It's far too easy for abusers to exploit smart toys and trackers

June 7 2021, by Saheli Datta Burton and Madeline Carr

Credit: Karolina Grabowska from Pexels

The wearable technology market is booming, with half a billion wearables sold globally in 2020. Apps on these devices, or the devices themselves, often claim to monitor our health to spot illnesses, track our

workouts to help us reach our fitness goals, or keep an eye on our children's whereabouts to enhance their safety.

But they're also divisive. Supporters of wearable technology claim that health trackers should be prescribed by the NHS and could even deliver an early warning of a possible COVID-19 infection. GPS tracking devices designed to be worn by children, meanwhile, are seen as a safety asset for parents.

Yet studies have found fitness trackers to be too inaccurate and misleading to be used by medical professionals, and that, because they've been rushed to market, wearables of all kinds are an insecure "Wild West" region of technology that requires urgent regulation.

In a recent report, we looked at the security risks associated with wearable devices, as well as "smart toys" that can record children in their homes. We found a concerning lack of security—especially for devices aimed at children—which lack even the most basic cybersecurity precautions, leaving them open to abuse.

Fitness trackers and personal data

One key issue with wearables is the data they generate and share. For instance, many fitness trackers rely on data on a person's location to map their workouts. That's great if you're keen to track the distance of your jogs, but it's not especially sensible if you're embarking on those jogs from a military base in hostile territory.

> Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). https://t.co/hA6jcxfBQI … It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable pic.twitter.com/rBgGnOzasq

— Nathan Ruser (@Nrg8000) January 27, 2018

Beyond that specific example, which caused some embarrassment for the US military in 2018, it's clear that sharing your location publicly, even in a safe civilian setting, comes with significant risks.

And it's not just the real-time tracking of your running route that could expose your whereabouts. Because these trackers upload your workouts to an app and share them publicly, it's possible for predators to use historic running, biking or hiking routes to predict where you might be at a given time. This safety issue isn't only restricted to workouts. Even something as innocuous as sharing a photo through your Apple watch can give away your geolocation.

Are trackers safe for children?

Even more concerning are devices designed to be worn by children, sales of which are expected to reach $875 million (£620 million) by 2025. These watches are marketed as wearable tech to keep kids safe, tracking their location and alerting parents when the watch's onboard "SOS" button is pressed—or if the child travels beyond a geofenced area.

Smart watches as safety devices on children's wrists may sound like a boon for anxious parents, but a 2017 survey of children's smart watches found that the all-important "SOS" button either got stuck or didn't work at all in most cases.

Additionally, flaws in some smart watches' accompanying apps have raised serious safety concerns. Security researchers have found they could not only easily access children's historical route data—like their path to and from school—and monitor their geolocation in real time, but they could also speak directly to the child, through the watch, without the call being reported in the parent's app.

Connected toys

Fears that internet of things devices can give people unauthorized access to children also extend to the "smart toy" market. Some of these toys contain hidden cameras and microphones which, if hacked, could be used to record the interior of your home, including children's rooms.

In 2017, German regulators recognized this danger by banning the sale of the Cayla "smart doll," labeling it as the kind of "de facto espionage device" that Germany's Telecommunications Act legislates against. In an unusual and unsettling move, the regulator went further by asking parents who'd bought one to destroy the doll to prevent illicit surveillance.

> Goodbye Spy #Toy: #Germany Bans My Friend #Cayla Doll | https://t.co/RcIiVGTPWy #IoT #Security #Privacy #Surveillance pic.twitter.com/P6gkrDqzkU
>
> — HackRead.com (@HackRead) February 18, 2017

Even if the manufacturers of smart toys and children's smart watches can guarantee far better security than that which led to the Cayla ban, there remain other surveillance concerns. In 2019, a UNICEF-led report highlighted how children's rights—to creativity, freedom of choice and self-determination—are challenged by smart devices. Present in schools, at home, and on the wrist, this kind of round-the-clock surveillance, the report argues, restricts carefree childhood and hurts kids' development.

Making trackers safer

Trackers and toys can be made safer. Before we allow these devices to flood the market, it's essential we standardize the minimum security

requirements that manufacturers must comply with—no matter where in the world these devices are made.

Key among these standards should be the removal of factory-default passwords on devices—which, like "admin" or "1234," are easily guessed or discovered by even the most novice hacker. Manufacturers should also publish a vulnerability disclosure to help users understand risks, and make regular software updates in response to vulnerabilities unearthed by security researchers.

Clearly, monitoring people's health via wearable trackers has the potential to radically improve access to medical care. Likewise, every parent wants their child to be safe, and smart devices, like mobile phones before them, could be a reliable tool for checking in with them. But without safety standards, these devices have the potential to cause more harm than they offset. Regulators must act fast to stop this growing market from leading to significant harms.

Provided by The Conversation