

ONE HUNDRED FIFTEENTH CONGRESS
Congress of the United States
House of Representatives

COMMITTEE ON ENERGY AND COMMERCE

2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6115

Majority (202) 225-2927

Minority (202) 225-3641

January 31, 2018

Mr. James Quarles
Chief Executive Officer
Strava, Inc.
500 3rd Street #110
San Francisco, CA 94107

Dear Mr. Quarles:

We are writing to request a briefing on Strava's privacy and data security practices in light of recent troubling news reports indicating that the company has publicly shared detailed information that may put its users at risk.¹ Among other concerns, security analysts have raised the possibility that this information may expose the identities and locations of personnel at military sites and other sensitive areas.²

As a GPS tracking company, your company collects data from wearable fitness trackers and from its mobile app on users' workouts, locations, and movements.³ The information collected is so precise that Strava can determine whether a user is traveling on foot, by bicycle, or in a vehicle.⁴ Since November 2017, the company has publicly shared online an interactive heat map of its users' movements over the past two years.⁵ In recent days, news reports have called attention to the various ways this information could jeopardize individuals' personal safety

¹ *U.S. Military Revising its Rules After Fitness Trackers Exposed Sensitive Data*, Washington Post (Jan. 29, 2018).

² *Id.*

³ *U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging*, Washington Post (Jan. 29, 2018).

⁴ *Strava Fitness App Can Reveal Military Sites, Analysts Say*, New York Times (Jan. 29, 2018).

⁵ See note 3.

and U.S. national security.⁶ The Strava heat map can be used to trace military supply and routes, identify military and humanitarian personnel, and map U.S. military bases.⁷

The increasing popularity of fitness trackers and other wearable technology has raised serious questions about the types of data they collect and share and the degree to which consumers control their own personal information.⁸ The data these devices collect reveals users' precise locations, daily activities, and health information.⁹ Most consumer technology companies, however, are not required to set baseline privacy standards or ensure that users' information is secured.¹⁰

In this case, Strava made no attempt to secure information, and instead published location information on the Internet for anyone to see.¹¹ Although the location information was aggregated and anonymized, analysts warned that the data Strava posted can easily be cross-referenced with other publicly available information to identify individual users.¹²

The Committee on Energy and Commerce has a longstanding interest in the privacy and security of consumers' personal information, including information collected by wearable technology. We therefore request that Strava provide a briefing to Committee and Member staff to discuss the following questions:

1. How did Strava decide to publish the heat map online? Was the company aware that the information in the heat map could be de-anonymized to identify individual users?
 - a. Did the company take any efforts to mitigate safety risks to its users before publishing the heat map?
 - b. Before the heat map was published in November 2017, were users given any notice that their information would be included?
2. According to press reports, only users who opted out did not have their information shared in the heat map.¹³ What are the default privacy settings for Strava accounts? Was it a default setting to share location information to the global heat map?

⁶ *Id.*

⁷ *Id.*

⁸ *Strava Map Fallout: How Much Do You Know About Your Fitness App's Tracking?*, USA Today (Jan. 29, 2018).

⁹ *Id.*

¹⁰ See note 1.

¹¹ *Id.*

¹² See note 4.

¹³ See note 8.

3. Consumers have previously expressed confusion about the multiple settings used by Strava to control how user information is shared.¹⁴ What privacy options are currently available to Strava's users?
4. Strava's privacy policy warns that user information may not be anonymous and can be shared with third parties, but consumers may not be clear what that means.¹⁵ What types of data does Strava provide to third parties? What kinds of entities have access to this data, and what do they use it for?
5. What are Strava's data security practices? What security and privacy practices does Strava require of the entities with whom it shares user information?
6. What changes is Strava making to its privacy or data security practices in response to this release of location data?

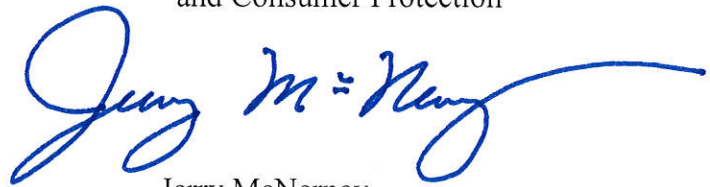
Please contact Caroline Paris-Behr with the Democratic Committee staff at (202) 225-3641 by February 9, 2018, to schedule the briefing. Thank you for your attention to this matter.

Sincerely,


Frank Pallone, Jr.
Ranking Member


Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection


Diana DeGette
Ranking Member
Subcommittee on Oversight
and Investigations


Jerry McNerney
Member of Congress

¹⁴ *Using a Fitness App Taught Me the Scary Truth About Why Privacy Settings are a Feminist Issue*, Quartz (Aug. 1, 2017); *Strava Begins Selling Your Data Points, and No, You Can't Opt-Out*, Engadget (May 23, 2014).

¹⁵ Strava, Strava Privacy Policy (strava.com/legal/privacy) (accessed Jan. 29, 2018).



Peter Welch
Member of Congress



Ben Ray Lujan
Member of Congress



Yvette D. Clarke
Member of Congress



Tony Cardenas
Member of Congress



Debbie Dingell
Member of Congress