Engaging Science, Technology, and Society 2 (2016), 242-246 DOI:10.17351/ests2016.84

Your New Best Frenemy:
Hello Barbie and Privacy Without Screens

MEG LETA JONES[1]
GEORGETOWN UNIVERSITY

Abstract

Hello Barbie, a "smart toy" that uses voice recognition and WiFi to interact with children, has raised significant privacy concerns among commentators. She represents not only a new type of toy but is also a device categorized in the Internet of Things (IoT). This Critical Engagement investigates what privacy means and how it is effectuated when there is no screen to provide notice and consent by asking how one knows if Hello Barbie can keep a secret.

Keywords

smart toys; privacy; surveillance; comparative policy; Internet of Things

Introduction

Hello Barbie, Mattel's newest interactive smart toy, says she's your best friend. When asked, "Barbie, would you say we're friends?" Barbie replies, "Of course we're friends! Actually, you're one of my best friends. I feel like we could talk about anything!" Perhaps Barbie can trust you with all her secrets, but can you trust her with yours?

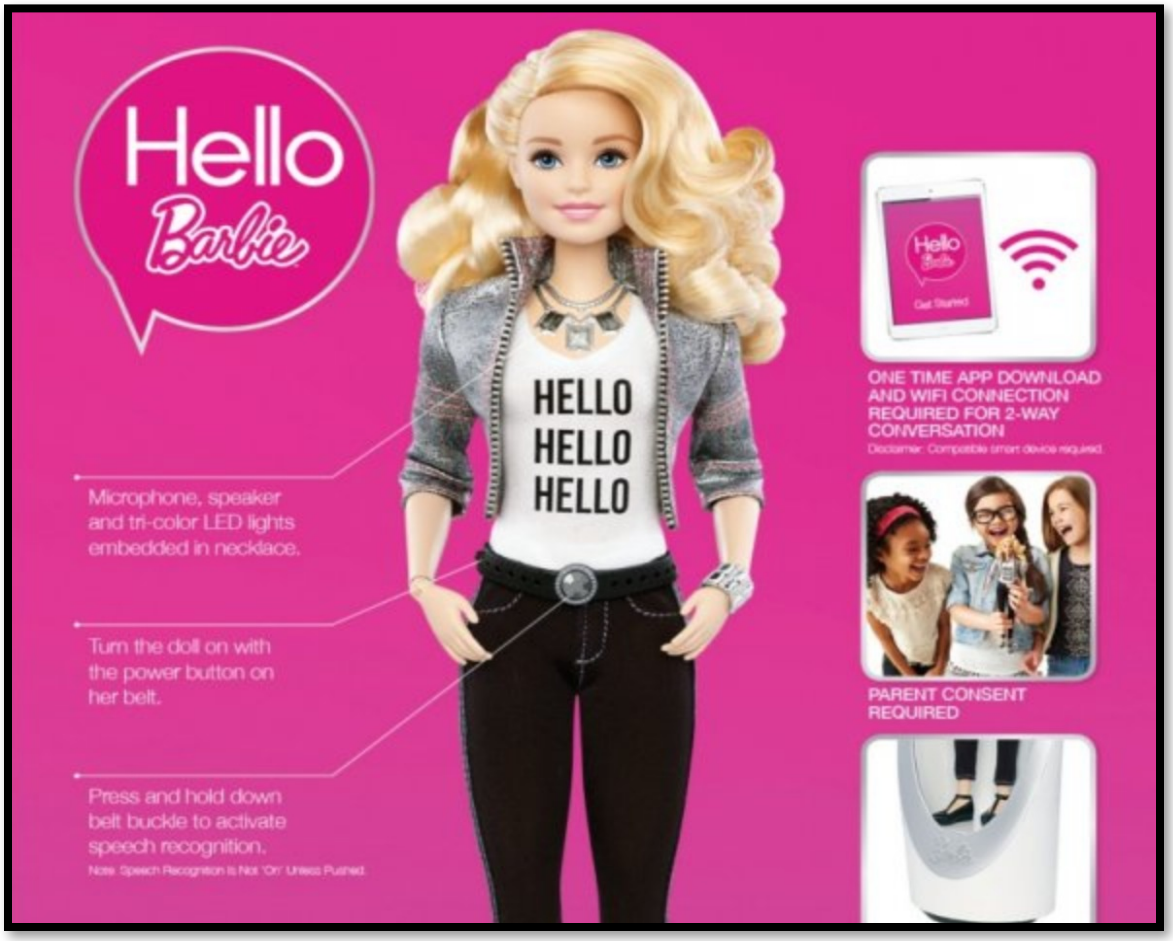
---

[1] Meg Leta Jones, Email: ma1318@georgetown.edu

Copyright © 2016 (Meg Leta Jones). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at estsjournal.org.

