ISG Research™

Online Maps Reveal Secrets - Should Enterprises Worry?

News reports this week revealed some unintended consequences of personal but publicly available mapping data, specifically how a fitness app made a map available aggregating user activity, which also happened to unintentionally reveal locations and behavioral patterns of U.S. military personnel. Meanwhile, much less publicized - but

much more important in many ways - is an early January publication of vulnerabilities of certain location-tracking devices. We expect instances like these to not only continue but also to increase in number and volume, highlighting the urgent need for meaningful discussions about the Internet of Things, location privacy, and national security.

Publication date: Friday, 2 February 2018

Table of Contents

ONLINE MAPS REVEAL SECRETS - SHOULD ENTERPRISES WORRY?

By Ron Exler

WHAT IS HAPPENING?

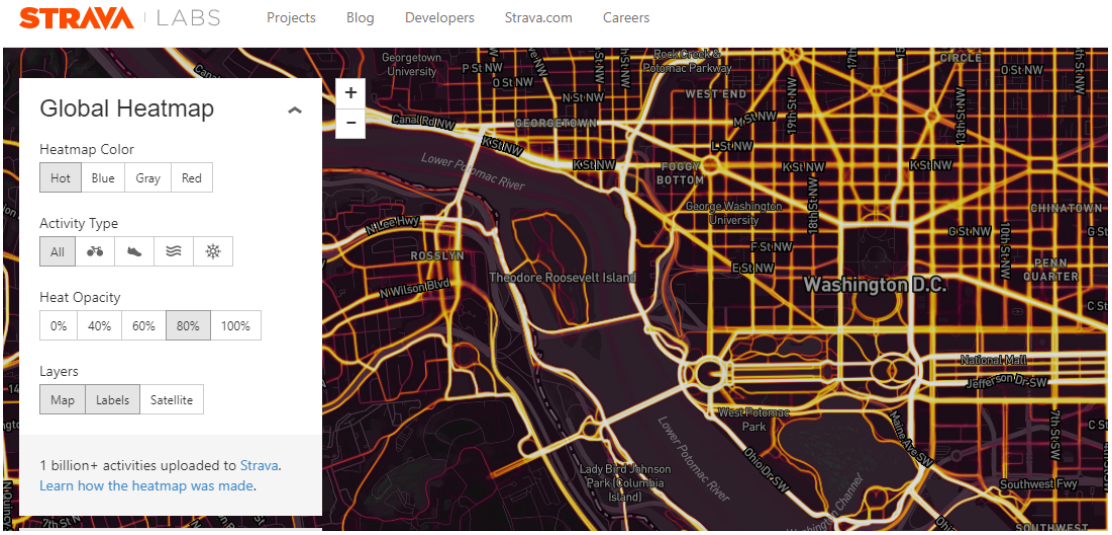
News reports this week revealed some unintended consequences of personal but publicly available mapping data, specifically how a fitness app made a map available aggregating user activity, which also happened to unintentionally reveal locations and behavioral patterns of U.S. military personnel. Meanwhile, much less publicized - but much more important in many ways - is an early January publication of vulnerabilities of certain location-tracking devices. We expect instances like these to not only continue but also to increase in number and volume, highlighting the urgent need for meaningful discussions about the Internet of Things, location privacy, and national security.

WHY IS IT HAPPENING?

The Strava fitness app is like many others that allows users to collect data on their personal fitness activities, such as running routes. Many fitness tracking wearables embed a Global Positioning System (GPS) chip that sends location data to the Cloud, where it's available for personal records and aggregated for other purposes.

In November 2017, Strava posted on its Web site a global "heat map" showing each of the approximately 3 million location data points ever uploaded to its service from more than 1 billion uploaded activities. Heat maps on the website show locations in aggregate with brightness or color variations as visual indication of the frequency of data points at each location (Figure 1).

Figure 1: Fitness Tracker Global Heat Map



Source: ISG Insights via Strava Web site

Among the noteworthy outcomes of heatmap analysis are (1) location and behaviors of personnel at military installations worldwide, and (2) the location of some otherwise-unpublicized government installations, military and otherwise. Obviously ,widespread knowledge of either of these data sets can put people, installations, and other assets at risk.

But there's more. Earlier in January, security researchers found vulnerabilities in some popular online services used to manage location-enabled devices. Unauthorized users could use the vulnerabilities, which include authorization and API glitches, to access the live location data of device users. Dubbed "Trackmageddon," *the vulnerabilities were identified in more than 100 services managing millions of devices.* While so far only reported in a few security-oriented publications, these vulnerabilities could be extremely serious for users of Internet of Things devices using the affected services, exposing not only live location data but also phone numbers and device types. Flaws could allow malicious updating of firmware and sending other commands to devices.

IMPACT

Identifying secret military locations or previously unknown information about places from technologies is nothing new. Pigeons wearing cameras took aerial photographs of enemy positions in World War I. Commercial satellites have for decades revealed sensitive information. In 2009, Google Earth images exposed a Pakistani airbase used by the U.S. for drone missions. Apple Maps imagery revealed a secret base in Taiwan.

Heat maps are also not new. In the most famous case, Dr. John Snow mapped a cholera outbreak in 1854 London and used the resulting heat maps to figure out that certain water pumps had sickness clusters nearby. The maps supported his theory that cholera is a water-borne disease. Today, heat maps have a variety of uses and with aerial photographs also show land use alteration, crop health, population density, and natural disaster damages.

For enterprises, there are important lessons in the Strava exposure and Trackmageddon discoveries. Millions of employees and contractors wear or carry tracking devices on the job. Fleet managers track truck drivers, for example. Wearables for workplace safety are appearing, and they include location tracking. Even employee information and services apps for mobile phones collect location data. Sensors can track asset location through supply chains. The data almost always goes to the cloud for use in a contracted service – and sometimes (if not usually), those services aggregate and resell collected data.

The U.S. Department of Defense is evaluating the security issues raised by the revelation of the Strava heat map, according to a Pentagon spokesperson. There could be changes to policies and procedures in response to the wearables situation. But such "evaluation" is reactive, not the proactive behavior ISG typically recommends.

It's not just the military that needs to protect secrets and staff. Sometimes businesses test innovative ideas or technologies in secret locations. Others have secret warehouses. Energy companies might want to hide locations of high-risk generation facilities. Employee whereabouts could be confidential at certain times.

Enterprises need to be transparent with employees, by telling them when and how apps collect, use, and share location data. Employer apps and devices may need "Off" switches for non-working times. Employers should also train employees on device usages and privacy policies concerning location. And enterprises should demand that any app services and devices selected must be transparent with the details of how they use, share, and protect all data collected, including location services.

We are still concerned that developers, providers, and users of many of the emerging connected devices and services consider security as an afterthought, if at all. *Enterprise buyers can help change that reality by demanding complete adherence to security best practices, both on devices and for collected data throughout the supplier chain of custody*. For now, however, it's buyer beware for consumers and businesses alike.

ASSOCIATED INSIGHTS

Five Reasons to Pay Attention to Location Services in 2018