Towards a Comprehensive Analytical Framework for Smart Toy Privacy Practices

Moustafa Mahmoud, Md Zakir Hossen, Hesham Barakat,
Mohammad Mannan, and Amr Youssef
Concordia Institute of Information Systems Engineering
Concordia University, Montreal, Canada
{m_mahmou,m_osssen,h_bara,mmannan,youssef}@ciise.concordia.ca

ABSTRACT

Smart toys are becoming increasingly popular with children and parents alike, primarily due to the toys' dynamic nature, superior-interactivity, and apparent educational value. However, as these toys may be Internet-connected, and equipped with various sensors that can record children's everyday interactions, they can pose serious security and privacy threats to children. Indeed, in the recent years, several smart toys have been reported to be vulnerable, and some associated companies also have suffered large-scale data breaches, exposing information collected through these toys. To complement recent efforts in analyzing and quantifying security of smart toys, in this work, we propose a comprehensive analytical framework based on 17 privacy-sensitive criteria to systematically evaluate selected privacy aspects of smart toys. Our work is primarily based on publicly available (legally-binding) privacy policies and terms of use documentation, and a static analysis of companion Android apps, which are, in most cases, essential for intended functioning of the toys. We use our framework to evaluate a representative set of 11 smart toys. Our analysis highlights incomplete/lack of information about data storage practices and legal compliance, and several instances of unnecessary collection of privacy-sensitive information, and the use of over-privileged apps. The proposed framework is a step towards comparing smart toys from a privacy perspective, which can be useful to toy manufacturers, parents, regulatory bodies, and law-makers.

CCS CONCEPTS

• **Security and privacy → Social aspects of security and privacy**; • **Social and professional topics → Privacy policies**;

KEYWORDS

Smart Toys, Privacy Policy, Terms of Use, Evaluation Framework, Applications Analysis

STAST2017, December 5, 2017, Orlando, FL, USA

ACM ISBN 978-1-4503-6357-0/17/12…$15.00
https://doi.org/10.1145/3167996.3168002

ACM Reference Format:
Moustafa Mahmoud, Md Zakir Hossen, Hesham Barakat, Mohammad Mannan, and Amr Youssef. 2017. Towards a Comprehensive Analytical Framework for Smart Toy Privacy Practices. In *STAST2017: 7th International Workshop on Socio-Technical Aspects in Security and Trust, December 5, 2017, Orlando, FL, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3167996.3168002

1 INTRODUCTION

Smart toys are gaining popularity in recent times with a rapid growth in sales every year.[1] The apparent educational value has led more parents to adopt these toys for their children. Advances in voice recognition technologies, and the introduction of several hardware sensors have enabled new generations of smart toys to be more intelligent, interactive and dynamic than their predecessors. On the other hand, these enhanced capabilities allow the toys to collect a wide array of personal/device information that could be used for profiling individual children. As many of these toys are also Internet-connected, exposure of the collected information from the toys, personal devices, back-end servers and third-parties, can be a serious threat for the security and privacy of children (including the risk of identity theft; see e.g., [11]).

Recognizing these unique risks to children, governments and regulatory authorities in different regions are introducing specialized laws/acts, e.g., the US Children's Online Privacy Protection Act (COPPA [6]); see also the EU General Data Protection Regulation (GDPR [13]). However, the latitude of privacy concerns for children is getting wider with the revelation of large scale data breaches and loopholes in security mechanisms of the these toys. For example, the VTech leak in 2015 [27] and the recent CloudPets leak in 2017 [35] exposed personal data of nearly six million parents and children; in both cases, adequate security measures were sorely lacking (see also [28]). My Friend Cayla has been banned in Germany for its insecure bluetooth connection [36], allowing a nearby attacker (e.g., up to 15 meters) to interact with children and spy on them.

The information collection practices in smart toys have also been scrutinized recently. For example, the Campaign for a Commercial-Free Childhood (CCFC) condemned the way Hello Barbie collects children's data [15]. The privacy policy of Hello Barbie stated that they may use the collected data "for other research and development and data analysis purposes," without a clearer definition of the scope and extent to which the information can be used. Such vague explanations about data practices may allow them to use the

[1] According to Juniper Research [31], smart toy sales are expected to grow up to three times in a span of just five years from 2017 to 2022.

collected information for a wide range of purposes (see e.g., [34]). The US Federal Trade Commission (FTC) has conducted several studies (see e.g., [4, 5, 7]) in recent years, highlighting the lack of disclosure about data practices in mobile apps targeting children and teens. These FTC reports identified an increased availability of privacy policies: 45% apps contained direct links to their privacy policies in the latest survey [7] in comparison to 16-20% in the earliest one [4]; however, ideally, 100% apps should provide a direct privacy policy link.

