



Emmeline Taylor



Katina Michael

At the top of some children's Christmas present wish list in 2015 would have been the new *Hello Barbie* doll (1). Mattel's latest doll connects to the Internet via Wi-Fi and uses interactive voice response (IVR) to effectively converse with children (2). When the doll's belt button is pushed, conversations are recorded and uploaded to servers operated by Mattel's partner, ToyTalk (3).

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 (4). As Mattel's website says (1): "Just like a real friend, Hello Barbie doll listens and adapts to the user's likes and dislikes" (5).

But is Barbie the Friend She Promises to Be?

Some might welcome Hello Barbie, and similar talking dolls such as *My Friend Cayla* (6), as a fun and novel development in smart toys that will keep children occupied. Others have voiced concerns, such as the #HellNoBarbie (7) from the *Campaign for a Commercial-Free Childhood* (8).

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 (9). "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 the fine print is in ToyTalk's Hello Barbie privacy statement, so there are a few important points to consider before wrapping her up and

putting her under a Christmas tree (10).

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 (11)?

In England, the draft Investigatory Powers Bill introduced “equipment interference,” which allows security and intelligence agencies to interfere with electronic equipment in order to obtain data, such as communications from a device (12). 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 recognize 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 (13). Photos of children and parents, audio files, chat logs, and the name, gender, and birthdate of children were accessed by the hackers (14).

It’s not just toys that are at risk (15). 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 (16).

Smart toys are going to be tempting propositions for hackers, with some already proving that they could make My Friend Cayla swear (17), to more usual targets such as hacking credit card details (18).

Barbie has also been in hot water before (19). The Barbie Video Girl (20) 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 (21).

The Internet of Things provides direct access to children and their spaces through an increasing array of products and gizmos (22). 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 that 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 cre-

ative 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.

Acknowledgment

This article is adapted from an article published in *The Conversation* titled “Hello Barbie, hello hackers: Accessing personal data will be child’s play,” on Dec. 16, 2015. Read the original article <http://theconversation.com/hello-barbie-hello-hackers-accessing-personal-data-will-be-childs-play-52082>.

Author Information

Emmeline Taylor is Senior Lecturer, Criminology, Australian National University.

Katina Michael is Professor, Faculty of Engineering and Information Sciences, University of Wollongong, Australia.

References

- (1) “Hello Barbie™ Doll - Blonde Hair,” *Mattel Shop*, 2016; <http://shop.mattel.com/product/index.jsp?productId=65561726>.
- (2) K. Michael and A. Hayes. “High-tech child’s play in the Cloud,” *IEEE Consumer Electronics Mag.*, vol. 5, no. 1, pp. 123-128, 2015.
- (3) “About us,” *Toy Talk*, 2016; <https://www.toytalk.com/about/>.
- (4) Chip Chick, “Hello Barbie is world’s first interactive Barbie Doll,” *YouTube*, Feb. 15, 2015; <https://www.youtube.com/watch?v=RJMvmVCwoNM>.
- (5) CNET, “CNET News – Saying hello to Hello Barbie,” *YouTube*, Sept. 16, 2015; <https://www.youtube.com/watch?v=zVaVaf8QqWc>.
- (6) *My Friend Cayla*, 2014; <http://myfriendcayla.co.uk>.
- (7) CCFC, “Hell no Barbie: 8 reasons to leave Hello Barbie on the shelf,” *Campaign for Commercial-Free Childhood*, 2015; <http://www.commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf>.
- (8) *Campaign for Commercial-Free Childhood*, 2016; <http://www.commercialfreechildhood.org/>.

