Evaluation of the perception of Brazilians about smart toys and children's privacy

Fernanda Amancio*, Marcelo Fantinato*, Patrick Hung†, Gustavo Coutinho‡ and Jorge Roa§
*University of Sao Paulo, Sao Paulo, Brazil 03828–000
Email: {f.amancio, m.fantinato}@usp.br
†University of Ontario Institute of Technology, Oshawa, Canada L1H 7K4
Email: patrick.hung@uoit.ca
‡Federal Institute of Ceara, Jaguaribe, Brazil 63475–000
Email: gustavo.coutinho@ifce.edu.br
§National Technological University, Sarmiento, Argentina C1041AAJ
Email: jroa@frsf.utn.edu.ar

***Abstract*—The concept of children's toys has undergone many changes over the years, evolving from simple physical products to toys that add elements of the digital world using software and hardware components. This evolution has raised concerns about potential child privacy issues regarding the use of smart toys. A smart toy consists of a physical component connected to a computer system with online services to enhance the functionality of a traditional toy. This type of toy is still not widely known in Brazil and hence the opinion of Brazilian consumers regarding the acceptance of this technology when it is widespread in this country is not known yet. This paper aims to present the results of an evaluation about the perception of potential Brazilian consumers about issues involving children's privacy with the use of smart toys and whether this technology would be accepted when available in the Brazilian toy market. Semi-structured interviews were conducted with 14 participants producing data that were analyzed through the content analysis technique. The results showed concern on the part of parents when their children are connected to the internet. Moreover, parental control in smart toys would be well accepted by these potential consumers.**

I. Introduction

During the 20th century, technologies capable of offering more interactivity to traditional toys were developed, which attracted great attention from its target audience. This movement led to the creation of electronic toys. This type of toy is characterized by the union of the traditional models with electronic components. Companies manufacturing these new products have achieved billionaire returns due to the large acceptance and popularization of these devices [1]. An example of an electronic toy is the teddy bear *Teddy Ruxpin* [2]. This toy reproduces the contents of a cassette tape embedded in its back and moves its mouth and eyes, simulating the reading of stories for children.

The evolution of the toys did not stop with the electronic models. More recently, smart versions have emerged. Smart toys are devices that consist of a physical component connected to a computer system with on-line communication services [3]. These toys offer a more realistic experience to children, simulating, for example, natural language. Artificial intelligence techniques are usually used to achieve this type of experience [4]. As an example of this new type of toy, the doll Hello Barbie can be cited, known for being the first doll that can have a two-way conversation with children [2]. This doll uses voice recognition and makes use of cloud computing technologies to interact with children, sending dialogues to a cloud service, and returning appropriate responses.

With the emergence of these clever toys, potential privacy and safety issues with children came up [5]. The Hello Barbie technology is one of the cases that has been criticized for the possible negative effects on some aspects of privacy and security. As an example, the following scenario would be possible: a child might bring a smart toy to the dining table; this device could then capture sensitive information from any conversations by any party at the table to a third party without the prior consent of those responsible for the child [5]. Even if there are well-defined privacy terms for a particular smart toy, the communication of the toy with other devices or the internet may still be intercepted by unauthorized persons and the information transmitted may be misappropriated.

The availability of smart toys in developed countries has become increasingly relevant, stimulating discussion on children's privacy issues [6]. On the other hand, in developing countries, smart toys are not widespread yet. The language support may partly explain why this new type of toy is still not available in the Brazilian market, for example. Since smart toys are a recent technology, they are mostly available only in the English language [7]. Considering the need for expansion of their manufacturers, this scenario should change in a few years. In a possible expansion, the Portuguese language should be one of the first to be considered, since Brazil is a large world market for this type of technology [8].

In this scenario, the opinion of the Brazilian population about the use of smart toys and their children's privacy issues that could potentially harm their users is not yet known. To investigate this scenario, a study was carried out on the perception of potential Brazilian consumers about privacy issues involving smart toys in order to see if it would be accepted when available in the Brazilian market. This paper aims to present the results of the evaluation conducted through semi-structured interviews with 14 participants. The data col-

lected were analyzed through the content analysis technique. The interview was conducted in order to obtain participants' thinking patterns regarding privacy issues when it comes to children in the use of technologies and whether smart toys would be accepted by these potential consumers.

The remainder of this paper is organized as follows: Section II presents the theoretical background with the basic concepts related to the topics addressed in this paper; Section III presents the works related to the study addressed here; Section IV presents the research method adopted in the study; Section V presents the plan elaborated for application of the chosen method; Section VI presents the results of the interview conducted; Section VII presents a discussion of the results; and, finally, Section VIII presents the conclusion of this paper.

II. Background

This section presents basic concepts covered in this article, including smart toys, security, privacy and child privacy, and privacy in the use of smart toys.

A. Smart Toys

A smart toy is defined as a device consisting of a physical component associated with distinct types of sensors, containing a relevant level of computing power and communication capabilities with the internet or other mobile devices [9]. In this context, a smart toy can be considered as a device on the internet of Things (IoT) environment.

Figure 1 presents two examples of smart toys. Mattel's Hello Barbie is a doll that talks to the child using phrases and answers from a fixed, pre-determined database that contains around 8,000 phrases. CogniToys Dino is a dinosaur that uses a cognitive system to answer questions using phrases and answers not predetermined through IBM Watson system. Both toys connect to the internet via Wi-Fi and have an associated smartphone application.

Fig. 1. Examples of smart toys: (a) Hello Barbie, (b) CogniToys Dino

The smartphone applications associated with these two toys can provide parents or guardians with control of the children's activities. In the case of CogniToys Dino, this only includes the child's bedtime. For Hello Barbie, parents can use the associated website to listen to and share recordings of their children's conversations, as illustrated in Figure 2 [7].

