THE CAPITOL FORUM Vol. 7 No. 15 January 17, 2019

Anta Sports/Amer Sports: Fitness App Could Pose U.S. Security Vulnerability, Trigger CFIUS Questions

Deal Update

Heat maps of the world created by the fitness tracking app Movescount reveal some odd anomalies. Where users have input their running data for maps around San Francisco, Dallas or Boston, massive clumps of orange appear, as might be expected. More surprising are the tangerine-colored lines that encircle locations in places like Afghanistan, Djibouti and Iraq.

While anyone can sign up for the app, it's a fair bet the high levels of activity recorded around the U.S. Embassy in Baghdad or the U.S. Navy's Camp Lemmonier in Djibouti are generated by Americans—specifically, American military personnel. The same can be inferred from the orange lines running through the Army's Fort Drum in New York and around Quantico, Virginia, home to a major Marine base.

Soon, a Chinese company could be in control of the data behind the maps—and a great deal more related information.

On December 7, Amer Sports (HEL: AMEAS), the Finnish sports-equipment manufacturer behind the Movescount app, announced an agreement to be acquired by China's Anta Sports (HKG: 2020) and Hong Kong-based private equity firm FountainVest in a 4.6 billion euro ($5.27 billion) deal.

Heat maps aside, a Chinese company gaining control of behind-the-scenes data on Americans raises significant national security concerns about the transaction that cyber-security experts said needs review by the federal government's multi-agency Committee on Foreign Investment in the U.S. (CFIUS).

"These kinds of apps pair highly granular location information with very detailed biometric information, so that can portray a very revealing picture of an individual's activities, fitness level and patterns," said Sharon Bradford Franklin, director of surveillance and cybersecurity policy at New America's Open Technology Institute.

The risks posed by the disclosure of service members' information through fitness apps was brought to light early last year by a 20-year-old Australian student who on Twitter noted that data from Strava, an app targeted at cyclists and runners, could be used to locate bases and establish soldiers' routines.

By August, the DOD had prohibited the use of GPS tracking devices in operational areas after maps on Strava and Polar Flow, its training and workout competitor, revealed sensitive locations. Movescount's heat maps are generated by aggregating individual runners' routes over several years, meaning most maps would have included data before the DOD released its policy.

A Chinese buyer means the issues surrounding Movescount go even deeper because of growing U.S. concerns about the Chinese government using the country's businesses to gain critical information on Americans.

Amer Sports appears to be gearing up for a possible CFIUS review. The companies' combination agreement allows Anta Sports to abandon the deal if the committee recommends that President Trump block the transaction, an indication that the companies had either filed or planned to file for a U.S. national security review.

Although Suunto, Amer Sports' watch and compass segment, is based in Finland, the company operates a U.S. subsidiary in Utah. Any U.S. presence such as corporate offices or data storage would be enough to trigger CFIUS jurisdiction, one committee expert said.

Spokespeople for Anta Sports, FountainVest and Suunto declined to discuss the prospects for the proposed acquisition and a CFIUS review beyond what the companies have previously disclosed in public filings.

A CFIUS review of the transaction would need to consider the changing nature of Suunto's offerings. This week, Suunto said it would phase out Movescount by the summer of next year, allowing the app's users to transfer their data to the "Suunto app." Introduced last year, the Suunto app also tracks exercises and generates heat maps.

Personally identifiable information. The troves of data collected by the Suunto fitness apps could certainly pique CFIUS's interest in Chinese ownership of the company. Over the past several years, the panel has turned its focus from scrutinizing traditional defense industrial-base deals and toward examining the national security risks presented by companies with access to large pools of personal information.

In August, Congress broadened CFIUS's powers with the Foreign Investment Risk Review Modernization Act (FIRRMA), though some rulemaking is still in the works. As the Treasury Department grapples with CFIUS's new scope under FIRRMA, it's considering proposing some rules around personally identifiable information, department officials said in October.