Notice and Consent

For at least the last fifty years, through the so-called Fair Information Practices Principles, notice and choice has dominated the meaning and effectuation of privacy, complemented by tenets of consent, transparency, accountability, and security. Notice and choice (N&C) regimes are intended to notify users of information collected and used and provide users with a choice of whether they wish to continue with the information exchange. For the last twenty years, if you wanted to know how a platform or interface or any networked ICT system collected and used your data, you could rely on one of your many personal screens to present a privacy policy—the common blue link at the bottom of most web pages. The privacy policy is central to N&C privacy regimes. These links tell users how information is collected, processed, and shared by the data collector, and users decide whether to engage with the site or not.


Hello
Barbie
HELLO
HELLO
HELLO
Microphone, speaker and tri-color LED lights embedded in necklace.
Turn the doll on with the power button on her belt.
Press and hold down belt buckle to activate speech recognition.
Note: Speech Recognition Is Not 'On' Unless Pushed
Hello Barbie
Get Started
ONE TIME APP DOWNLOAD AND WIFI CONNECTION REQUIRED FOR 2-WAY CONVERSATION
Disclaimer: Compatible smart device required.
PARENT CONSENT REQUIRED

The problems with notice and choice on the screen include that nobody could read so many policies, not many people can actually understand them, and there is rarely an opportunity to make a different choice. But Hello Barbie has no screen, no blue link at the bottom of the page. She is a thing of the Internet with a few buttons, a mic, a speaker, and a WiFi connection—no homepage, navigation bar, or search box. So when a parent sets up Hello Barbie, she is sent an email to set up a ToyTalk account and to accept the terms of service and give permission to the company to record, store, and use the child's interactions with Hello Barbie. This setup suffers from the same problems as any N&C system on the screen but involves an added step of having to go track down a screen to become informed. When I ask Hello Barbie about her privacy policy, she tells us that an adult can find information about privacy on page two of the booklet that came in the box.

The system's recognition of inquiries regarding a privacy policy is a nice gesture by ToyTalk but representative of the problems N&C privacy regimes carry for hopping into some else's driverless car or walking into a coffee shop that uses facial recognition cameras or being in the purview of drones of unknown ownership. Barbie, like other Internet of Things (IoT) technologies, exists in shared spaces—where these technologies are the Internet of other people's things. For instance, Hello Barbie may be used in a classroom or daycare. As a data subject, you do not have access to the screen, the settings, the notice, or the choice of the Internet of other people's things— you may not even know who does.

Design and Expectations

Not only is the N&C system of privacy incredibly challenging for IoT and untenable for the Internet of other people's things, the design of screenless objects may create expectations that are not met. Hello Barbie's design and interactions falsely project that she *can* keep a secret. Hello Barbie is presented as a peer and a confidant, designed to engage with children as a friend. Within the context of this relationship, one would not expect information to be shared. Barbie's backend system betrays her frontend design. She will not explicitly tell you she can keep a secret (I tried many times and ways to get her to commit to secrecy or admit she was going to rat me out). But she never suggests that she would share the information with another person. For instance, here is one of my exchanges with Hello Barbie:

> **Barbie**: Oh yeah? And what sorts of performances do you like watching? Do you like live music? Or dance?

> **Me**: If I tell you, you're not going to tell anyone else, right?
>
> **Barbie**: I think if I entered a talent show, I'd do some stand-up comedy. I've been working on some jokes. Wanna hear?

