05.16

PinG

Privacy in Germany

Datenschutz und Compliance

4. Jahrgang
September 2016
Seiten 165–204

www.PinGdigital.de

ESV ERICH SCHMIDT

Dolls and Artificial Intelligence: Can they keep a child's secret?

Paulo Brancher

Paulo Brancher is a Partner at Azevedo Sette Advogados (São Paulo, Brazil) and a Professor of Business Law at the Law School of São Paulo Catholic University (PUC/SP), Brazil. He holds a PhD and is a candidate to be full professor ("Livre Docente") at the same University. .

I. Introduction

Once upon a time children talked to their toys and answers were only heard in their imagination. Later on toys were able to reproduce recorded messages and answers were not only limited but also depended upon the push of a button by the child. Suddenly, developments in technology, with its magic of bits and bytes, granted power to toys, the so called "artificial intelligence". And playing with dolls was never the same again ...

Indeed, we witness technology revolution in many fronts and that involving toys is only one of many examples of technology inclusion in all moments of our lives. If in the past children communication with their toys was a reflection of life lived and interaction with their parents, brothers and friends, currently we begun to experience a completely different reality. The window to the outside world opens earlier and earlier, and toys are taking a leading role.

In the movie Toy Story, toys talked to each other when their owner left the room. That image made many kids stalk their own toys to see if they were planning something in their absence. Twenty years later, toys are starting to talk not to each other, but to kids. Using the same technology as Siri, Hello Barbie, My Friend Cayla and Dino are just the beginning of a new generation of toys that are as connected to the internet as any smartphone or tablet we have all been using and upgrading over the last decade. They use voice recognition, Wi-Fi connection, and database to respond to kids' questions, play games, and even remember things they were told.

In turn, this whole new world brings legal issues. For example, connected toys or devices used by children may be susceptible to hacking and may compromise their owners' privacy. It also creates ethical concerns since parents are deciding how much privacy their children should give up before they even know what privacy is.

The purpose of this article is to show how some toys recently brought to market have extraordinary capacity to interact with children in a way only imaginable in sci-fi movies a while ago. As a result, we shall address legal aspects arising from such interaction, including protection of personal information and risks inherent to lack of security against attacks so typical to virtual environment. Likewise, we shall address some ethical issues involving children's early contact with machines employing artificial intelligence and later review applicable laws on the matter with a view towards establishing whether Governments are ready to deal with this kind of challenge regarding early exposure of children to the virtual world.

II. Marvelous toys ...

Hello Barbie[1] is a doll equipped with an embedded microphone, voice recognition software that enables interaction with children employing artificial intelligence. Barbie is able to connect to an user's Wi-Fi network through a free smartphone app. When its belt buckle is held down, everything the child says is transmitted to cloud servers where it will be stored and reviewed by ToyTalk, Mattel's technology partner. By talking to its owner, the doll is able to create a tailor made database, enabling a more precise interaction with the child. It wouldn't be exaggerated to consider that one of the targets of the doll is to be considered a real friend that can talk about anything.

My Friend Cayla[2] is a doll that requires download of an app called Violet. It has Bluetooth connection that enables the owner to make phone calls. Cayla can talk and interact, play games, share photos and read stories. When talking to a child, Cayla looks for answers to questions in known Internet sources such as Google Search, Wikipedia and Weather Underground. It has 1,5 thousand words in a bad-list to limit conversations in "adult talk" subjects (such as religion, politics and sexuality). In these cases, Cayla encourages the child to go ask a parent or teacher.

Dino[3] was developed by a company named Elemental Path under a project called CogniToys. This tiny plastic dinosaur uses an IBM Watson question answering (QA) computing system that IBM built to apply advanced natural language processing, information retrieval, knowledge representation, automated reasoning and machine learning technologies to the field of open domain question answering.

