

Product article:

<https://www.theverge.com/circuitbreaker/2019/5/23/18636839/amazon-wearable-emotions-report>

Components:

Microphone

Values tested:

Security

User safety

Privacy

Responsibility

Description:

Amazon preparing a wearable that 'reads human emotions,' says report. Bloomberg has spoken to a source and reviewed internal Amazon documents, which reportedly show the Alexa voice software team and Amazon's Lab126 hardware division are collaborating on the wearable in development. The device, working in sync with a smartphone app, is said to have microphones that can "discern the wearer's emotional state from the sound of his or her voice." In a mildly dystopian twist, Bloomberg adds that "eventually the technology could be able to advise the wearer how to interact more effectively with others."

Product article:

<https://techcrunch.com/2019/05/10/gps-trackers-flaw/>

Components:

GPS

Microphone

Values tested:

Security

User safety

Privacy

Responsibility

Description:

There are an estimated 10,000 devices in the U.K. — and thousands more around the world. The team told several of the device makers of the flaws, but Mabbitt said there's no way to fix the vulnerabilities without recalling every device.

Product article:

<https://www.dailymail.co.uk/health/article-2317536/Dementia-patients-fitted-GPS-tracking-device-s-save-police-time-money.html>
<https://gizmodo.com/japan-is-tagging-and-tracking-elderly-with-stickers-1789844123>

Components:

GPS

Values tested:

Inclusion
Security
Wellbeing

Description:

Is it better to track your loved ones even though it may mean they are a) targeted or b) exposed in terms of their security?

Product article:

<https://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/>

Components:

GPS + more classic wearable sensors - long review of several devices

Values tested:

Inclusion
Privacy
Wellbeing

Description:

The seductive lure of activity and health wearables make it easy to forget, or ignore, the inherent security and privacy risks involved. Imagine the impact after a few weeks of this behavior. Your poor sleep quality is triggered by alcohol and lack of exercise. These, combined with a sleep deficit that slowly affects your overall health, leads to weight gain, increased blood pressure, and other problems. And all of this data is stored in your wearable device—or, more accurately, in its cloud software. The fact that so much data is collected through a wearable device, such as an activity tracker, a smartwatch, or a pulse tracker, means that there are tangible risks involved. If that data was carelessly stored, and then stolen through a data breach by a malicious third party and sold to unscrupulous organizations that want to use that data to assess your health risks, you could one day face steep increases in health insurance, or even a policy cancellation. The risk of this is so real that some companies are buying data breach insurance to protect themselves in the case of consumer information getting into the wrong hands. If you've willingly shared this data with your health insurer, through discount options at work, you may already be facing rising insurance costs without any data breach necessary, since many employers offer "good health" discounts to employees who stay within regulation weight and exercise parameters to receive a significant savings on health insurance. These are significant repercussions for simply wearing a device on your wrist to tell you how many steps you took a day and what your resting heart rate averages. It's up to the consumer to determine the level of risk they're willing to take versus the benefit they get from their wearable devices.

Product article:

<https://securelist.com/i-know-where-your-pet-is/85600/>

Components:

BLE, GPS sensor

Values tested:

privacy

data ownership - shares data with 3rd parties unexpectedly

security

Description:

Trackers often use Bluetooth LE technology to communicate with the owner's smartphone, but not always correctly. If not done correctly, the device can receive and execute commands from anyone. Moreover, they can be disabled or hidden from the owner—all that's required is proximity to the tracker.

Product article:

<https://www.nbcnews.com/tech/tech-news/net-connected-vibrator-collects-users-intimate-data-lawsuit-claims-n843566>

Component:

Data storage methods

Microphone

Values tested:

data ownership

privacy

security

questions the value of being sensitive to the misuse of collected intimate data

Description:

Lovense's privacy policy says any data that pass through its servers are encrypted and are deleted within seven days. It says video calls between partners are encrypted and don't pass through its servers at all.

Product article:

<https://www.pentestpartners.com/security-blog/screwdriving-locating-and-exploiting-smart-adult-toys/>

Component:

Bluetooth Low Energy

Microphone

Values tested:

Security

Data ownership

Description:

What you save in battery life and complexity comes at the price of easy discoverability and exploitability. Whilst BLE does have support for security, it is rarely implemented. When it is implemented it's often done poorly.

The app for this device potentially collects a lot of personal and intimate data -- the app accesses your phone or tablet's microphone, camera, and location tracking. That means a lot of potentially intimate information could be hacked or shared without consent if something went wrong.

Product article:

Google Home

<https://foundation.mozilla.org/en/privacynotincluded/products/google-home/>

Component:

Microphone

Location

Values tested:

Privacy

Description:

As Google Home shares your information with 3rd parties for unexpected reasons and can “spy” through your microphone without your knowledge as well as grab your GPS, there is the potential for targeted advertising following you around the internet.

