article: ActivityTracker, BadPassword, column, Fitbit, gear, heatmap, infosec, internet, LocationData, LocationTracking, mobile, politics, privacy, security, services, Strava, transportation

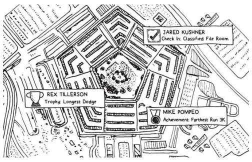

Illustration by D. Thomas Magee

The 2018 cybersecurity race to the bottom is off to an exciting start. First out of the gate is Strava — now widely known as the "social network for athletes" -- and its reckless data-visualization "heat map" gimmick that revealed details of secret military

It was the kind of incident deserving of a plot line in a ridiculous Hollywood drama. And yet, here we are, with Twitter and the whole world discussing and dissecting fitness routes of soldiers and agents in sensitive locations, such as American bases in Afghanistan and Syria, a possible secret CIA base in Somalia, military facilities in war zones and much more.

I'm not sure how many times we need to go through this. The trifecta parable of confusing privacy settings, postpublication safety considerations and the requirement of major headlines for companies to give a shit. It's as if the makers of completely different internet.

Let's be clear: Fitness apps have a massive privacy problem. MapMyRun, Nike + RunClub and Strava (to name a few) all come with scary default privacy settings that are combined with mapping tools. These apps are a dream come true for stalkers, terrorists and spies.

And yet, nearly 10 years after Please Rob Me made a devastating mockery of Silicon Valley's reckless location-sharing mania — by using publicly available social-media information to show when people's homes are vacant — Strava just burps and says, "Hold my beer."

Strava's global heat maps have

November 2017 boasting "1 billion activities" and "3 trillion latitude/longitude points" mined from "10 terabytes of raw input data" from its users. (Spoiler alert: unsuspecting user plot twist ahead. We'll probably never know how much of this inadvertent sharing came from Strava's carelessly confusing privacy settings.)

Yet it was the observations of one national-security-policy nerd on Twitter over the past weekend that got all the infosec chickens clucking. "Strava released their global heatmap," tweeted Nathan Ruser. "13 trillion GPS points from their users (turning off data sharing is an

Op-Sec. US Bases are clearly identifiable and mappable."

And Strava's location data patty-cake playtime with the data of its "global community of millions of runners, cyclists and triathletes" who use Fitbits and phones *is* amazing. For spies and bad guys, that is.

With the data, press reported that it's possible to "establish the names and hometowns of individuals who have signed up for a social sharing network where runners post their routes and speeds. One popular route on a base in Iraq has been nicknamed "Base Perimeter" by the U.S. runners who regularly use it. Another outsidecalled "Sniper Alley."

Strava heatmap of an area in Kandahar, Afghanistan which includes an airfield.

If only someone in the San Francisco startup's offices had foreseen this. Except they sort of did. People had for months been [trying to tell](#) Strava that its privacy protocols were dangerous and that its maps were just a little problematic.

These issues with Strava had been well-established by at least July of last year when a female runner and journalist exposed the company's very real privacy problems in [an article for Quartz](#).

ignored because the app's fairly dangerous privacy mess was described as a "feminist issue." As in, it got shuffled off as a women's problem.

Strava's response to the July 2017 article — calling out its reckless privacy practices as a threat to women — was to publish a blog post two days later essentially blaming users for not doing its privacy settings correctly.

It's hardly a coincidence that the people most at risk of violence from apps that exploit user privacy and location data are the ones most routinely ignored when they raise the alarm.

Anyway, when increasingly larger

exciting new feature, self-guided online tours of military facilities in war zones, Strava attempted to reuse its old blog post from last year as a statement.

When no one would go away, Strava issued a new statement saying that it takes the safety of its users seriously. The company will now focus on privacy awareness to address security issues.

That's great. This is fine. Well, not really. Nathaniel Raymond, director of the Signal Program on Human Security and Technology at the Harvard School of Public Health, told press that the public availability of the data represents "a potential catastrophe."

Strava heatmap of the area surrounding The Pentagon in Washington DC.

The US military kind of agrees. A lot. *Reuters* reported by midweek that US Defense Secretary Jim Mattis ordered a review of the situation and will be changing its guidelines for the use of all wireless devices on military facilities. As is tradition, no one's confirming or denying anything. "Pentagon spokesman Colonel Robert Manning told reporters at a news briefing he did not know of any instances in which U.S. base security had been compromised as a result of the mapping," the outlet reported.

been taken down for review, pending user privacy clarifications (making sure people understand what they're sharing), meetings with military and hopefully also domestic-violence shelters and also women in general. But if this is you expecting this, you would be wrong.

The maps are still live as a wire, and people are poring over them like porn from an alien planet. "People wearing Strava-enabled fitness trackers appear to have been poking around a Thames shipwreck containing nearly 1,500 tonnes of explosives from the Second World War," *The Register* reported in this great post on cautioning us on how to avoid jumping to conclusions as more people tear into the data looking for new things to make headlines out of in the coming weeks.

We can only hope that some good comes out of the Strava heatmap debacle. I don't mean the kind where Strava seizes the opportunity to radically change the way user privacy is taught to ordinary people, to take the lead in creating sustainable data sharing practices for at-risk populations, or any such impossible nonsense. I mean the more realistic kind, where people find Disneyland's secret entrances.

selected by our editorial team, independent of our parent company. Some of our stories include affiliate links. If you buy something through one of these links, we may earn an affiliate commission.

Popular on Engadget

Honda to end production of its hydrogen and plug-in hybrid Clarity cars

Facial recognition systems are denying unemployment benefits across the US

'Seinfeld' might not be available to stream for months

iPhone bug 'breaks' your WiFi when you join an oddly-named network