The lack of easily accessible privacy policies and complexity of the policies hinder parents' ability to fathom potential risks of smart toys and the companion apps for their children. Office of the Privacy Commissioner of Canada (OPC) also offers guidelines on how information related to children can be collected. According to OPC, collection, use and sharing of information about children under 13 years of age, must be approved by their parents. However, in a recent study [25] parents were found to be paying no attention to privacy warnings before allowing their children to play with toys with known issues, such as Hello Barbie.

Several studies on legacy privacy policies generally focus on determining information collection practices in more generic cases, including, privacy policies of smartphone apps and web services; see e.g., [1, 32, 41]. Studies on smart toys generally focus on security analysis (e.g., implementation/design flaws [12, 33]). Currently, there is a lack of a comprehensive framework to evaluate and compare smart toys in terms of their privacy policies (and terms of use documents). Such a framework may increase parents' ability to make a more informed decision regarding the toys they purchase for their children.

In this work, we propose a broad range of criteria to analyze various privacy aspects of smart toys. In particular, we define 17 privacy-sensitive features as part of our analysis framework. Our selection criteria for smart toys span four axes: category, functionality, availability, and the use of companion apps. Toy category spans different types of toys, such as dolls, talking toys, and robots for children. Toy functionality includes mobility (e.g., toys that can be remotely controlled), physical capabilities (e.g., gripping or moving objects), sensors (e.g., microphone, camera, IR sensor, gyroscope), output capabilities (e.g., speakers), and wireless communication (e.g., WiFi, Bluetooth, IR). We select toys that are easily available in Canada/USA from an online or regular store. Finally, we give preference to toys with companion smartphone apps, as they present another attack vector and increase toy privacy risks.

Based on our selection criteria, we evaluate a representative set of 11 smart toys and their companion apps. Table 1 lists our selected toys and the hardware sensors and communication channels they are equipped with (for more information on the toys, see Appendix A). Furthermore, to verify permission usage and identify information collection and potential misbehaviors, we perform static analysis of the companion apps. Our results demonstrate multiple instances of unnecessary and unjustified information collection, absence of legal compliance and highly over-privileged companion apps. Note that our comparison is mostly based the stated policies; these policies may omit important information (e.g., no mention of collecting home addresses), or provide false information (e.g., adherence to COPPA, strong security measures at the server-side). More experimental validation is needed beyond our preliminary static app analysis (e.g., actual information leakage from toys, apps, and toy web-services). Such validation is out of scope for this work.

Table 1: Available sensors and communication channels in our selected smart toys

	Devices and Sensors									Communication		
	Microphone	Speaker	Camera	IR-Vision	Gyroscope	Motion Detector	Touch Detector	Accelerometer	Thermometer	WiFi	Bluetooth	IR
Hello Barbie	✓	✓								✓		
Toymail	✓	✓								✓		
Sphero BB-8	✓	✓			✓	✓				✓	✓	
Wowwee Chip	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓
Smart Toy Monkey	✓	✓								✓	✓	
CogniToys Dino	✓	✓								✓	✓	
Edwin the Duck		✓							✓	✓	✓	
Anki Cozmo		✓	✓		✓					✓	✓	
My Friend Cayla	✓	✓								✓	✓	
I-Que Robot	✓	✓								✓	✓	
Zenbo	✓	✓	✓		✓	✓				✓	✓	

Our main contributions are as follows:

- We propose a comprehensive analytical framework with 17 privacy-sensitive criteria to evaluate privacy policies and terms of use documents of smart toys. We augment the framework with static analysis of companion apps that are essential for the toys' functioning.
- We evaluate 11 recent smart toys using our framework, and compare them based on the proposed privacy criteria. The framework apparently captures the most serious privacy considerations, and can be used to evaluate a diverse set of smart toys and their companion apps.
- We show that most toys collect privacy-sensitive information and share them with third parties for unclear purposes. Moreover, companion apps are largely over-privileged, requesting dangerous permissions that are not necessary, or not used at all.

Communicating our results. On Nov. 18, 2017, we have shared our results with all the toy companies in our evaluation—through dedicated email addresses for sharing privacy concerns, when available (for four companies); otherwise, we used general support emails or web forms (for seven companies). As of Nov. 29, 2017, Toymail and Sphero have acknowledged the receipt of our report (beyond automated responses). Two emails bounced back with an invalid email address error.

2 EVALUATION FRAMEWORK

In this section, we define a diverse set of criteria that we believe are representative of various privacy aspects in smart toys. The criteria we explore encompass five categories: application authenticity and permissions; privacy policy documentation; ToU documentation; information collection; and information storage, sharing and protection. The selected set of criteria are initially inspired by the data quantification categories of Sadeh et al. [32], and iteratively refined during our analysis of the smart toys. To augment our analysis of

the available documentation, we perform static analysis of the companion apps. We use the word *feature* and *criterion* interchangeably throughout the rest of the paper.

2.1 Criteria

In this section, we define the rating criteria of our evaluation framework. For each criterion, a toy may fully or partially satisfy it, not satisfy it, or may not provide relevant information.

