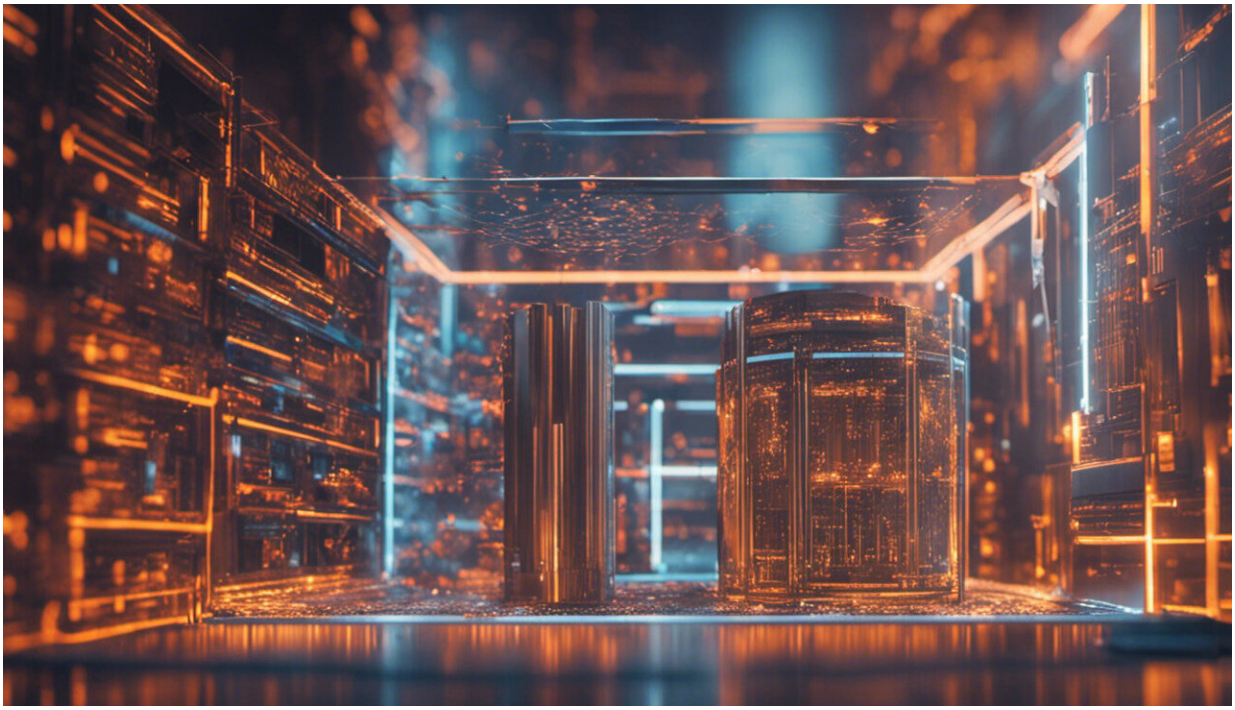
4 ways 'internet of things' toys endanger children

May 10 2018, by Marie-Helen Maras



Credit: AI-generated image (disclaimer)

As Amazon releases an Echo Dot smart-home device aimed at children, it's entering a busy and growing marketplace. More than one-third of U.S. homes with children has at least one "internet of things" connected toy – like a cuddly creature who can listen to and respond to a child's inquiries. Many more of these devices are on the way, around the world

and in North America specifically.

These toys wirelessly connect with online databases to recognize voices and images, identifying children's queries, commands and requests and responding to them. They're often billed as improving children's quality of play, providing children with new experiences of collaborative play, and developing children's literacy, numeric and social skills.

Online devices raise privacy concerns for all their users, but children are particularly vulnerable and have special legal protections. Consumer advocates have raised alarms about the toys' insecure wireless internet connections – either directly over Wi-Fi or via Bluetooth to a smartphone or tablet with internet access.

As someone with both academic and practical experience in security, law enforcement and applied technology, I know these fears are not hypothetical. Here are four examples of when internet of things toys put kids' security and privacy at risk.

1. Unsecured wireless connections

Some "internet of things" toys can connect to smartphone apps without any form of authentication. So a user can download a free app, find an associated toy nearby, and then communicate directly with the child playing with that toy. In 2015, security researchers discovered that Hello Barbie, an internet-enabled Barbie doll, automatically connected to unsecured Wi-Fi networks that broadcast the network name "Barbie." It would be very simple for an attacker to set up a Wi-Fi network with that name and communicate directly with an unsuspecting child.

The same thing could happen with unsecured Bluetooth connections to the Toy-Fi Teddy, I-Que Intelligent Robot and Furby Connect toys, a British consumer watchdog group revealed in 2017.

The toys' ability to monitor children – even when used as intended and connected to official networks belonging to a toy's manufacturer – violates Germany's anti-surveillance laws. In 2017, German authorities declared the My Friend Cayla doll was an "illegal espionage apparatus," ordering stores to pull it off the shelves and requiring parents to destroy or disable the toys.

Unsecured devices allow attackers to do more than just talk to children: A toy can talk to another internet-connected device, too. In 2017, security researchers hijacked a CloudPets connected stuffed animal and used it to place an order through an Amazon Echo in the same room.

2. Tracking kids' movements

Some internet-connected toys have GPS like those in fitness trackers and smartphones, which can also reveal users' locations, even if those users are children. In addition, the Bluetooth communications some toys use can be detected as far away as 30 feet. If someone within that range looks for a Bluetooth device – even if they're only seeking to pair their own headphones with a smartphone – they'll see the toy's name, and know a child is nearby.

For instance, the Consumer Council of Norway found that smartwatches marketed to children were storing and transmitting locations without encryption, allowing strangers to track children's movements. That group issued an alert in its country, but the discovery led authorities in Germany to ban the sale of children's smartwatches.

3. Poor data protections

Internet-connected toys have cameras that watch kids and microphones that listen to them, recording what they see and hear. Sometimes they

send that information to company servers that analyze the inputs and send back directions on how the toy should respond. But those functions can also be hijacked to listen in on family conversations or take photographs or video of children without the kids or parents ever noticing.

Toy manufacturers don't always ensure the data is stored and transmitted securely, even when laws require it: In 2018, toymaker VTech was fined US$650,000 for failing to fulfill its promises to encrypt private data and for violating U.S. laws protecting children's privacy.

4. Working with third parties

Toy companies have also shared the information they collect about kids with other companies – much as Facebook shared its users' data with Cambridge Analytica and other firms.

And they can also surreptitiously share information from third parties with kids. One toy company came under fire, for example, in both Norway and the U.S. for a business relationship with Disney in which the My Friend Cayla doll was programmed to discuss what were described as the doll's favorite Disney movies with kids. Parents weren't told about this arrangement, which critics said amounted to "product placement"-style advertising in a toy.

What can parents do?

In my view, and according to consumer advice from the FBI, parents should carefully research internet-connected toys before buying them, and evaluate their capabilities, functioning, and security and privacy settings before bringing these devices into their homes. Without proper safeguards – by parents, if not toy companies – children are at risk, both

individually and through collection of aggregate data about kids' activities.

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

Provided by The Conversation