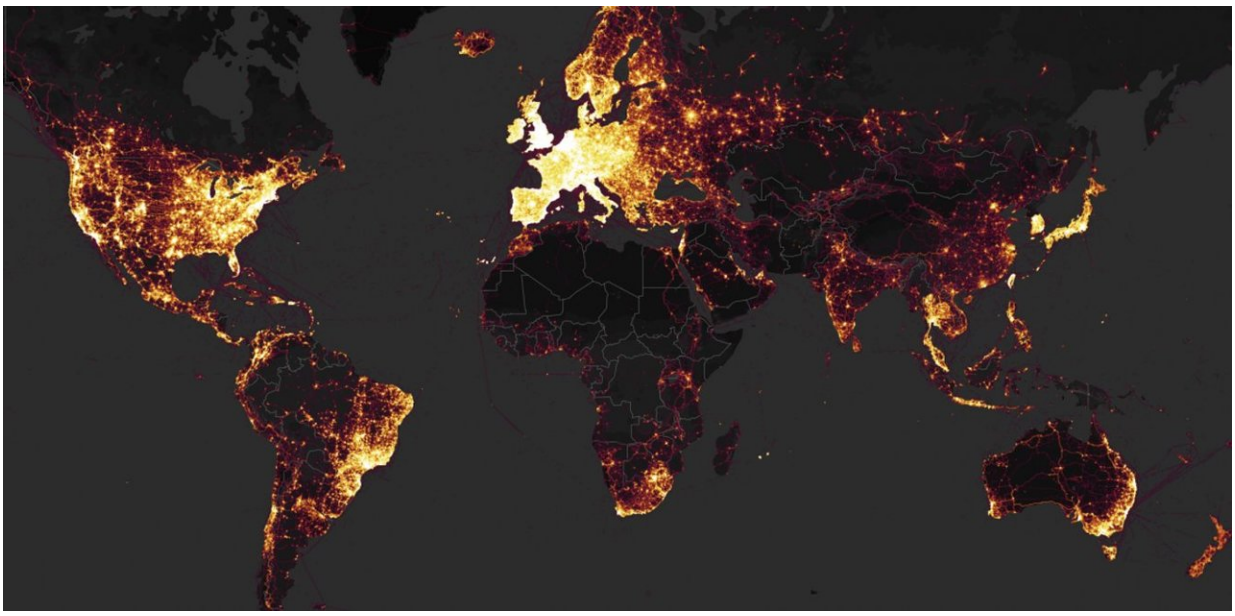
Strava storm: why everyone should check their smart gear security settings before going for a jog

February 1 2018, by Jason R. C. Nurse



Credit: Strava

Fitness tracking app Strava recently kicked off a privacy and security storm after it was revealed that its software had potentially exposed the location of secret military bases, courtesy of a data visualisation tool called a "heatmap".

The heatmap was created to depict the activities of Strava users across

the globe. But while it's a great idea in general (and quite a nice heatmap), a closer inspection of the user data generated by the tool highlights some worrying developments.

It's also a reality check for consumers of wearable gadgets – be they a National Security Agency operative or a retired librarian going for a gentle jog – who are lax with the privacy and security settings on apps that monitor location and other personal data.

Nathan Ruser, a 20-year-old student based in Australia, pored over Strava's heatmap and tweeted his findings, saying that the "pretty" data visualisation tool – which mapped 13 trillion GPS points from the app's users – wasn't "amazing for op-sec [operations security]. US bases are clearly identifiable and mappable."

By publishing the heatmap of Strava users' activities and their locations, the San Francisco-based company had seemingly leaked the location of secret bases and routes service personnel use for exercise.

Don't be dumb about smart tech

The Internet of Things (IoT) represents a new advancement in technology that harnesses data to help streamline our lives. The simplest way to think of the IoT is as a network of devices and objects with embedded electronics – deemed "smart" – that communicate to perform various tasks.

IoT technologies enable voice commands to control appliances such as lights, TVs and even door locks. At work, smart office buildings offer significant promise for handling controls such as energy saving options and may soon become ubiquitous. And, on the move, wearable technologies such as fitness trackers and smart watches allow people to track and monitor their exercise regimes.

But there are clear security and privacy concerns associated with using these different forms of new technology. And there's a danger that consumers – egged on by digital companies whose income heavily relies on data sharing – jump too quickly at the convenience of new personal tech without understanding the risks.

In research circles, the risks accompanying IoT technology – including data leakage via consumer wearables – have been known for some time now. One of the earliest comprehensive reports on the topic – from cyber security firm Symantec – linked wearables and other tracking devices to risks including identity theft, profiling and stalking users.

Credit: AI-generated image (disclaimer)

If a criminal accesses someone's real-time online fitness tracker data (be

it from Strava, FitBit or a smart watch) they could determine that person's whereabouts – in and out of work and home. Oversharing on social media has been a problem for many years as it can lead to crime online and in the physical world.

It gets worse. Recently, we conducted research on this topic, to investigate the potential dangers facing users when they share data from fitness trackers and social media.

We found that if a criminal or an organisation were able to combine data fragments gathered from a tracker and a social media profile, then users faced significant privacy risks.

These include financial loss (home burglary based on the knowledge of user location and address) and targeted profiling by marketing companies or even potential employers, who habitually screen candidates based on their online profiles.

Chairman of the bored

When speaking to users about these risks, we discovered their general awareness was quite low. The study confirmed other research that we have recently conducted where – to some users – "privacy is the boring bit" of using smart technologies.

The Strava incident, while important, is the tip of the iceberg when it comes to risks associated with the use of personal IoT technology in the workplace. For instance, an employee with a malware-infected smart device could then connect it to their employer's network.

While organisations are largely prepared for this type of risk if it originates from a personal laptop, it's a different issue with wearable devices – which are now being heavily targeted by malware miscreants.

The discrete nature of wearables presents another problem: they are typically paired with a secondary device and are more likely for that reason to avoid security measures, where checks are only conducted if a device is directly connected to the corporate network. Another real problem is that malicious employees seeking to harm their organisation may use IoT technology for nefarious means, such as stealing intellectual property, or using hidden devices to inconspicuously record private office conversations.

The Strava episode is a stark reminder that as technology becomes smarter, it poses significant risks to people's home, work and social lives if not properly considered, discussed and addressed. Privacy and security settings are there for a reason: use them.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Strava storm: why everyone should check their smart gear security settings before going for a jog (2018, February 1) retrieved 24 April 2024 from https://phys.org/news/2018-02-strava-storm-smart-gear.html