Fit to Be Spied: Fitness Trackers and OPSEC Risks

By Dayton Ward
NCO Journal

March 9, 2018

With technology continuing to improve and exist as an ever-present part of our daily lives, Soldiers must remain situationally aware and continue to practice sound operations security. (Graphic by Dayton Ward, NCO Journal)

U.S. military leaders expressed concern after recent revelations that data collected and transmitted by personal fitness devices pose potential security risks to military personnel and installations around the world.

An interactive global map posted on the internet identifies the locations of people who use different models of personal fitness tracker bracelets and other devices. When this information became public in January, questions arose in response to the map appearing to highlight locations of U.S. military bases and other sensitive facilities. Also depicted are concentrations of activity in and around these areas, presumably by service members wearing trendy fitness accessories with geotracking software.[1]

Posted to the internet in November 2017, the map is the creation of a U.S.-based software company. A mobile application developed by the firm utilizes geolocation data retrieved from GPS satellites.[2] The app collected information between 2015 and September 2017 from fitness trackers and mobile devices with GPS functionality. The resulting map and its underlying data gained widespread attention in late January after an Australian university student found it while conducting international security studies research.[3]

Fit for Duty?

"Geotracking" is the practice of identifying a person's physical location through the use of data transmitted from a GPS-enabled device.[4] This feature, found in fitness bracelets, cellular phones, and other mobile and wearable technology, is especially popular with running and cycling enthusiasts. The software applications these devices employ allow users to chart routes, distance, speed, and biometric data such as heart rate. Performance information recorded day by day lets the user monitor their progress over a set period.[5]

Even the Army embraced the popularity and usefulness of these "high tech gadgets." In 2013, a six-month pilot called for 2,200 Soldiers to wear fitness trackers as part of a health and wellness campaign. The test involved uploading data from an individual Soldier's tracker to their personal computer or mobile phone and tracked their progress in steps walked or run, along with distances achieved and calories burned. The devices even logged sleep patterns.[6]

The pilot program demonstrated the usefulness of monitoring and analyzing this type of data to paint a picture of a Soldier's health and fitness routines, highlighting areas for improvement and contributing to their overall wellness goals. Today, such trackers are now a common sight. Their popularity has grown in recent years, with athletes and other fitness enthusiasts sharing their charted data as a means of challenging and motivating themselves and others.

Despite these apparent benefits, particularly when it comes to monitoring the health of Soldiers, there are possible drawbacks. As is the case with other devices that allow for this type of interactivity, there is a risk of complacency as we forget how this technology acquires and transmits seemingly benign information, all of which is vulnerable to exploitation for malicious purposes.

The recently published map brings this issue into sharp focus, inadvertently revealing locations of U.S. military installations in some of the most dangerous regions of the world.[7]

Awareness Is Key

"Recent data releases emphasize the need for situational awareness when members of the military share personal information," said Maj. Audricia Harris, Pentagon spokesperson for the Office of the Secretary of Defense (https://www.defense.gov/About/Office-of-the-Secretary-of-Defense/), while quoting from a statement provided to media outlets on January 29, 2018.[8] The official response also insists that while the public release of this GPS data resulted in no known impacts to troop safety, Secretary of Defense James Mattis ordered a review of the Department of Defense's policies regarding the use of fitness trackers and mobile devices on military installations.[9]

"We have confidence in commanders to employ tactics, techniques, and procedures that enhance force protection and operational security with the least impact to individuals," said Col. Robert Manning III, director of Defense Press Operations at the Pentagon, during a January 29 news conference.[10]

Col. Manning issued a reminder to all DoD personnel that they should "place strict privacy settings on wireless technologies and applications," and that "such technologies are forbidden at specific DoD sites and during specific activities." He also reiterated that service members should limit their use of publicly accessible social media platforms while deployed to sensitive locations.[11]

Related: Leadership in the Social Media Age (*NCO Journal*) (http://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2018/January/Social-Media/)

DoD Directive 8570.11M (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf) requires all active duty and reserve personnel, as well as civilian employees and contractors to complete annual training on the subjects of cyber awareness and information security.[12] Despite these regular sustainment training initiatives we see daily demonstrations of just how easy it is to innocently or inadvertently share information with a global audience. Soldiers must maintain constant awareness of the risk posed by the casual use of mobile devices and social media platforms to safeguard their personally identifiable information as well as potentially sensitive material, which can impact operations security.

