

How smart toys may be spying on kids: What parents need to know

August 26 2024, by Angelika Jacobs



Twelve toys were examined in a study on smart toys and privacy. Credit: University of Basel / Céline Emch

Toniebox, Tiptoi, and Tamagotchi are smart toys, offering interactive play through software and internet access. However, many of these toys

raise privacy concerns, and some even collect extensive behavioral data about children, report researchers at the University of Basel, Switzerland.

The Toniebox and the figurines it comes with are especially popular with small [children](#). They're much easier to use than standard music players, allowing kids to turn on music and audio content themselves whenever they want. All a child has to do is place a plastic version of Peppa Pig onto the box and the story starts to play. When the child wants to stop the story, they simply remove the figurine. To rewind and fast-forward, the child can tilt the box to the left or right, respectively.

A lot of parents are probably thinking, "Fantastic concept!" Not so fast—the Toniebox records exactly when it is activated and by which figurine, when the child stops playback, and to which spot they rewind or fast-forward. Then it sends the data to the manufacturer.

The Toniebox is one of twelve smart [toys](#) studied by researchers headed by Professor Isabel Wagner of the Department of Mathematics and Computer Science at the University of Basel. These included well-known toys like the Tiptoi smart pen, the Edurino learning app, and the Tamagotchi virtual pet as well as the Toniebox. The researchers also studied less well-known products like the Moorebot, a mobile robot with a camera and microphone, and Kidibuzz, a smartphone for kids with parental controls.

One focus of the analysis was security: is data traffic encrypted, and how well? The researchers also investigated data protection, transparency (how easy it is for users to find out what data is collected), and compliance with the EU General Data Protection Regulation. Wagner and her colleagues are presenting their results at the [Annual Privacy Forum](#) in early September.

The paper is [published](#) in the journal *Privacy Technologies and Policy*.

Collect data while offline, send it while online

Neither the Toniebox nor the Tiptoi pen come out well with respect to security, as they do not securely encrypt data traffic. The two toys differ with regard to [privacy concerns](#), though: While the Toniebox does collect data and send it to the manufacturer, the Tiptoi pen does not record how and when a child uses it.

Even if the Toniebox were operated offline and only temporarily connected to the internet while downloading new audio content, the device could store collected data locally and transmit it to the manufacturer at the next opportunity, Wagner surmises. Wagner says, "In another toy we're currently studying that integrates ChatGPT, we're seeing that log data regularly vanishes." The system is probably set up to delete the local copy of transmitted data to optimize internal storage use, Wagner says.

Companies often claim the collected data helps them optimize their devices. Yet it is far from obvious to users what purpose this data could serve. "The apps bundled with some of these toys demand entirely unnecessary access rights, such as to a smartphone's location or microphone," says the researcher. The ChatGPT toy still being analyzed also transmits a data stream that looks like audio. Perhaps the company wants to optimize [speech recognition](#) for children's voices, the Professor of Cyber Security speculates.

A data protection label

"Children's privacy requires special protection," emphasizes Julika Feldbusch, first author of the study. She argues that toy manufacturers

should place greater weight on privacy and on the security of their products than they currently do in light of their young target audience.

The researchers recommend that compliance with security and [data protection](#) standards be identified by a label on the packaging, similar to nutritional information on food items. Currently, it's too difficult for parents to assess the security risks that smart toys pose to their children.

"We're already seeing signs of a two-tier society when it comes to privacy protection for children," says Feldbusch. "Well-informed parents engage with the issue and can choose toys that do not create behavioral profiles of their children. But many lack the [technical knowledge](#) or don't have time to think about this stuff in detail."

You could argue that individual children probably won't experience negative consequences due to toy manufacturers creating profiles of them, says Wagner. "But nobody really knows that for sure. For example, [constant surveillance](#) can have negative effects on personal development," Wagner adds.

More information: Julika Feldbusch et al, No Transparency for Smart Toys, *Privacy Technologies and Policy* (2024). [DOI: 10.1007/978-3-031-68024-3_11](#)

Provided by University of Basel

Citation: How smart toys may be spying on kids: What parents need to know (2024, August 26) retrieved 3 September 2024 from <https://techxplore.com/news/2024-08-smart-toys-spying-kids-parents.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.