- (9) Z. Jason, "Hello Barbie: Fashion-obsessed talking doll thinks I'm amazing – Or so she said," *The Guardian*, Dec. 4, 2015; <http://www.theguardian.com/life-andstyle/2015/dec/04/hello-barbie-talking-doll-mattel-toy-talk-fashion>.
- (10) "Privacy policy," *Toy Talk*, Jan. 5, 2016; <https://www.toytalk.com/hellobarbie/privacy/>.
- (11) Tomo News.Net, "Hello Barbie 'creepy eavesdropping doll' at New York Toy Fair violates privacy," *YouTube*, Mar. 13, 2015; <https://www.youtube.com/watch?v=31GvRZKWrhQ>.
- (12) Draft Investigatory Powers Bill, U.K. Parliament, 2015; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.
- (13) Press release, "FAQ about cyber attack on VTech Learning Lodge," *vtech*, Feb. 3, 2016; https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge/.
- (14) D. Goodin, "Internet-connected Hello Barbie doll gets bitten by nasty POODLE crypto bug," *The Guardian*, Dec. 5, 2015; <http://arstechnica.com/security/2015/12/internet-connected-hello-barbie-doll-gets-bitten-by-nasty-poodle-crypto-bug/>.
- (15) P. Timms, "Hello Barbie: Wi-fi enabled doll labelled a bedroom security risk," *ABC News* (Australia), Nov. 28, 2015; <http://www.abc.net.au/news/2015-11-27/wi-fi-enabled-hello-barbie-doll-raises-security-concerns/6981528>.
- (16) K. Albrecht and L. McIntyre, "Privacy nightmare: When baby monitors go bad," *IEEE Technology & Society Mag.*, Sept. 2015; <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7270426>.
- (17) K. Munro, "Making children's toys swear," *PenTestPartners.com*, Jan. 23, 2015; <http://www.pentestpartners.com/blog/making-childrens-toys-swear/>.
- (18) R. Hackett, "Hello Barbie Doll vulnerable to hackers," *Fortune*, Dec. 4, 2015; <http://fortune.com/2015/12/04/hello-barbie-hack/?iid=sr-link1>.
- (19) K. Michael, "The FBI's cybercrime alert on Mattel's Barbie Video Girl: A possible method for the production of child pornography or just another point of view," presented at *4th Reg. Conf. Cybercrime and Int. Criminal Cooperation (CICC11)*, Sydney, Australia, May 2011.
- (20) "Barbie® Video Girl™ Doll," *Mattel Fisher Price*, 2015; <http://service.mattel.com/us/TechnicalProductDetail.aspx?prodno=R4807&siteid=27&catid1=508>.
- (21) L. Goode, "FBI: Video Barbie could hold evidence in child abuse cases," *WSJ*, Dec. 8, 2010; <http://blogs.wsj.com/digits/search/fbi%20video%20girl%20doll%20could%20hold%20evidence/?s=fbi+video+girl+doll+could+hold+evidence>.
- (22) K. Albrecht and K. Michael, "Connected: To everyone and everything," *IEEE Technology & Society Mag.*, vol. 32, no. 4, pp. 31-34, 2013.

TS

CORRECTION

In the Fiction feature "Held Captive in Cyberworld" by Michael Eldred in the December 2015 issue of *IEEE Technology and Society Magazine* there were errors introduced in editing and typesetting that interfered with meaning in significant ways.

On page 56, column 2, line 5 "the Matta called Turingia" should read "Matta called Turingia". On page 57, column 1, line 3 "produce as third" should read "produce a third". On page 57, column 1, line 32 – due to an editing error, the text reads "automatically affect a solution," when it should have read: "automatically effect a solution." Unfortunately, this error made nonsense out of a precise statement about how a Turing machine works.

On page 61, column 3, and continuing on to page 62 characters that should have been printed as Greek theta (θ) were printed as "q", and instances of the Greek letter pi (π) were printed as "p."

Also, in the same section, superscripts were dropped ("e.^{sup}(i θ) becoming "eiq" and "e.^{sup}(i π) becoming "eip").

These problems on pp. 61 and 62 rendered the text incomprehensible because the linking pun on "pie" and "pi" (Greek letter) and the humorous graphic interpretation of Euler's identity as an electron ridden by an imaginary number with a pi(e) in its hand became mangled.

TS