The key difference between QA technology and document search is that document search takes a keyword query and returns a list of documents, ranked in order of relevance to the query (often based on popularity and page ranking), while QA technology takes a question in natural language, seeks to understand it in much greater detail, and returns a precise answer to the question. This is different from Apple's Siri, which relies on a variety of partners such as Google, Yelp and Wikipedia and has pre-programmed answers to make it seem more conversational and human.

Dino connects to a Watson cloud computing service via the internet. Parents connect the toy to a home Wi-Fi network and then they enter some details about their child on the corresponding app, including age, grade level, favorite color, sport, or food. This helps the toy to interact with the child. But using Watson, it can also evaluate a child's ability and skill level on its own. Dino takes this type of information into account to determine the complexity of its answers (a question such as "How far is the moon?" can be answered "very, very far away" or "238,855 miles (384,400 km) away").

But not only toys are taking the place of adults in talking to children. ToyTalk,[4] Mattel's technology partner, has a number of apps that intended to interact with children on a Q&A basis. In "Speakalegend" children can talk with mythical creatures. In "Speakazoo", they can have a chat with the animals they like the most. "Speak or Treat" is an interactive game where children talk to vampires and other horrifying creatures to understand how to play and how to win the game. And this is only the beginning of this journey ...

III. Privacy issues

All this innovation comes, as usual, with a simple and typical question, but with very complex and unsatisfactory answers: how is my child protected from Internet exposure? The first aspect to consider is how privacy is controlled by parents and how these toys can assure that children's data is not used for unauthorized activities.

All apps have privacy policies where it is possible to understand the way data is collected and used. As we can see from their respective privacy policies, standard clauses are used when parents accept to use the software on behalf of their children. In Hello Barbie, parents accept their children's voice can be recorded and data kept with limited purposes: "*We use Recordings only for limited purposes. We may also use, store, process, convert, transcribe, analyze or review Recordings (along with text and transcriptions derived from the 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. We do not use Recordings or their content, including any personal information that may be captured therein, to contact children or to advertise to them*".[5]

My Friend Cayla is very honest when it comes to its limitation on guaranteeing Internet security: "*We will undertake internal reviews of our data collection, storage and processing practices and security measures, including appropriate encryption and physical security measures to guard against unauthorized access to systems where we store personal information. Please remember however that unfortunately no method of transmission over the Internet, or method of electronic storage, is 100% secure. Therefore, we cannot guarantee its absolute security*".[6]

And Dino's data collection methods may not be as limited as we may think: "*We may disclose to third parties, certain Play Data from or Usage Data regarding the Site and Offerings. However, in such cases, you and your child's Play Data and Usage Data is aggregated with the Play Data and Usage Data of others and does not identify you or your child individually. From time to time, we may establish a business relationship with other businesses whom we believe trustworthy and who have confirmed that their privacy practices are consistent with ours*".[7]

But the real world is not so compliant with privacy policies. In accordance with specialized news,[8] flaws have been identified in My Friend Cayla software. Essentially, anyone with the know-how can hack into Cayla's system to modify commands and change

1 More information available at: http://hellobarbiefaq.mattel.com/about-hello-barbie/ (Last accessed on May 20, 2016).
2 More information available at: http://www.myfriendcayla.com/#!us/c5ja (Last accessed on May 20, 2016).
3 More information available at: https://elementalpath.zendesk.com/hc/en-us (Last accessed on May 20, 2016).
4 More information available at: https://www.toytalk.com/ (Last accessed on May 20, 2016).
5 Privacy Policy available at: https://www.toytalk.com/legal/privacy/ (Last accessed on May 21, 2016).
6 Privacy Policy available at: http://www.myfriendcayla.com/#!privacy-policy/cus (Last accessed on May 21, 2016).
7 Privacy Policy available at: https://cognitoys.com/privacy (Last accessed on May 21, 2016).
8 My Friend Cayla doll can be HACKED, warns expert – watch kids' toy quote 50 Shades and Hannibal, available at: http://www.mirror.co.uk/news/technology-science/technology/friend-cayla-doll-can-hacked-5110112

her responses to questions, making her say anything they want – including words on her 1500-strong "bad" list.