Table I presents a comparison between traditional toys, electronic toys, and smart toys, illustrating how toy computing

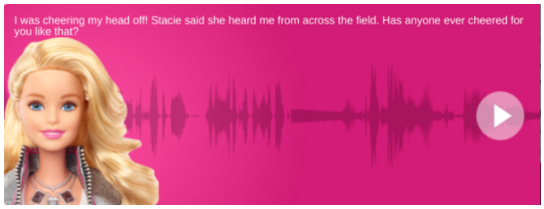

Fig. 2. Screenshot of the conversation panel between a child and Hello Barbie.

has evolved into a new paradigm that inspires exclusive privacy concerns for children [10]. Traditional toys are fully self-contained and do not have processing or networking capabilities to communicate with any other device. While a child is playing with a traditional toy, their parents do not have to worry at any time, because the toy will not be able to store any personal data of the child. With the introduction of electronic toys with embedded systems, these toys present sensory capabilities and the ability to collect and store data entered from user interactions. This data is limited and used only for interaction and is generally discarded immediately. While an electronic toy has the potential to collect and store user data, it operates on a fully autonomous platform such as a Trusted Computing Base (TCB). An electronic toy has limited or no network capability. In this way, privacy concerns are limited to nonexistent in this architecture. On the other hand, smart toys by their nature inherit the privacy concerns associated with mobile devices and the Bring Your Own Device (BYOD) policy [11]. When the smart toy technology allocates computing power to a mobile device, it stays out of the TCB and the device becomes untrustable. A mobile device also can collect a wide variety of context information about the user, including their location data. The smart toy architecture allows and usually requires information to be shared with services and other users.

One of the most important concerns when it comes to privacy in the use of smart toys, compared to traditional and electronic toys, is the network capability that allows sharing information on a network [6]. A mobile service can connect through a network to many other entities, including other mobile services, web services, servers, devices, and other users (as illustrated in Figure 3). In fact, the ability of a mobile service to connect and communicate with an extensive and possibly unknown number of external entities makes the issue of data sharing a major concern.

B. Children's Privacy in the Use of Smart Toys

Security is the protection offered to preserve the integrity, availability, and confidentiality of the resources of a computer information system (including hardware, software, firmware, information/data and telecommunication devices) [13]. In this context, smart toys should keep, above all, the confidentiality of their users' information. That is, if a child, for example, provides personal information to the device, intentionally or otherwise, the smart toy should ensure that such private or

TABLE I
COMPARISON AMONG TYPES OF TOYS (ADAPTED FROM RAFFERTY, KROESE AND HUNG [10])

Feature	Traditional toy	Electronic toy	Smart toy
Interaction medium	– Physical – Mechanical	– Physical (buttons) – Sensors (e.g., light, motion)	– Physical (touch) – Visual (camera) – Auditory (microphone) – Sensors (GPS, motion etc.) – Network (wireless interface)
Data collection	– None	– Limited	– High (pervasive)
Data sharing	– None	– Limited or none	– Many recipients
Potential to collect location data	– None	– Maybe	– Yes
Processing capabilities	– None	– Limited	– Advanced
Networking capabilities	– None	– Limited or none	– Communicates with other devices and services – Wi-Fi, Bluetooth, NFC, RFID, USB
Data storage	– None	– Limited to device	– On device (flash memory, SD card) – External to device (cloud, database, server)
Architecture and TCB	– Autonomous – Trustable	– Autonomous – Trustable	– BYOD (untrustable device)
Platform	– Closed	– Closed	– Open

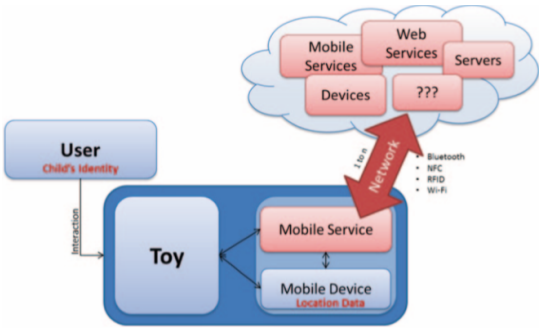

Fig. 3. Architecture of communications and threats of smart toys [12].

confidential data will not be available or will be disclosed to unauthorized persons.

Privacy is defined as the right of an individual to determine how, when and to what extent information about themselves is disclosed to another person or to an organization [14]. With increasing interconnectivity and the volume of personal information collected and stored, users have become increasingly aware of the size of access that companies, government agencies, and even other users have to their personal information and private details of their day-to-day life [13]. As a result, there is a growing concern about the privacy of information in the digital world.

There are several reasons to consider children as users most susceptible to invasion of privacy [15]. These users do not have the ability to discern when the privacy of certain actions needs to be considered as well as they do not understand the relevance of shared information. This group of users needs specific social and legal protections because they are considered less able to protect themselves.

The association of the concepts of children's privacy and smart toys occurs naturally, seeing that there is a growing exposure of children to this new type of technology. When this group of users interacts with smart toys, sensitive information can be shared. As a result, data sharing becomes a relevant concern given the ability of smart toys to connect and communicate with an extensive and possibly unknown number of external entities [12].

The process described in Figure 3, which shows the user's links to the toy, and the services contained in these toys, along with their ability to transmit this data, is considered a threat architecture that can affect privacy when a child interacts with a smart toy. These threats can be summarized in three points: child's identity, location data, and network communication. Location data sharing is one of the sensitive content for children, making it easier to access when a malicious person wants to collect such data.

Data that can be collected from a child is typically used for online marketing [15]. Besides this, location data allows tracing of user behavior that is not publicly available. In addition, when physical location data is being shared with other users, it is important to consider the physical safety of a child in relation to child predators. These predators can, for example, locate children based on their GPS location [7].

