Hello Barbie, hello hackers—accessing personal data will be child's play

December 15 2015, by Emmeline Taylor And Katina Michael

Who is she talking to? Credit: Mattel

At the top of some children's Christmas present wish list this year will be the new Hello Barbie doll.

Mattel's latest doll connects to the internet via Wi-Fi and uses interactive voice response (IVR) to effectively converse with children. When the doll's belt button is pushed, conversations are recorded and uploaded to servers operated by Mattel's partner, ToyTalk.

Hello Barbie tries to engage with children in intelligible and free-flowing conversation by asking and responding to questions, as well as being able to learn about its users over time.

As Mattel's website says:

Just like a real friend, Hello Barbie doll listens and adapts to the user's likes and dislikes.

But is Barbie the friend she promises to be?

Some might welcome Hello Barbie and similar talking dolls, such as My Friend Cayla, as a fun and novel development in smart toys that will keep children occupied. Others have expressed concerns, such as the #HellNoBarbie from the Campaign for a Commercial-Free Childhood.

As one reporter found, Hello Barbie prompts those conversing with her to divulge information about themselves, but when the focus is on her she quickly changes the subject to invariably gender-normative subjects and fashion.

Hello Barbie: Let's get serious and talk about something really important: fashion.

She mines children for personal details but gives little in return, other than vacuous compliments and fashion advice. Her friend credentials come further into question as she routinely discloses all the information gathered to ToyTalk who operate the speech processing services for Hello Barbie.

What's in the privacy statement?

As with many products, the detail that really matters is in the fine print; in this instance ToyTalk's Hello Barbie privacy statement, so there are a few important points to consider before wrapping her up and putting her under the Christmas tree.

ToyTalk outlines that it may:

[…] use, store, process, convert, transcribe, analyze or review Recordings in order to provide, maintain, analyze and improve the functioning of the Services, to develop, test or improve speech recognition technology and artificial intelligence algorithms, or for other research and development and data analysis purposes.

Essentially it can use the information gathered from the child, or anyone who converses with Hello Barbie, for any purpose that it chooses under the vague wording "data analysis purposes".

ToyTalk will also share recordings with unknown "vendors, consultants, and other service providers" as well as "responding to lawful subpoenas, warrants, or court orders".

Has Hello Barbie become a sophisticated surveillance device masquerading as an innocuous child's toy?

In England, the draft Investigatory Powers Bill introduces "equipment interference", which allows security and intelligence agencies to interfere with electronic equipment in order to obtain data, such as communications, from a device. This would mean that government agencies could lawfully take over children's toys and use them to monitor suspects.

These data collection practices are significant, as they reach much deeper than marketing practices that collect information about children's

likes and preferences. In conversing with toys, such as Hello Barbie, children reveal their innermost thoughts and private play conversations, details of which are intended for no one else to hear.

Once a child has developed a friendship with Hello Barbie, it might not be so easy to take her away.

Security risks

ToyTalk does recognise that "no security measures are perfect" and that no method of data transmission can ever be "guaranteed against any interception or other type of misuse".

Just last month the toy maker VTech reported 11.6 million accounts were compromised in a cyberattack, including those of 6.3 million children. Photos of children and parents, audio files, chat logs and the name, gender and birth date of children were accessed by the hackers.

It's not just toys that are at risk. There are ongoing reports of baby monitors being hacked so that outsiders can view live footage of children (and family), talk to the infant and even control the camera remotely.

Smart toys are going to be tempting propositions for hackers, with some already proving that they could make My Friend Cayla swear, to more usual targets such as hacking credit card details.

Barbie has also been in hot water before. The Barbie Video Girl has a camera lens embedded in the doll's chest disguised as a pendant which prompted the FBI to issue a warning that it could be used to make child pornography.

The Internet of Things provides direct access to children and their spaces through an increasing array of products and gizmos. Such security

breaches not only act as a stark reminder of the vulnerability of children's high-tech toys, but also lead us to reflect on other risks the trend in so-called smart toys might be introducing into children's lives.

An invasion of play

But Hello Barbie doesn't just reveal a child's private conversations to large corporations, and potentially law enforcement agencies. She also tells tales much closer to home: to parents.

A smartphone app enables parents to listen to the conversations between their child and their Hello Barbie. They can also receive alerts when new recordings become available, and can access and review the audio files.

Anyone with access to the parent account can also choose to share recordings and other content via Facebook, Twitter or YouTube. While some may see this as a novel feature, it is important to consider the potential loss of privacy to the child.

Play is an important part of the way children learn about the world. A key part of this is the opportunity for private spaces to engage in creative play without concerns about adults intruding.

It looks like Hello Barbie's dream to be a fashion-setter might just come true as she pioneers a new trend for smart and connected toys. In turn, the child loses out on both a trusted toy and on the spaces where they can lose themselves in other worlds without worrying about who's listening in.

Source: The Conversation