The Vivid Toy Group, entity behind the creation on My Friend Cayla, commented in the same news that the doll is designed for creative play and has numerous levels of security in place to ensure that children are safe when using the doll and the associated app. But when the child asks Violeta (Cayla's app) a question, this information request is stored by Nuance Communication (for Apple-based users) or Google (for Android/Google based users). Therefore, messages are not encrypted, which leads to lack of security.

As mentioned above, ToyTalk's privacy policy also doesn't inspire much security. As Mattel's partner in the development of Hello Barbie, it states that recordings of a child's voice can be used for data analysis and can be shared with third parties, though it points out these are service providers, like Microsoft, who support the toys' speech recognition feature. Parents can use a companion smartphone app to listen to recordings and even receive a notification when new recordings are available. Parents can also share or delete recordings. Security researchers have also revealed flaws in the network that Hello Barbie's creators use to upload a child's recorded conversation to the cloud, where phrases are processed using artificial intelligence so that Barbie's response simulates an actual conversation.

Security research firm Bluebox understands that this potential weakness may let hackers listen to the recordings. Additionally, given the way Hello Barbie connects to Wi-Fi, a hacker can trick the doll into connecting to a rogue hotspot. That may allow a hacker to hear what the children say, and possibly even send Barbie new things to say. Parents might end up trying to explain to their children why Barbie is swearing or making threats.[9]

The creators of Dino stated that the connection to Watson is not directly made due to privacy reasons. The toy is connected to an Elemental Path proprietary platform, which then is connected to Watson for QA statements. All stories, jokes, educational exercises and personalized experiences are located in the platform. Watson is used as the logical left-brain to Elemental Path's creative right brain.[10]

While Dino was still in pre-sale, IBM's general privacy policy didn't seem to create a safe environment: "*The information you provide to IBM, as well as the information we have collected about you indirectly, may be used by IBM for marketing purposes. Before we do so, however, we will offer you the opportunity to choose whether or not to have your information used in this way. You may at any time choose not to receive marketing materials from us by following the unsubscribe instructions included in each e-mail you may receive, by indicating so when we call you, or by contacting us directly*".[11]

All companies involved claim they have taken numerous steps to ensure their toys meet security and safety protocols. However, on November 2015 there was a scandal involving the names, addresses and personal details of nearly 500,000 British families and their children that were obtained by hackers in a cyber-attack on VTech's website – a website that is used for downloading children's games, books and other educational content. VTech admitted that a database of names and addresses containing up to five million accounts worldwide had been breached.

It is inevitable to conclude that without a strong level of protection over flow of data, all information can be hacked. A high level of protection is expected in military, political and business communication, but is not supposed to be commercially reasonable to be used in toys. More than a legal issue, this also raises concerns on parental role and ethical impacts on playing with toys that intend to replace human interaction.

IV. Parental control and ethical issues

We all know what happens if kids are left alone. Parental control is not the ubiquitous power that avoids tragedies, but it helps a lot to control damages. The problem with parental control for toys employing artificial intelligence is not necessarily the ability of the parents to have access to what their children are doing. It is the fact that they are the ones allowing their kids to have access to a world that does not necessarily play by the rules. In a way, they play a double controlling role: what their children do and what the toy itself is able to make. This seems to be somehow unbalanced.

Hello Barbie enables parents to have full access to the content exchanged between the toy and the child: "*ToyTalk uses parental email in order to obtain parental consent for your children's use of the Services and to create a parent account, which allows you to access the Parental Settings section of the ToyTalk website. For your convenience, ToyTalk offers a unified parent account so if your children also use or want to use other ToyTalk children's products or services, you may use the same account to manage your children's use of all such products or services. (...)*".[12] As a result, parents can use the app to listen to recordings and to receive notifications when new recordings are available. They can also share or delete recordings.

