

Fitness app loophole allows access to home addresses

June 7 2023, by Matt Shipman



Credit: Unsplash/CC0 Public Domain

Despite attempts to anonymize user data, the fitness app Strava allows anyone to find personal information—including home addresses—about some users. The finding, which is detailed in a new study, raises

significant privacy concerns.

"Strava users expect their [personal information](#) to be protected, and our work shows that this is not always the case," says Anupam Das, senior author of a paper on the work and an assistant professor of computer science at North Carolina State University. "This could be particularly problematic for users who are concerned about stalkers or have other reasons to desire that their [location data](#) be kept from the public."

Strava is a mobile fitness-tracking app that allows users to track their exercise activities, but also includes features designed to help users connect with each other. These features can be used to organize clubs around shared interests, such as hiking or cycling. For example, the app includes a "heatmap" feature that aggregates [user data](#). While all of the user data is anonymized, the heatmap feature allows users to see how many other Strava users go hiking, running or cycling in a given area.

"Strava stresses that the heatmap feature uses only aggregate data, which should make it impossible for anyone to capture [private information](#) about any specific user," Das says. "However, we found a loophole."

Specifically, the researchers found it is possible for anyone to look up all of the Strava users in a given area. It is also possible for users to look at the aggregate data on a heatmap and see where each of the anonymous users' routes begin and end.

"In a densely populated area, with lots of routes and lots of users, there is so much data that it would be extremely difficult to track any specific person," Das says. "However, in areas where there are few users and/or few routes, it becomes a simple process of elimination—particularly if the person someone is looking for is a highly active Strava user. Even users who have marked their accounts as private show up when anyone searches for a list of all the users in a given municipality, so marking an

account private doesn't necessarily provide additional protection against this tracking technique."

"We did reach out to Strava about this, and the company has said that it does not share heatmap data unless several users are active in a given area," says Kevin Childs, first author of the paper and a former undergraduate at NC State. "However, we were still able to identify the home addresses of some users in certain areas using the heatmap, and confirmed those identifications using voter registration data."

However, there is something that users can do to protect their privacy.

"Users can go into their Strava account settings and opt out of contributing data to the 'aggregated data usage' feature, which would remove their routes from the heatmap altogether," Das says.

The paper, "[Heat Marks the Spot: De-Anonymizing Users' Geographical Data on the Strava Heatmap](#)," was presented May 25 at the 7th Workshop on Technology and Consumer Protection ([ConPro '23](#)) in San Francisco.

Provided by North Carolina State University

Citation: Fitness app loophole allows access to home addresses (2023, June 7) retrieved 4 May 2024 from <https://techxplore.com/news/2023-06-app-loophole-access-home.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--