A measure of controversy has erupted over those rules proposals. Last September, then-House Financial Services Committee Chairman Jeb Hensarling, a Texas Republican, and Maxine Waters,

a California Democrat who now chairs the panel, discouraged Treasury Secretary Steven Mnuchin from including language covering "personally identifiable information" in the rules.

Instead, the lawmakers urged a narrower description, "sensitive personal data." In the letter, Hensarling and Waters cautioned that the rules language should "maintain the country's open investment climate" and refer only to information related to national security concerns.

"The bar in other words, is intentionally high," according to the letter. "Information that may simply identify individuals or prove a source of embarrassment if disclosed is not sufficient to trigger CFIUS jurisdiction without a potential threat to national security."

Regardless of changes to the statute, for the past several years most attorneys that handle CFIUS matters have recommended clients seek the committee's approval in foreign-investment transactions if they involve access to consumer data, said John Kabealo, a lawyer specializing in foreign investment issues.

"That's really only increased as data breaches have become more common," he said.

A new view of national security. CFIUS's increased focus on personally identifiable information reflects the Trump Administration's shift toward the view that economic security is a component of national security. Trump's National Security Strategy formalized that policy by highlighting concerns about manipulation and theft of personal data, said Robert S. Spalding, a former U.S. Air Force general who served as senior director for strategic planning at the National Security Council in the Trump White House.

"It's about dollars and cents, and those are more important than a carrier battle group," he said. "But for the most part, our national security professionals haven't made that shift."

Movescount's users hail from all over the world. Although U.S. Army spokespeople interviewed by *The Capitol Forum* were unaware of the app or soldiers' use of it, the website's heat maps, profiles and online forums indicate usage by U.S. military personnel.

"We are aware that Department of Defense personnel use devices, applications and services with geolocation-enabled capabilities," Lt. Col. Audricia Harris said in an email. "Devices, applications and services with geolocation capabilities present a significant risk to the Department of Defense personnel on and off duty, and to our military operations globally. The rapid emergence of technology requires constant refinement of policies and procedures to enhance operations security and the protection of information."

The app only uses data for heat maps from members who have set their profile to "public" and includes a "special algorithm" that prevents an active person from creating heat during their daily commute that would reveal where they live, according to Movescount's website.

Users must manually upload their activities to the Movescount app for data such as heat maps to be recorded. Suunto's Movescount watch doesn't automatically sync to the app.

As a Finnish company, Suunto abides by European Union privacy regulations; personal information can't be shared outside of approved Suunto employees without a Finnish court order.

Users must provide their email to register for Movescount, but they can volunteer more information such as their birthday and home location. Movescount also furnishes health researchers with user data, including training times and heart rates.

"Whatever it is, it will never have your identity such as username or email attached to it!" the company states on its website. "Only the numbers are collected."

As Movescount is phased out, its users can transfer most of their exercise information to the Suunto app, but not body measurements such as height, weight and heart rate, according to the company. Activities from Movescount can't be synced with the new app.

In the Movescount phaseout, the company will comply with the data retention requirement of the General Data Protection Regulation (GDPR), the EU's new privacy law, said a spokesperson for Suunto's parent company, Amer Sports. Under GDPR's data-minimization provision, companies can't keep data longer than necessary, although the law doesn't mandate a specific deadline for discarding the information.

Seeing the raw data. Behind the scenes, most fitness tracking apps can view the raw data, said Kalyanaraman Shankari, a PhD. candidate at the University of California, Berkeley, whose research on Google showed the company tracking its users' locations despite privacy settings.

"The people running Strava and Fitbit will know, because your data gets sent to them and is stored on servers," she said.

However, if Suunto uses end-to-end encryption for the data, even the company wouldn't be able to access data for a particular individual, she added.

Movescount's data is protected by multiple levels of passwords and encryption, according to a Suunto spokesperson.

For some security experts, that protection isn't enough. While foreign ownership of Movescount could increase national security risks, a clear danger already exists, said Andrew J. Grotto, an international security fellow at Stanford University's Center for International Security and Cooperation.

"We would be worried if a U.S. company owned this," Grotto said.