Although privacy-related issues are common, they are relatively new to the domain of smart toys because of the child's user base and the physical toy component. These toys separate themselves from other categories and identify themselves as a distinct area from the rest for privacy concerns [12]. There are a few strategies created for security and privacy of online services. These strategies include the Open Web Application Security Project (OWASP[1]) and the STRIDE threat model[2] [12]. These strategies are security-oriented, with little or no focus on privacy, and are not specifically focused on smart toys. In addition to these privacy and security strategies that are not comprehensive, laws that address children's privacy in the use of smart toys are poorly known.

Some countries have laws and regulations that address the individual privacy of their citizens. In particular, the United States of America enacted the Children's Online Privacy Protection Act (COPPA), in 1998, to impose restrictions on the collection of data for children under 13 years old [15]. This is

[1]https://www.owasp.org

[2]https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

one of the reasons why many online services (e.g., Facebook) have 13 years old as the minimum age for creating an account on their services [16]. According to the age considered by COPPA, a child has no sense of the danger in sharing their personal data, thereby harming their privacy and making room for malicious people to collect their data [15].

III. Related Work

Table II presents three studies that conducted some type of opinion analysis with respect to smart toys. Two of them were interviews while one of them was a survey.

Jones and Meurer [2] addressed the privacy issue of children who interact specifically with Hello Barbie in the United States of America. This work has shown that the American consumer public has analyzed smart toys, more specifically Hello Barbie. According to these authors, Hello Barbie is not advanced enough to tell the user if she keeps a secret. Moreover, according to the authors, the toy tends to share with third parties and with potential networks, such as Twitter, private conversations between children and their parents. This tendency to share data has the potential to negatively impact the trust of children and parents or guardians. The authors conducted a qualitative survey, collecting data through interviews with parents and with the company ToyTalk, responsible for monitoring Hello Barbie. The following questions were asked: can Hello Barbie keep a secret? Will Hello Barbie respect your privacy when requested or will it do the opposite? How is information presented for parental and guardian supervision? For this, the participants were induced to talk to the doll, and a clear disconnection in their conversations with the doll could be observed since participants' responses were rarely understood or interpreted properly. This lack of understanding extended to conversations in which secrets were shared. Hello Barbie often asks for the trust of children and their parents but is simultaneously built to nullify relationships of trust. She is superficially designed to act as a child's best friend, but the doll records and shares all the conversations with the child's parents. Parents, on the other hand, have full control over stored chats, but their children's data has the potential to be shared with numerous third parties. The authors' conclusion is that in both cases it is clear that Hello Barbie can definitely not keep a secret.

McReynolds *et al.* [7] conducted interviews with parents of children interacting with Hello Barbie and CogniToys Dino. They investigated themes such as expectations about these toys, privacy concerns, and possible expectations of those responsible for the child. For example, they investigated whether or not it should be possible to set CogniToys Dino bedtime and when Hello Barbie should be disconnected from the internet. The authors of this paper report that children often do not know that other people can hear what was said for the toy, which can jeopardize their safety if a malicious person misuses this information. The main focus of this study was to conduct an interview with parents of children interacting with Hello Barbie or CogniToys Dino. The objective was to investigate, for example, children's expectations about this type of toy; the possible expectations of parents or guardians regarding such toys; and privacy concerns. The recruitment of the participants happened through the sharing of ads sent by email, Facebook, and word of mouth. As a result, the interviews were scheduled with nine pairs of participants. The interviews also happened with the children of the participants. The types of questions were related to the use of toys, control over the conversations, the purchase of the product, and related privacy. To analyze the interviews, a grounded theory approach was used, in which a set of themes is developed, and then these themes are grouped according to the participants' answers. The interviews were transcribed and the authors analyzed the answers of the participants according to the questions asked. Two researchers independently coded each interview while developing a codebook through an interactive discussion with the rest of the research team, then creating broader themes from the coded data. Conflicts among coders have been resolved through discussion to reach full consensus. As a result of the study, it was concluded that: many parents are surprised about the recording ability of these toys and the typically expressed privacy concerns; the children often do not realize that the toys were recording or that the recordings were accessible by the parents; and toy interaction models are not yet sophisticated enough and flexible enough to meet the expectations of children, since they are often exposed to interaction with devices that naturally listen and respond even if they are not designed as toys, such as Apple's Siri and Amazon's Alexa.

Author[3] *et al.* [17] carried out a work to particularly study Brazilian and Argentinian consumers' perceived innovativeness, risks and benefits of smart toys and their purchase intention toward such toys. The study was carried out through the application of an off-line questionnaire applied to two groups of potentials consumed, one Brazilian group and one Argentinean. Their results indicated that Brazilian consumers have better perception and evaluation of the toy and thus higher purchase intention than Argentinian consumers do. According to these authors, such difference may be explained by the cultural differences between the two countries, such as relatively low vs. high uncertainty avoidance. This empirical study showed that participants in both countries assessed the smart toy as equally innovative and risky. This demonstrates the data privacy concerns in Brazil and Argentina. Further, the research also demonstrated how perceived innovativeness of a product may have either positive or negative impact on product evaluation and purchase intention in diverse cultures. The authors also provided their recommendations for smart toys manufacturers to address these issues for the future products. The results of the study suggested that smart toy manufacturers can emphasize the toy's innovativeness to enhance consumer acceptance level in relatively low uncertainty avoidance cultures and relatively high-power distance countries such as Brazil. Whereas, in cultures with relatively higher uncertainty avoidance and relatively low power distance such as Argentina,

[3]Anonymous due to the double-blind review process.

