United States Senate
WASHINGTON, DC 20510

February 7, 2018

The Honorable James N. Mattis
Secretary of Defense
U.S. Department of Defense
1400 Defense Pentagon
Washington, D.C. 20301

Dear Secretary Mattis:

We commend the Department of Defense (DoD) for undertaking a review of its guidelines for the use of wireless devices, such as mobile phones and fitness trackers, at military facilities around the world in light of the recent discovery that a popular fitness tracking app has exposed the locations and identities of individuals working in sensitive areas. As part of this review, we encourage you to consider a couple additional items of concern that may jeopardize national security and endanger the privacy and safety of our servicemembers.

First, a January 24, 2018 article published in Quartz,[1] recounted the continuous collection of precise user location data by Google Android phones. This data is collected and sent back to Google, "including everything from GPS coordinates to nearby Wi-Fi networks, barometric pressure, and even a guess at the phone-holder's current activity." The article makes clear the difficulty for an average user to opt out of this location tracking. For servicemembers using Android-based phones, there is a strong likelihood that most users are sending precise location and activity data to Google, and, by extension, all divisions of its parent company, Alphabet.

In Questions for the Record (QFRs) from a November 1, 2017, Senate Select Committee on Intelligence hearing, Google's Senior Vice President and General Counsel, Mr. Kent Walker, was asked whether information it collects on U.S. government employees is processed or stored in Russia or China. In his answer, he noted that Google does "not have data centers that store information collected on *U.S.-based* government employees in Russia or China [emphasis added]."[2] Given this response, we are concerned about the storage of location data of *foreign-based* government employees, such as servicemembers and diplomatic personnel stationed overseas. As part of the Pentagon's review of wireless devices, we encourage you to look into whether there are any special risks to servicemembers using Android phones or Google services, in terms of having their locations tracked and stored by Google, whether in U.S. or foreign-based data centers. In addition, as to foreign-based storage of U.S. person information, we ask that you

---

[1] David Yanofsky, "If You're Using an Android Phone, Google May Be Tracking Every Move You Make," *Quartz*, 24 Jan. 2018, qz.com/1183559/if-youre-using-an-android-phone-google-may-be-tracking-every-move-you-make/.
[2] Kent Walker, "Responses to Questions for the Record for Mr. Kent Walker, Senior Vice President and General Counsel, Google," U.S. Senate Select Committee on Intelligence, written responses, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/Google%20Response%20to%20Committee%20QFRs.pdf.

evaluate the respective foreign government's ability to access that U.S. person information, as well as the privacy protections and legal process available to affected U.S. persons.

Second, Google's Android phones collect data on all Wi-Fi base stations and send it back to Google as part of its mapping and location programs. At the same hearing, Mr. Walker was asked whether Google uses Wi-Fi networks on military bases or in other government buildings to map those locations.[3] We are concerned that DoD Wi-Fi base stations in military bases and facilities around the world could be mapped unwittingly by servicemembers using Android phones. This concern expands beyond phone use by servicemembers to include anybody, including foreign support personnel and even servicemembers' family on base, who happen to be carrying an Android phone while on or near a military site. In an era of increasingly contested cyber domains, we could be unknowingly allowing our adversaries to map DoD networks for cyber intelligence, surveillance, and reconnaissance and operational preparation of the environment.

Mr. Walker responded that Wi-Fi base station owners may opt-out of this collection by using a "nomap" process made available to consumers on one of Google's customer help pages. The instructions seem difficult to use, even if DoD personnel knew they existed at all. As many of our routine modern-day conveniences are now vulnerabilities that our adversaries can and will exploit, we respectfully request you answer the following questions within 30 days as part of your review.

1. Does the DoD regularly "nomap" its Wi-Fi networks so that Google cannot use them in location tracking?

2. Is it appropriate for the DoD and/or the U.S. Government to bear the burden of taking affirmative steps to prevent surreptitious mapping when it is not even party to any kind of contractual relationship with the entitity that is mapping?

3. Has Google, or any other internet technology company, ever notified the DoD that it should engage in this "nomap" step to protect the location of its Wi-Fi networks, and therefore, location of its service personnel? If so, when did DoD receive each notification? If not, what steps does DoD plan to take to remedy the providers' lack of notification?

4. Does U.S. Cyber Command, the associated service cyber components, and the Defense Information Systems Agency have the necessary resources to respond to the growing threat from location-tracking devices? What additional tools, resources, or partnerships with the private sector are necessary?

Thank you for your service to this nation and your attention to these matters of national security.

Sincerely,

---

[3] *Id.*

TOM COTTON
United States Senate

RICHARD BLUMENTHAL
United States Senate