

Department of Defense Learning about Data Security the Hard Way

January 30, 2018 - You may never have heard of a phone application called Strava. It is a fitness application that tracks your workout progress on your phone. One of the apps features is that it can track user workouts in great detail worldwide. To help promote the application, the company decided to publish something it calls a global "heat map". That map showed the activities of the apps users over a two month period. This past week, someone in Australia noticed that workouts were being tracked in some very remote areas of the Middle East. It turns out that many of those remote workouts were from American troops stationed in places like Syria, Iraq and Afghanistan. In fact, in some cases the troops were stationed at supposedly secret bases. That cat is now out of the bag.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

Strava's heat map provides a wealth of data to anyone who wants it. It actually tracks the routes that people run. Anyone looking at it regularly could probably figure out the popular running routes for specific military bases.

The company is taking this breach seriously and has said publically that they are committed to protecting people working in hostile environments. Unfortunately, the problem isn't limited to Strava. It actually has more to do with the capabilities of smart phones and devices such as smart watches, tablets and other exercise devices. It is very clear that the federal government needs to come up with policies to regulate the use of these devices in the military and with government contractors and NGOs.

All American smartphones have GPS built into them. While this allows the user to access GPS from just about anywhere, it also allows just about anyone who is interested to locate the phone. Google tracks pretty much everywhere you go with your Android devices unless you turn that tracking ability off. And since most phones are shipped with this tracking ability turned on, anyone with an Android device is vulnerable from the minute they first turn on their phone. Apple has similar features built into their phones.

What is largely a convenience item for the vast majority of the public presents a significant security issue for the government; especially the military. That said, there are a lot of civilians who have real reasons not to be tracked too. Victims of domestic violence. People that have been stalked. They have legitimate reasons for not wanting to be tracked by anyone.

How the government deals with this issue over the long term probably requires some study. But there is clearly an immediate need for a sort term solution. That should start with policies issued to employees (civilian and military) along

with instructions on how to carry out those policies. In this case, an order to turn off all tracking on all personally owned devices, instructions on how to go about this, and some teeth in the form of punishment for anyone who doesn't comply.

Over the long term, the Department of Defense really needs to look long and hard at the wisdom of placing people in the field and allowing them to take a smart phone with them. There is a happy medium when it comes to maintaining high morale and national security. We're not sure what that happy medium looks like but without some new policies, what happened in the case of Strava will happen again with other applications and, at some point, it will get someone killed. That's shouldn't be acceptable to anyone.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow me on Twitter:

Follow ACCESS