TABLE II
STUDIES WITH OPINION ANALYSIS ON SMART TOYS

Reference	Authors	Year	Technical procedure	Approach	Collection technique	Analysis technique	Number of participants
[2]	Jones and Meurer	2016	–	Qualitative	Interview	Content analysis	Not informed
[7]	McReynolds *et al.*	2017	Grounded Theory	Qualitative	Interview	Content analysis	27 participants
[17]	Author[a] *et al.*	2018	–	Quantitative	Survey	ANOVA	118 participants

[a] Anonymous due to double-blind review process.

smart toy manufacturers can reduce consumers' perceived innovativeness by associating the conversational technology with existing technology such as voice recognition mobile apps to enhance consumers' evaluation of the toy.

Similar to the three papers cited, the present study seeks the perception of potential consumers regarding privacy focused on smart toys. In spite of this, the two studies that also carried out interviews like the one that this work realized did it in the specific context of the United States of America, a developed country that already has access to this type of technology. On the other hand, the other work that carried out the study also in Brazil and Argentina, developing countries, did through another technical procedure, that is, an offline questionnaire applied mainly to students, which does not represent exactly the profile of consumers for this type of smart toy. As a summary, this work seeks to obtain the qualitative opinion directly from Brazilian consumers, as representatives of developing countries, through direct interviews with this type of individual.

IV. RESEARCH METHOD

This section summarizes the research method applied to conduct this study. As a technical procedure, a semi-structured interview was used. An interview is a type of research that seeks to collect information directly from an interest group with respect to the data one wants to obtain [18]. In order to reach the result sought in this study, the semi-structured interview was applied to an audience composed of parents from gestation to parents with children up to 19 years old.

This profile of interviewees was chosen because parents are beginning to worry about the privacy and safety of their children since pregnancy. Moreover, even after the children move from the infancy to the adolescence phase, parents may still remember how was their concerns related to these aspects. Considering that, according to the World Health Organization (WHO), a person is a teenager from 10 to 19 years old [19], the age limit of the children for a parent to be considered for the interviews was 19 years old.

A semi-structured interview is a research tool used to collect data in oral or written form, which should occur in an interaction between the researcher and the interviewees [20]. Because it is semi-structured, the interview script may have some closed questions, where the interviewee may offer a short answer, such as yes or no, and may also contain open-ended questions, where interviewees should report more about their opinions, but without running away of the proposed theme.

The application of the interview in this study was performed in a virtual way, using tools capable of maintaining an interaction with video, including Skype, Hangouts, and Facebook. The virtual medium was chosen so that it was possible to collect opinions from people from different regions. For the data analysis, the content analysis method was used, more specifically the categorical analysis of the thematic type. This method is characterized by dismembering the text in units (or categories), presenting as advantage fastness and effectiveness [21]. It was chosen for helping to organize the opinions of the respondents in a clear way in order to reach the categories that represent their opinions, reaching conclusions for the purpose of the study.

The research method is characterized as follows [18]:

- **Genre "empirical"**: it is an empirical research since the results of the data collection should be generated considering only the experiences of pregnant women and parents of children aged from 0 to 19 years regarding their own perceptions about privacy issues when it comes to their children (or future children) using technologies. The empirical genre is based on common experience and observation, a fact that relies only on lived experiences and on the observation of things, not on theories.
- **Nature "applied":** it is an applied research since the researchers aimed to address the specific problem of children's privacy in the use of smart toys in a practical way, without aiming to broadly advance the scientific theory. The applied nature aims to generate knowledge for practical application, driven by the solution of specific problems, involving only local truths and interests.
- **Goal "descriptive":** it is a descriptive research since its objective was to present a characterization of the facts and of the phenomenon being studied, i.e., the parents' opinion on children's privacy in the use of smart toys, more than a simple exploratory analysis. However, it was not the goal of this study to present a study in depth on the reasons why a certain scenario was found, i.e., the study did not have an explicative/explanatory character; the researchers were not concerned to describe in detail why some given results were found.
- **Approach "qualitative":** it is a qualitative research since, due to the nature of the problem and the goal sought, there was no concern with numerical representativeness, but rather with the deepening of the understanding of a specific social group. Thus, the data analyzed were non-metric, with subjective characteristics. For data collection and analysis were used, respectively, semi-structured interview and content analysis.

V. Interview Plan

The purpose of conducting the interviews was to attempt to capture patterns of interviewees who are potential consumers of new technologies for children, possibly including smart toys. We sought to see if parents are concerned about privacy issues when it comes to children using technology and whether smart toys would be accepted when available in Brazil.

The script for the semi-structured interview was elaborated based on issues related to the concern with the privacy of children in the use of technologies. For this, the material studied in the bibliographic study was considered as starting point, which was improved through meetings for discussion among the researchers involved.

The questions were designed in a way to not lead the interviewees to think directly about smart toys and privacy-related issues to increase the chance of getting more natural thinking patterns from participants. In addition, by directly mentioning these terms, especially smart toys, some participants could feel embarrassed not to know them as they are not yet available in Brazil. Thus, a script with questions was assembled that relate to privacy issues that may occur in the current daily lives of parents with their children and that could lead to issues desired by this study. It was aimed to elaborate questions to be presented in a natural way, without technical terms, scientific jargons and formalisms, i.e., trying to create a chat environment. To start a conversation, characterization questions were chosen so that it could help create a conversation environment in which the interviewee felt comfortable. Subsequently, to insert the subject, a question was presented linked to the most basic and common use of current technologies (i.e., Facebook), followed by a first mention, in a still rather generic way, to possible problems associated with these technologies. Next, the subject of smartphones was introduced, to get closer to a type of technology more similar to smart toys, followed by a specific mention of the internet and its potential dangers. Then, there was an explicit mention of criminals acting in this context. Finally, the last two questions dealt with the toys that would be connected on the internet and would then bring the dangers raised in the previous question to this focus, even in cases where parents have never thought or heard of smart toys.