So, parents are responsible for providing its children with the toy, reading the content and accept privacy policies (and their correspondent limitations), controlling the level of interaction and content of the dialogue between the children and the toy, knowing, however, that Internet communications are not 100% safe.

In addition to that, it is fair to say that parents are deciding, in the very early stages of life, whether their children will not have privacy. In other words: sharing private information will be an inner characteristic to anyone.

In another field, the Campaign for a Commercial Free Childhood (CCFC), which is a group of privacy advocates, tried to stop the release of Hello Barbie in the late 2015. CCFC aimed to support parents efforts to "*raise healthy families by limiting commercial access to children and ending the exploitive practice of child-targeted marketing*".[13] As seen in the Privacy Policy applicable to Hello Barbie, there is nothing within the guidelines that would prevent the company from using the information gleaned by the doll to market additional products to children.

9 Why you should say 'goodbye' to Hello Barbie, available at: http://www.usatoday.com/story/tech/columnist/komando/2015/12/22/hello-barbie-hack-kim-komando/77636502/ (Last accessed on May 23, 2016).

10 This Toy Dinosaur Uses IBM's Watson as a Brain, available at: http://www.wired.com/2015/08/toy-dinosaur-uses-ibms-watson-brain/ (Last accessed on May 25, 2016).

11 Privacy Policy available at: http://www.ibm.com/privacy/details/us/en/ (Last accessed on March 25, 2016).

12 Privacy Policy available at: https://www.toytalk.com/legal/privacy/ (Last accessed on May 21, 2016).

13 The dark side of buying your children smart toys: Expert warns Hello Barbie can be hacked, as VTech suffers major data breach, available at: http:/www.dailymail.co.uk/sciencetech/article-3340789/The-dark-buying-children-smart-toys-Expert-warns-Hello-Barbie-hacked-VTech-suffers-major-data-breach.html#ixzz41CltyXhh (Last accessed on March 25, 2016).

It is a world consensus that children are more vulnerable when it comes to data collecting and processing, and that the consequences of an overwhelming marketing campaign towards children are not yet clear, but are most likely bad. Companies behind the new smart toys try to ensure that the extracted data derived from recordings does not contain any audio files or real voices – they are collected for research and development purposes. But if no method provides complete certainty that the operator has reached and obtained consent from a parent, is it possible to be sure that all data collected is anonymized before being shared or stored?

An interesting point that has not yet been brought up is the liberty given to parents to hear their children's recordings, and the possibility to share them with third parties. If the company is subjected to data anonymization and cannot use any of the recordings for marketing processes, why should parents be allowed so much liberty over their children's private information? It is most certainly an in-house privacy breach covered by educational purposes.

Moreover, would this new generation of toys be a tool for education or simply a detour away from socialization? Hello Barbie and My Friend Cayla, as the name itself says, try to seem like a real friend, with their own robotic voices and girly conversation topics. Dino, in turn, as a dinosaur, stands a bit farther from the friend zone. Because it cannot replace a pet or a person, it has a lower chance of being identified with the real world. Technology is unstoppable and it can, and should, be used in our favor. Children learn from computers every day. If it comes in the form of a Dino or a doll, that should encourage them even more to learn and grow. But the consequences should be the same as any other toy – the things children say to these toys should not be used for marketing purposes and parents should not be able to control it if they are not part of the conversation.

Other ethical questions are inevitable: Should children's private conversations be shared with corporations or strangers? It is a fact that children have confidence in dolls and reveal intimate details about their lives, but new dolls won't keep those secrets. Is the doll a "friend", or a marketer? There may be no direct ads, but shouldn't children be free from exposure to indirect messages? For example, should children know about toys of other brands? What brand is going to be on the top of results or interactions?

We all know that dolls have always talked and interacted with children through the power of their imagination. Use of their own initiative and creativity to hold conversations with toys was always key for them to find their own personality, build their relationships and reach sound development.