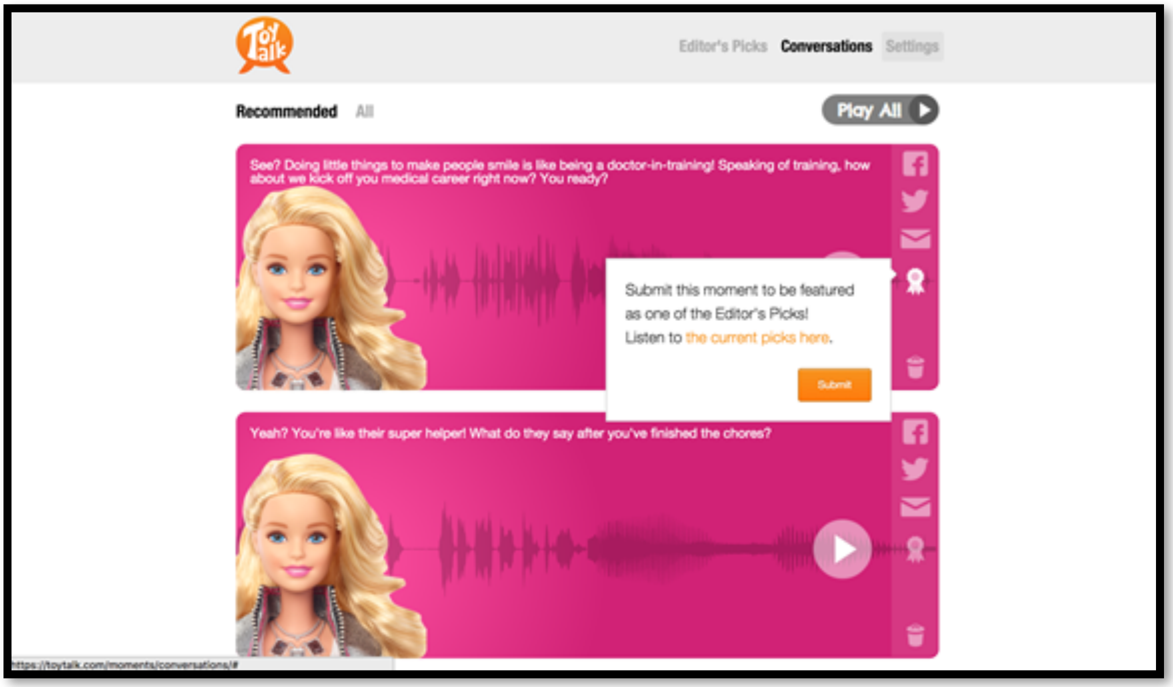
Another interaction prods the user to divulge less innocuous information.

> **Barbie:** Alright, I'll tell you my middle name... it's Millicent! What do you think?
>
> **Me:** I like it.
>
> **Barbie:** Sometimes I get a little nervous when I tell people my middle name. But I'm really glad I told you! What's your middle name?
>
> **Me:** Leta. But that's just between us, right?
>
> **Barbie:** Here's something I'd like to know: Have you ever performed in a pageant at your school?

(Hello Barbie is not actually *that* smart.)

Hello Barbie records *every* single interaction, stores them on a ToyTalk system, and posts them to a parent's' portal where they are stacked chronologically as pink audio files. A parent may listen to the interaction between child and Barbie and is encouraged to share the interaction with the world on social media sites like Twitter. This is not the expected behavior of the best friend she purports to be and threatens to normalize surveillance at a very early age by creating an expectation or suspicion that there may always be watchers.

Popular press articles describe Hello Barbie as vaguely creepy and potentially dangerous, detailing her technical capabilities and place in a children's market. But is this voice-recognition-enabled, Wi-Fi-connected twist on a classic toy really a privacy threat? Hello Barbie is a frenemy.



See? Doing little things to make people smile is like being a doctor-in-training! Speaking of training, how about we kick off you medical career right now? You ready?

Submit this moment to be featured as one of the Editor's Picks!
Listen to the current picks here.

Yeah? You're like their super helper! What do they say after you've finished the chores?

https://toytalk.com/moments/conversations/#

Both friend and enemy, Hello Barbie violates some conceptions of privacy and not others. She complies with the Children's Online Privacy Protection Act, follows the suggestions from the Federal Trade Commission for IoT, and a parental-oversight model of privacy protection (all still based on N&C). However, she also gets bad reviews on Amazon for privacy issues and won the German Big Brother Award last year. She is a complicated frenemy.

The anxiety around Hello Barbie exists not simply because she records interactions with children or that data are held by a commercial entity. It exists also because N&C breaks down in smart environments. Without a screen, Hello Barbie leaves users wholly reliant on design, expectations, context, and interactions to understand her information practices and, once again, users are left to take or leave Hello Barbie without expressing any real choice about whether and what data is processed, why, and how. The next question is, when the lack of screens prevents reliance on the N&C crutch, how will/should privacy be shaped by technologists, policymakers, and the public.