In response to the recent data release and resulting concerns, the DoD's review of current policies will determine the need for additional guidance and training.[13] While that evaluation continues, noncommissioned officers can still exercise initiative and take precautionary steps to ensure they and their Soldiers continue to practice sound OPSEC with regards to information sharing and mobile devices.

For example, the U.S. Army Criminal Investigation Command offers a series of "cyber tips (https://www.army.mil/article/111305/cid_cyber_tips_protecting_your_online_identity)" Soldiers can employ to protect themselves. Chief among these guidelines is advice on understanding the "end user agreement" accompanying the use of devices like fitness trackers, smartphones, and other internet-enabled devices as well as the software they utilize and the social media platforms they can access. Soldiers also need to be diligent when it comes to configuring each device and software application's privacy settings. This practice is particularly essential for wearable and mobile technology, given these items' ability to transmit geolocation data.[14]

NCOs have the greatest influence on training Soldiers to be mindful of the potential risks that come with the use of these devices, as is currently done with government and personal computers, cellular phones, and other mobile technology. With the ongoing concerns surrounding information and operations security, NCOs can fold reminders about the proper privacy settings for fitness trackers into their unit's regular physical training programs. Similar reviews are also excellent guided discussion and opportunity training topics, as well as useful additions to holiday and leave safety briefs.

In Closing

Recent examples of sensitive data released to the public demonstrate the ongoing need for government and military personnel to remain vigilant when sharing official and private information. Despite their popularity, fitness trackers, just like smartphones and other mobile technology, must be used responsibly. When using these devices, common sense and situational awareness

are crucial to protecting personal data and practicing sound operations security.

Notes

1. Liz Sly, "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *The Washington Post*, January 29, 2018, accessed February 2, 2018, https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html (https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html).
2. Strava, "Features for Athletes, Made by Athletes," Strava.com website "Features" page, accessed February 2, 2018, https://www.strava.com/features (https://www.strava.com/features).
3. Liz Sty, "U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging."
4. Definition of "geotracking" provided by *PC Magazine*'s online encyclopedia, accessed February 5, 2018, https://www.pcmag.com/encyclopedia/term/62908/geotracking (https://www.pcmag.com/encyclopedia/term/62908/geotracking).
5. Strava, "Features for Athletes, Made by Athletes."
6. Amy Bushatz, "Army Issues FitBit Bands in Test Fitness Program," Military.com website, October 22, 2013, accessed February 9, 2018, https://www.military.com/daily-news/2013/10/22/army-issues-fitbit-bands-in-test-fitness-program.html (https://www.military.com/daily-news/2013/10/22/army-issues-fitbit-bands-in-test-fitness-program.html).
7. Liz Sly, Dan Lamonthe, and Craig Timberg, "U.S. Military Reviewing Its Rules After Fitness Trackers Exposed Sensitive Data," *The Washington Post*, January 29, 2018, accessed February 9, 2018, https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html (https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html).
8. Elizabeth McLaughlin, "GPS Data Shared by Fitness Apps Has Not Compromised Location of U.S. Troops: Pentagon," *ABC News* website, January 29, 2018, accessed February 2, 2018, http://abcnews.go.com/International/gps-data-shared-fitness-apps-compromised-location-us/story?id=52688704 (http://abcnews.go.com/International/gps-data-shared-fitness-apps-compromised-location-us/story?id=52688704).
9. Elizabeth McLaughlin, "GPS Data Shared by Fitness Apps has Not Compromised Location of U.S. Troops: Pentagon."
10. Jim Garamone, "DOD Studying Implications of Wearable Devices Giving Too Much Info," DOD News, Defense Media Activity, January 29, 2019, accessed February 9, 2018, https://www.defense.gov/News/Article/Article/1426579/ (https://www.defense.gov/News/Article/Article/1426579/).
11. Liz Sly, Dan Lamonthe, and Craig Timberg, "U.S. Military Reviewing Its Rules after Fitness Trackers Exposed Sensitive Data."
12. Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, *Information Assurance Workforce Improvement Program*, DOD 8570.01M, Department of Defense, December 19, 2005, accessed February 5, 2018, http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf (http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf).
13. Liz Sly, Dan Lamonthe, and Craig Timberg, "U.S. Military Reviewing Its Rules after Fitness Trackers Exposed Sensitive Data."
14. 14. U.S. Army Criminal Investigation Command, "CID Cyber Tips: Protecting Your Online Identity," *Army News* website, September 19, 2013, accessed February 5, 2018, https://www.army.mil/article/111305/cid_cyber_tips_protecting_your_online_identity (https://www.army.mil/article/111305/cid_cyber_tips_protecting_your_online_identity).