And by having the whole internet and Watson to answer to children's questions, parents will probably play a second role in terms of trustful information. In this regard, would the next generations be tolerant with the real world and with the fact that human beings fail and do not have responses for everything?

Maybe the bits and bytes evolution may turn robots into genuine listeners for real needs of human beings. But playing a Q&A game is totally different from living a relationship with emotional interaction.

As it is clear from the above thoughts, dolls with artificial intelligence do not only raise legal issues. Parents' consent is necessary and is good, but it is also the opening of an unknown and sometimes very dangerous world.

V. Where are the regulators?

Although it is not fair to say that governments are not paying attention to this matter, the existing national and international laws are very limited in scope, focusing on parental consent as a panacea for all problems that may arise with this interaction.

The US COPPA – Children's Online Privacy Protection Act – protects privacy of children under the age of 13. Among other things, this law requires operators to give notice to parents and to obtain verifiable parental consent prior to collecting, using, or disclosing personal information from children under 13 years of age. Any method to obtain verifiable parental consent must be reasonably calculated in light of available technology to ensure that the person providing consent is the child's parent. The Rule sets forth a non-exhaustive list of methods that meet the standard of verifiable parental consent. Specifically, paragraph (b)(2) states that methods to obtain verifiable parental consent that satisfy the requirements of the paragraph include: providing a consent form to be signed by the parent and returned to the operator by postal mail or facsimile; requiring a parent to use a credit card in connection with a transaction; having a parent call a toll-free telephone number staffed by trained personnel; using a digital certificate that uses public key technology; and using email accompanied by a PIN or password obtained through one of the verification methods listed in the paragraph.

In Europe, Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR) – supposed to be effective in Member States by 2017/2018 – states in its foreword (38): "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counseling services offered directly to a child*".

Regarding children's data, foreword 75(a) notes that children are "*vulnerable individuals*" and that processing children's data is an activity that may result in risks "*of varying likelihood and severity*".

Directive 95/46/EC (the "Data Protection Directive") did not contain any specific restrictions on processing children's data. GDPR's major provision in relation to children is Article 8, which requires parental consent to be obtained for information society services offered directly to a child under the age of 16 – although this ceiling can be set as low as 13 by a Member State, and only applies where processing would take place based on the child's consent. The controller is also required, under Article 8(2) of the GDPR, to make "*reasonable efforts*" to verify that consent has been given or authorized by the holder of parental responsibility in light of available technology.

Foreword (38) notes that the use of child data in marketing, for profiling purposes or in connection with the supply of services to children are areas of concern requiring specific protection under the GDPR.

Although this doesn't seem to be much, COPPA and GDPR provide parents with more control over use of online information. But as we see, this is not a desired answer or regulation able to face the challenges imposed by toys with technological resources and artificial intelligence.

VI. Conclusion

Human beings and technological evolution are inseparable. So none of the issues brought up in this article mean to criticize or even demonize the fact that children now may interact with devices that are more than toys. They are, at the end of the day, a new and funny way for children to discover the world and help them to develop their skills and personality. This has always been the role played by toys.

But given the resources such toys have and the lack of security in internet connection and also the fact that parents may not be aware of the risks involving privacy issues and the exposure their kids may have in interacting with such toys, we understand that regulators should be more proactive to strengthen the rules regarding exposure of children in the internet. Review on such regulation should cover at least the following aspects: (a) privacy for children is not the same as privacy for adults: parents should be more educated as to what they are consenting to when they give such toys to their kids; (b) toys should be certified with minimum level of safe communication, in order to make hackers' lives a bit more difficult when trying to break communications between children and their dolls; (c) marketing rules regarding such toys should be reviewed so that children should not be exposed to specific products or brands when interacting with them; also, toys should be neutral when providing any type of information related to competitors.

We hope that this new incredible era brings as many good memories for children as we have with those very simple toys we use to play when we were kids.