The script used for interviews is presented in the following:

1) Characterization questions:
   - Education?
   - Number of children?
2) Context questions:
   - Do you allow your child to use Facebook?
   - Do you think the advancement of technology has made the world more dangerous for children?
   - When did your child start using smartphones?
     - If already uses: do you think it happened at the right age?
     - If still does not use it: when do you think it should start?
   - Do you see any danger when your child is using the internet?
   - Have you ever heard of criminals who have been able to steal information on the internet to kidnap children?
   - Would you give your child a toy that could talk to him (listen and respond)?
   - Do you know if your child has any toys connected to the internet?

The sequence in which the questions are asked makes themes such as "whether the advancement of technology has made the world more dangerous" provoke parents to reflect more on privacy issues in the use of smart toys. The questions directly related to the use of toys capable of communicating with their children were left to the end so that parents were already involved in thinking about issues in which their children might be exposed when using technology. Thus, they were able to make a more critical reflection on the possibility of giving their children a toy of this nature.

Different Brazilian states were considered for the selection of the interviewees, in order to obtain perceptions of parents with different cultural experiences, taking into account the national region. In addition to the region, interviewees of different education levels were selected as a means of differentiation. Tables III, IV, V and VI present the characterization of the interviewees.

TABLE III
Frequency of Participants by Gender

Gender	Number of participants
Female	12
Male	2

TABLE IV
Frequency of Participants by Education Level

Education level	Number of participants
Incomplete high school	1
Complete high school	4
Incomplete university degree	2
Complete university degree	5
Incomplete masters degree	1
Complete masters degree	1

TABLE V
Frequency of Participants by State

State	Number of participants
Ceará	7
São Paulo	4
Bahia	2
Piauí	1

Participants who agreed to participate in the survey were invited to read a consent term explaining the research and their rights to anonymity. Only after the participants read and agreed to participate, the interview stage began. Each interview was conducted individually with each participant. The schedule was chosen according to the availability of the participants.

TABLE VI
PROFILE OF PARTICIPANTS WITH RESPECT TO THEIR CHILDREN

Participant ID	Number and age of children
1	pregnant
2	1 child (1 year old)
3	1 child (1.5 years old)
4	2 children (1.5 years old + 3.5 years old)
5	1 child (1.6 years old)
6	1 child (2 years old)
7	1 child (2.6 years old)
8	2 children (3 years old + 9 years old)
9	1 child (5 years old)
10	1 child (5 years old)
11	1 child (7 years old)
12	1 child (7 years old)
13	1 child (8 years old)
14	2 children (16 years old + 18 years old)

VI. RESULTS

The interviews took place between September and October 2017. The interviews were recorded and the time spent with each participant was in an average of ten minutes. Figure 4 presents the methodological process used, split divided into seven steps [22]. Figure 5 summarizes the results of this methodological process, including the tree of elements used through the content analysis and the number of elements obtained in each one of the seven steps, when applicable [22]. Considering the content analysis method used, all the collected text must be dismembered through seven steps until it reaches the goal of the study. For this, the collected information needs to be categorized, arriving in this way in smaller categories that represent all the content of the collection of data. Following, each step of the methodological process is described.

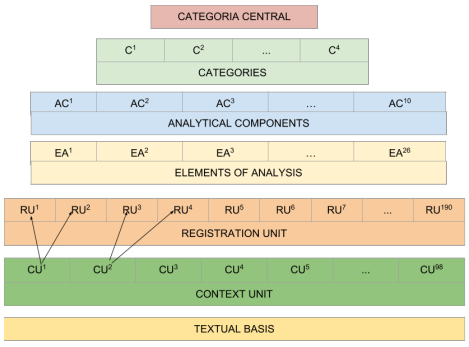

Fig. 4. Methodological process steps (Adapted from Coutinho [22])

(1) **Elaboration of the textual basis**. All the data produced by the research with the 14 participants (interviews) were transcribed and transformed into written text, which began to play the basic role for the accomplishment of the codification. The coding is the transformation of raw data by clipping, aggregation, and enumeration to achieve a representation of the content, which enables the formulation of categories [21]. Categorization is known as an operation to classify constitutive elements of a set by differentiation and then by regrouping according to gender, with the criteria previously defined and analyzed. This process was aimed at obtaining the perception

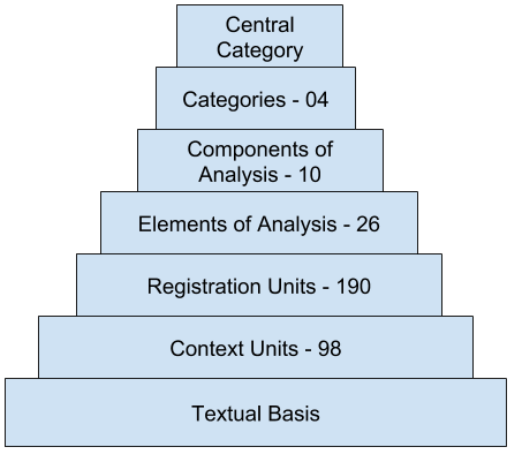

Fig. 5. Tree elements used in content analysis (Adapted from Coutinho [22])

of parents regarding privacy and security issues in the use of technologies by children, and to understand if the technology of smart toys would be accepted in Brazil.

(2) **Identification of context units**. Context unit can be defined as understanding elements to later encode the record unit. A context unit corresponds to a segment of the message, where dimensions are critical to an accurate understanding of the meaning of a registration unit [21]. From the textual basis, the reading and the cutting of parts of this text were done to give origin to the context units. The cutouts varied in size, always aiming to contemplate the thought of the participant on the subject. In the end, 98 context units were returned.

