Mobile security firm says it defeated Strava's privacy feature with simple geometry

Strava, Inc., the maker of a GPS-based fitness app that has faced backlash in recent days for a heat maps feature that shows US military locations, has encouraged users to read about their privacy options and update their settings if they're that concerned.

But one of those key privacy options may not be very private at all, a mobile security firm says.

Strava's Privacy Zones feature, which allows people to create a geofence around their home or office in order to block other users from seeing those locations, is rendered useless through simple geometry. That's according to Wandera, a UK-based mobile security and data management firm that managed to figure out a Strava user's exact end point after a run, even with Privacy Zones enabled.

Dan Cuddeford, Wandera's director of systems engineering, said the company ran a series of tests last year around its US office in San Francisco. It set up two brand-new Strava accounts on two iPhones. On one of the accounts, workouts were public and no Privacy Zones were enabled, which are the default settings for Strava. On the second account, the team created a Privacy Zone of one-eighth of a mile around the office. (Strava offers five fixed distances for Privacy Zones.)

A test runner went for two runs, the first run with two iPhones and two separate Strava accounts, one with Privacy Zones and the other without. The second run occurred with one phone with Privacy Zones enabled to create a third Privacy Zone data point. From three recorded data points, Wandera was

able to use high school-level math to triangulate the runner's exact entry points and ending points.




Image: Wandera

Cuddeford added that, in many cases, relying on a smartphone's own GPS capabilities would end up being less accurate than using this triangulation method, especially in urban areas where GPS signals can be tricky. "What was really interesting here is that through good intent from Strava through this service, it actually makes the matter worse," he said in an interview with *The Verge*.

Wandera said it told Strava about its findings back in June 2017.

A spokesperson for Strava said in a statement to *The Verge* that while the company's engineering team "has been working to augment and improve privacy options well before we were contacted by this company and others, we appreciate their interest in our platform. In the coming weeks, Strava will be rolling out more privacy options for users."

It's definitely not the first time that security researchers have triangulated the location of mobile app users to demonstrate just how exposed they are, and for some people, the results from Wandera's Strava test might even seem obvious.

It turns out, Strava could learn something from Tinder
In 2014, a firm called IncludeSecurity (IncludeSec for short) showed how someone could find out a Tinder user's location using three or more distant measurements to a target, coming within 100 feet of said target. Tinder resolved the security flaw about four months after being contacted by IncludeSec, with then-CEO Sean Rad assuring users that the company

“implemented specific measures to enhance location security and further obscure location data.”

That same year, a user on PasteBin wrote about a similar vulnerability in the app Grindr, explaining how it’s possible for a “malicious entity” to send “distance-requests from three different points and using the responses to calculate the exact position of a particular user.”

In other words, GPS-based social apps are inherently using your location data. That’s great when you want to meet or connect with people in your community, but it can be creepy when a follower you’d rather not encounter in real life is able to figure out where you are (or where you work or where you live). In the case of Strava, this particular Privacy Zone feature is *supposed* to help shield people from that, but it turns out it may be doing very little to protect users.

Cuddeford said he recommended that Strava be “less accurate around its privacy zones” in order to obscure users’ locations. “Every time you come back, your exact location should be randomized.”

But, Cuddeford said, Strava’s primary feedback to the firm was that “users could opt out of the service altogether…which we respect, but what we’ve determined is that users can’t be expected to go through all of these settings.”

https://www.theverge.com/2018/2/7/16983408/strava-privacy-zones-wandera-security-geofence-safety-heat-maps