Product article:

https://sec-consult.com/en/blog/2018/06/true-story-the-case-of-a-hacked-baby-monitor-gwelltimes-p2p-cloud/?_ga=2.64405679.100405736.1536015084-963322602.1536015084

Component:

Camera

Microphone

Values tested:

Privacy

Security

Data ownership

Responsibility

Description:

Here we have a Chinese company that is never mentioned anywhere, developing insecure products and sending our most private information home to their Chinese servers. Although they have been confronted with the security issues months ago, they have decided not to fix them. It seems that consumer electronics with opaque supply chains, paired with insecure, built-in cloud features that are enabled by default will keep us busy in the future.

“I feel so violated,” she wrote on Facebook. “This person has watched me day in and day out in the most personal and intimate moments between my son and I. I am supposed to be my son’s protector and have failed miserably. I honestly don’t ever want to go back into my own bedroom.”

“They then gave us the number and email for the company. The number was out of service and obviously no one has responded to the email.”

Product article:

<https://arstechnica.com/tech-policy/2018/11/amazon-must-give-up-echo-recordings-in-double-murder-case-judge-rules/>

<https://foundation.mozilla.org/en/privacynotincluded/products/amazon-echo-show-spot/>

Component:

Microphone

Camera

Values tested:

Data ownership - do users really own their own data? At what point should the company own it?

Privacy

Description:

"Amazon does not seek to obstruct any lawful investigation but rather seeks to protect the privacy rights of its customers when the government is seeking their data from Amazon, especially when that data may include expressive content protected by the First Amendment," company lawyers [wrote](#) at the time.

Product article:

Q50 Child tracking watch: The Q50 is a smart watch designed for children. Allowing guardians to track the child's location, send messages, remotely monitor the child's surroundings and conversations and receive SOS alerts from the child among other features.

Component:

GPS

Microphone

Messaging

Server

Values tested:

Privacy

Security

Description:

Monitor conversations

Spoof location of watch

Intercept location of watch

Update / delete safety numbers on the phone

Product article:

Alexa recorded private conversation and sent it to random contact

Alexa user eavesdropped on another Alexa home

Component:

Mic

Values tested:

Security

Privacy

Description:

Company has stated that device does not record, but then...

Product article:

https://www.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

Component:

Mic

Database

Values tested:

Security

Privacy

Responsibility

Description:

All the contacts were exposed and cloudPets were overwritten with other data as well as threatening to delete all the data in the cloudPets.

Company did not own up to the mistake or alert their users.

"My bigger concern is that someone may be able to use this information to send inappropriate messages to my 6 year old daughter," pagel told Motherboard via email. "[My parents] certainly won't be sending any more messages to their granddaughter through this. And while I doubt we will throw the toy away, it's effectively been reduced to a way overpriced stuffed animal."

Product article:

<https://www.theverge.com/platform/amp/2017/10/10/16456050/google-home-mini-always-recording-bug>

Component:

Mic

Values tested:

Security

Privacy

Responsibility

Description:

Google Home Mini was randomly and near-constantly recording sounds in his home and transmitting them to Google. The company acknowledged the problem and is issuing a software update to resolve the issue, which appears to boil down to a failure of the touch sensor on the top. That seems to be the rub (pardon the pun) with Russakovskii's Mini: it thought that somebody was holding its finger down on the top and so was randomly activating and recording. The good news is that the lights turned on to indicate it was listening, but the bad news is that it didn't make an audible tone, so it took a trip through the Home's search history to discover the error.

SUGGESTIONS OF HOW TO DO THINGS DIFFERENTLY

<https://www.pentestpartners.com/security-blog/screwdriving-locating-and-exploiting-smart-adult-toys/>

BLE**WiFi**

IOT Video streaming: appropriate security measures on this WiFi connection would have mitigated the video interception vulnerabilities, yet only one of the manufacturers required a

password to connect to the WiFi hotspot, and this password was hardcoded, the same across all devices and easily looked up online.

Firmware updates

Can be hacked and therefore object can be damaged / device can be infiltrated and new software added

Buttons

In positive security practices, the Dino companion application does use TLS for communicating with the server and the device itself does require a button being pressed before it will record anything.

To Google's credit, it seems to have scrambled the engineering jets to figure out the issue and create a fix. The fix, though, is removing a feature from the Mini. Google has altered the software so a simple touch won't activate the Assistant, you have to say the wake word instead. Here's Google's statement about the issue.

Storage

Per the privacy policy: audio data collected for speech recognition is processed on the device and are not sent to remote servers.

Facial recognition

China is using A.I. to profile a minority: in a major ethical leap for the tech world, Chinese start-ups have built algorithms that the government uses to track members of a largely Muslim minority group.

Amazon's Rekognition software has been used by the police but returns inaccurate or biased results.

TRICKY COMPONENTS

Mozilla's guide has three basic questions to assess a device's ability to spy on its users: Does it have a camera? How about a microphone? Is it tracking your location?

Cameras, microphones, and location tracking capability are either embedded in the device or in the accompanying app used to control the device or both.

Mozilla also asks users as well to evaluate a product based on whether it uses product encryption, share information with third parties, allows a user or parental controls, provide security update and delete data its stores about the user.