(3) **Identification of registration units**. For each context unit, a new and more in-depth reading of the text was carried out, seeking a better reflection on the messages that the text brought, and could be expressed, for example, in keywords and meaningful expressions. Some questions to facilitate the discovery of meanings have been raised: what is being said in the text? What is its meaning? As a result, the registration units were identified and numbered according to the context units and the original textual basis. This process was carried out with the entire textual basis and its respective context units. The result was the identification of 190 registration units.

(4) **Identification of the elements of analysis**. Subsequently, the 190 registration units were organized based on the criterion of content similarity. As a result, they were reduced to a total of 26 elements of analysis, which came to play the role of properties of the components of analysis, as presented in Table VII. These properties are considered by Strauss [23] as characteristics of a category.

(5) **Identifying the components of analysis**. The 26 elements of analysis were then grouped, having as the criterion the content affinity. As a result, the 26 elements of analysis were grouped into 10 components of analysis and characterized as subcategories. These subcategories have the power of explanation; however, they do not represent a phenomenon themselves. Sub categories answer questions about the phenomenon, such as [23]: How? Why? When? Where? The

TABLE VII
ELEMENTS OF ANALYSIS: PROPERTIES OF COMPONENTS OF ANALYSIS

ID	Property of Component of Analysis
1	Correct age for the use of smart toys.
2	Correct age for smartphones.
3	Correct age for social networking.
4	Parental control in the use of social networks.
5	Parental control in the use of technologies.
6	Parental control in the use of smartphones.
7	Parental control in the use of smart toys.
8	Parental control in the use of the internet.
9	Parental control in the use of toys.
10	Acceptance of toys for conversation between parents and children.
11	Acceptance of smart educational toys.
12	Internet has brought good points.
13	The advancement of technology has brought good points.
14	The advancement of technology has brought danger to children.
15	The advancement of technology has brought negative points.
16	Internet brought negative points.
17	Internet use for malicious subjects.
18	Inappropriate content for children on the internet.
19	Lack of privacy and security in the use of social networks.
20	Privacy and security in the use of the internet impaired.
21	Difficulty of parental control in the use of social networks.
22	Lack of parental control in the use of technologies.
23	Difficulty in depriving children of smartphones.
24	Lack of parental control over the privacy of children.
25	Protection of children's privacy.
26	Lack of confidence in smart toys.

subcategories obtained are presented in Table VIII.

TABLE VIII
COMPONENTS OF ANALYSIS – SUBCATEGORIES

ID	Subcategory
1	Correct age for the use of technologies.
2	Parental control in the use of technologies.
3	Acceptance of new technologies for children.
4	Positive points in the advancement of technology.
5	Negative points in the advancement of technology.
6	Dangerous contents for children on the internet.
7	Children's Privacy and Safety harmed by the use of technologies.
8	Lack of parental control in the use of technologies.
9	Protection of children's privacy.
10	Emergence of new technologies for children.

(6) **Identification of categories**. From the identification of the 10 analysis components (called subcategories), it was possible to carry out an in-depth study and to define similarities between them. As a result, only four final categories were obtained from the ten analyzed subcategories, which are presented in Table IX.

TABLE IX
CATEGORIES

ID	Category
1	Parental control in the use of technologies.
2	Privacy and Security issues with the use of technologies.
3	Protection of children's privacy.
4	Emergence of new technologies for children.

(7) **Selection of the central category**. The central category represents the main theme of the research, has analytical power, gathers other categories to form an explanatory whole, must be frequent in the data, can explain considerable variations within the categories and the main point of the data, arising from the research itself or can be an abstraction [23]. In order to determine the central category, a careful analysis of the data returned to this stage of the research was performed. This analysis sought to reexamine the textual basis, the context units, the registration units, the elements of analysis elements (i.e., the properties), the components of analysis (i.e., the subcategories) and, finally, the categories extracted, to arrive at a central category that would be reflected in the entire content returned. The frequency with which each category was contained in the context units and the registration units is shown in Figure 6. As a result, the central category obtained is characterized by "parental control in the use of technologies" according to the analyzes carried out on the content as a whole, since it is the category most present in the participants' statements.

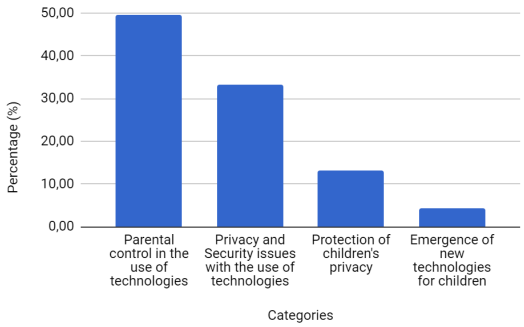

Fig. 6. Categories frequency in the context units and registration units

VII. DISCUSSION OF RESULTS

With the 14 parents who participated in the interview, there was a notable concern about privacy and safety when it comes to the technologies used by their children. In some cases, this occurred more directly; while in others this was indirectly perceived by the way participants answered the questions. As has been mentioned by them, new technologies have come to improve communication, however, especially for children, this can be considered a two-way street. When there is no proper parental control over children's use of these technologies, this may have ended up harming them. In the case where parents are around and may have control of what the child can see and do when using the internet, the danger is less likely to affect the child's privacy and safety.

Due to the first stages of data analysis (textual basis, context units, registration units, elements of analysis and subcategories), it was found that, in general, parents' opinions regarding the privacy of their children are similar. There is a concern about children using devices connected to the internet, including smartphones, tablets, access to social networks or toys with the ability to communicate with their children. Parents, in all their words, have been concerned about the privacy of their children, and the vast majority of them think

that to ensure privacy means basically to be in control of the connection with technologies that their children are using.

According to Tables VII and VIII, with the elements of analysis and subcategories, it is verified that, according to the data collected in the corresponding stages, parental control stood out the most. This shows that the parents interviewed placed more emphasis on their desire to have full control over what their children are accessing when subcategories like "Parental control in the use of technologies" appear.

Next, the four main categories extracted from the previous steps are presented in more detail. These categories generally represent all the content extracted from the interviews with the 14 participants, having different levels of importance, as highlighted in Figure 6.

- **Emergence of new technologies for children** (8 occurrences of the 98 context units / 8 occurrences of the 190 registration units): Of these occurrences, some have raised the positive importance of the emergence of new technologies, but only if accompanied by tools to help in parental control, as mentioned by participant #12: "I could give my child a toy that could talk to him, if it had some type of password to restrict certain subjects. If the questions asked by the toy were of any kind, I'd find it unfeasible; but if there was parental control over it, I might give him." Some reports have shown that participants are not interested in new technologies for their children, as shown by participant #14': "I'd not give my child a toy with the ability to speak and interact with him, because I think we need to control the information so as not to be in danger; though, we can't do it fully; in the case of a toy with the ability to talk to them, it'd be an additional way of being connected to the internet, and maybe I'd not be able to monitor everything."
- **Protection of children's privacy** (25 occurrences of the 98 context units / 25 occurrences of the 190 registration units): The answers indicate that parents worry about their children's privacy when using devices that have access to internet and social networks, as shown, for example, by the participant #3's report: "My child does not use social networks yet due to his age. I only intend to allow him to use when it is formally informed it is applicable to his age according to the app recommendations. It will be difficult to deprive him because he will see other children using and will also want for him; but I'm pretty conservative and I want to avoid it as much as I can."
- **Privacy and security issues with the use of technologies** (40 occurrences of the 98 context units / 63 occurrences of the 190 registration units): Most of the participants mentioned somehow the danger that children can run when connecting to the internet. As stated by some participants, children are innocent beings who often see no evil when talking to others on social networks, for example. Some participants also mentioned that some parents like to publish on social networks pictures of places where their children usually go to alone, allowing that malicious people can collect this information and plan how to do harm to the child. An example of this concern is participant #8's report: "I've heard of cases of criminals who stole children's information on the internet for kidnapping, and I think this is because parents end up putting their children's private life on social networks, post pictures of the places they attend, even the child's school uniform; I've seen cases on the internet in which predators end up seeing, observing, and doing harm to these children."
- **Parental control in the use of technologies** (75 occurrences of the 98 context units / 98 occurrences of the 190 registration units): According to some participants, children may have access to technologies and it would be interesting to see new ones such as smart toys (mainly the educational ones). However, means to help the parental control action need to exist. Specifically, in the case of smart toys, a function would be essential so that the parents could keep control of the information of what the toy speaks with the child. It was also possible to observe that some parents feel that if there is parental control over the use of technologies by children, they will themselves be less affected by problems related to lack of privacy and safety when it comes to children. As, for example, participant #3's report: "I believe that the advancement of technology has made the world somehow more dangerous for children; when parents have no control over what their children are accessing, children end up in danger. But only in relation to that. I think if you have parental control, technology is a way to really help." Also the report from participant #4: "I believe that technology has made the world more dangerous for children; if parents do not have control of what the child is using on the internet, it is certainly dangerous because the child gets very exposed and does not have maturity yet, in fact, to use it independently, without the control of some adult."

As a result of the study of the four categories, it was noticeable that parents present a great concern when it comes to privacy and security in the use of technologies by their children. However, they believe that if there is parental control, which can be backed up by some features on the internet-connected devices themselves, then the concern for privacy and security aspects may be less. Considering this thought and the data obtained with the analysis, parental control is considered the main category and can represent in general the content extracted from the interviews.

As a result, after categorizing all the opinions reported by the interviewees, it was possible to visualize that parents are concerned about their children's privacy when they are connected to any kind of technology, which includes smart toys connected to the internet. In addition, toys with the ability to hold a real-life conversation with their children would probably only be accepted if there was a fairly complete parental control function with which parents could monitor even what the toy spoke to their children and types information they could collect. This type of control is already available in

some of the toys on the market, but still quite limited, as mentioned in Section II.

This analysis was performed according to the conversations with the parents during the interviews. Only with the used method of semi-structured interview, it is not possible to be sure if the information certainly represents the opinions of the interviewees, since they may have, for example, tried to demonstrate a greater theoretical concern than they present in practice. To improve the reliability of the results, it would be necessary to add a method of observation, in which the researchers can capture, in addition to the interviewees' words, their reactions to the questions and their subjective behaviors during the interview.

VIII. Conclusion

This paper aimed to evaluate the perception of potential Brazilian consumers on issues related to children 's privacy involving smart toys. With the results, it was evidenced that the representatives of the Brazilian population interviewed present a high acceptance rate related to the technology of smart toys, assuming that these toys can be made available in Brazil. However, they should only be accepted if this technology is accompanied by features that enable parental control, including, for example, monitoring of the conversations their children will have with the toy. The Brazilian parents interviewed demonstrate an existing difficulty in controlling their children when it comes to technology use issues. Therefore, they usually indicate that a technology such as a toy connected to the internet and able to talk to their children would be an additional danger if there is no proper monitoring and techniques capable of helping control by the parents.

As main contributions, this paper presents an initial description of a sample of the Brazilian population related to their perception on privacy issues on smart toy technology, serving as a basis for future research on this topic. The description of a potential Brazilian profile may be used by the related industry in order to, for example, build a better marketing strategy based on these data. Knowing the perception of a sample of the Brazilian population contributes to the vision about the development of new techniques and privacy policies to be implemented by manufacturers, aiming at the protection of children's privacy, such as a function for parental control.

As future work, we plan to increase the number of participants in this research in Brazil, using, in addition to the interview as data collection, the observation method, to add more value in the study and achieve a greater percentage of certainty regarding the respondents' answers. As well as expand it to other countries, in order to make a comparison of the perception when it comes to countries of different levels of development, more specifically developed and developing countries. For this, a survey is being planned to be answered through social networks and by email.

References

[1] C. Byrne, "Hot toys are dead: Long live hot products," *Young Consumers*, vol. 7, no. 1, pp. 8–13, 2006. [Online]. Available: https://www.emeraldinsight.com/doi/abs/10.1108/17473610610681252

[2] M. L. Jones and K. Meurer, "Can (and should) hello barbie keep a secret?" in *Proceedings of the IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS)*. IEEE Press, 2016, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/document/7560047/

[3] P. C. K. Hung, F. Iqbal, S.-C. Huang, M. Melaisi, and K. Pang, "A glance of child's play privacy in smart toys," in *Proceedings of International Conference on Cloud Computing and Security (ICCCS)*. Springer Verlag, 2016, pp. 217–231.

[4] L. Rafferty, P. C. Hung, M. Fantinato, S. M. Peres, F. Iqbal, S.-Y. Kuo, and S.-C. Huang, "Towards a privacy rule conceptual model for smart toys," in *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS)*. AIS, 2017, pp. 85–102. [Online]. Available: http://aisel.aisnet.org/hicss-50/da/toycomputing/4

[5] K. Michael and A. Hayes, "High-tech child's play in the cloud: Be safe and aware of the difference between virtual and real," *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 123–128, 2016. [Online]. Available: https://ieeexplore.ieee.org/document/7353284/

[6] P. C. K. Hung, M. Fantinato, and L. Rafferty, "A study of privacy requirements for smart toys," in *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS)*, 2016, pp. 71.1–71.7. [Online]. Available: http://aisel.aisnet.org/pacis2016/71/

[7] E. McReynolds, S. Hubbard, T. Lau, A. Saraf, M. Cakmak, and F. Roesner, "Toys that listen: A study of parents, children, and internet-connected toys," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI)*. ACM Press, 2017, pp. 5197–5207. [Online]. Available: https://dl.acm.org/citation.cfm?id=3025735

[8] G. Murno. (2015) O mercado de brinquedos brasileiro é o sétimo maior do mundo. (in Portuguese). [Online]. Available: http://brasileconomico.ig.com.br/negocios/2015-03-10/o-mercado-de-brinquedos-brasileiro-e-o-setimo-maior-do-mundo.html

[9] P. C. K. Hung, Ed., *Mobile services for toy computing*, 1st ed. Berlin Heidelberg: Springer International Publishing, 2015.

[10] L. Rafferty, B. Kroese, and P. C. K. Hung, "Toy computing background," in *Mobile Services for Toy Computing*, P. C. K. Hung, Ed. Berlin Heidelberg: Springer Verlag, 2015, ch. 2, pp. 9–38.

[11] G. Disterer and C. Kleiner, "BYOD bring your own device," *Procedia Technology*, vol. 9, pp. 43–53, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221201731300159X

[12] L. Rafferty, M. Fantinato, and P. C. K. Hung, "Privacy requirements in toy computing," in *Mobile Services for Toy Computing*, P. C. K. Hung, Ed. Berlin Heidelberg: Springer Verlag, 2015, ch. 8, pp. 141–173.

[13] W. Stallings and L. Brown, *Computer Security: Principles and Practice*, 4th ed. Pearson International Editionl, 2008.

[14] L. Liu and M. T. Özsu, Eds., *Encyclopedia of database systems*. Berlin Heidelberg: Springer Verlag, 2009, vol. 6.

[15] D. A. Hertzel, "Don't talk to strangers: An analysis of government and industry efforts to protect a child's privacy online," *Federal Communications Law Journal (FCLJ)*, vol. 52, no. 2, pp. 429–451, 2000. [Online]. Available: https://www.repository.law.indiana.edu/fclj/vol52/iss2/7

[16] D. Holloway and L. Green, "The internet of toys," *Communication Research and Practice (RCRP)*, vol. 2, no. 4, pp. 506–519, 2016. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/22041451.2016.1266124

[17] Authors, "Anonymous due to double-blind review process," *journal title*, vol. x, pp. y–z, 2018. [Online]. Available: url

[18] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in software engineering*, 1st ed. Berlin Heidelberg: Springer Science & Business Media, 2012.

[19] E. Verhellen, *Convention on the Rights of the Child: Background, Motivation, Strategies, Main Themes*. Coronet Books Incorporated.

[20] S. Easterbrook, J. Singer, M.-A. Storey, and D. Damian, "Selecting empirical methods for software engineering research," in *Guide to advanced empirical software engineering*, F. Shull, J. Singer, and D. I. K. Sjoberg, Eds. Springer, 2008, ch. 11, pp. 285–311.

[21] L. Bardin, *Análise de conteúdo - Edição revista e ampliada*, 2nd ed. São Paulo: Edições 70 - AlmedinaBrasil, 2011, (in Portuguese).

[22] C. R. Coutinho, "Formação político-educativa do movimento dos trabalhadores rurais sem terra (mst) no contexto do governo lula (2003 a 2010)," Ph.D. dissertation, 2014, (in Portuguese).

[23] J. M. Corbin and A. L. Strauss, *Basics of Qualitative Research - Techniques and Procedures for Developing Grounded Theory*, 3rd ed. Thousand Oaks - CA, USA: SAGE Publications, 2008.