2.1.1 Application Authenticity and Permissions. Smart toys are generally accompanied by a companion mobile app, which can be downloaded from an app market (e.g., Google Play). Downloading the right app affiliated with the toy is essential for its intended functioning, and for security and privacy reasons (e.g., to avoid downloading a repackaged app with malware/adware/spyware). Moreover, over-privileged apps can pose privacy risks, as they may request extraneous permissions, which can be used to access sensitive information. We define the following criteria to cover these concerns.

A1 App-website-links: The official website of the toy contains a link to download its companion app from an app market (e.g., Google Play), and the app contains a link to the official toy website. This bi-directional linking verifies the app's origin; a toy is partially granted this feature if one of them is missing.

A2 Reasonable-permissions: The companion app requests only for permissions that are necessary for its intended functionality. We perform static analysis of the companion apps together with manual evaluation of provided features to rate this criterion.

2.1.2 Privacy Policy Documentation. Privacy policy communicates data practices of a service. An easily accessible and up to date privacy policy is essential for communicating privacy implications to parents who are responsible for permitting the collection of their children's information.

P1 Store-app-website-links: The companion app, its Google Play page, and the official website contain a link to the toy privacy policy; partially granted if either of them is missing.

P2 Update-info-notification: Any changes in the privacy policy should be reported to users. To fully satisfy this feature, the toy must have the date of last update mentioned in the policy along with explanation of how they report the updates to users; partially granted if either of them is missing.

2.1.3 Terms of Use Documentation. We consider ToU as an important aspect in our framework as it may contain important privacy practices; we define the following two features.

T1 Store-app-website-links: Similar to P1 (for ToU).

T2 Update-info-notification: Similar to P2 (for ToU).

2.1.4 Information Collection. Smart toys can collect a wide range of information during setup/installation (companion app), or while being used by children. They must comply with privacy acts or laws (specific to children or in general) of different regions where the toys are sold. We define the following criteria to highlight data collection practices in smart toys.

C1 Laws/acts-compliant: The privacy policy of a toy states explicitly the laws/acts they comply with, and the jurisdiction(s) under which they operate.

C2 Reasonable-PII-collection: The toy and its companion app collects *reasonable* PII. We define email address as reasonable PII, assuming email is used to communicate privacy policy and ToU changes to the user. Any PII beyond email is considered unreasonable.

C3 No-website-data-collection: The toy's website does not collect any information that can be used for user tracking or serving personalized ads.

2.1.5 Information Storage, Sharing and Protection. Recent data breaches (e.g., [27, 35]) raise questions on secure data storage and protection practices of smart toys. This is a major concern as one of the leaks ([27]) contained information that could lead to identification of individual children and their location. We define eight features under this category.

S1 Data-storage-location: The location of data storage is stated in the toy's privacy policy. Based on their storage location, companies may be subjected to specific regulations in case of a data breach incident. For example, data breach regulations in US states differ;[2] see also EU e-Privacy Directive[3] and GDPR [13].

S2 No-third-party-PII-sharing: Any information collected through the toy is not shared with third parties.

S3 Parental-PII-control: Parents can permanently delete the information collected by the toy and its companion app.

S4 PII-protection: The measures taken by the toy manufacturer to protect the collected information is properly documented in the privacy policy or the ToU. Currently, we simply rate a toy based on its use of TLS for all communications between the toy/user/device and back-end servers.

S5 Dedicated-privacy-support: The toy manufacturer offers dedicated support for privacy concerns (e.g., via a specific web page or email address, instead of a generic support contact).

S6 Protection-program-participant: The toy manufacturer participates in independent programs that provide additional support to users to resolve privacy issues. Such programs may include Judicial Arbitration and Mediation Services (JAMS [20]) and TRUSTe [37].

S7 Bug-bounty-participant: The toy manufacturer participates in bug bounty programs that encourage people to identify security and privacy issues in their toys/apps. Such participation may indicate a strong commitment towards information security and protection.

S8 Do-not-track-support: The documentation explains how the toy's website handles Do Not Track (DNT) requests. A DNT request means the user does not want his browsing data to be collected and tracked across sessions/devices.

2.2 Static Analysis

We use two complementary tools for static analysis: RiskInDroid [26] and Androwarn [24]. We use RiskInDroid to analyze the permission usage of companion apps in order to identify over-privileges (we limit our app analysis to Android apps only). RiskInDroid uses machine learning techniques to quantify risks posed by Android apps, and assigns a risk value between 0 to 100; higher value indicates higher risks. It uses static analysis to infer permission utilization in the app code, and categorizes them in four sets. In our analysis

[2] See: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

of companion apps, we focus on two sets, namely the declared permissions in the app Manifest, and the permissions that are actually used in the code. This is done by extracting the API calls from the decompiled source code and mapping them to the required permissions (using PScout [2]).

We denote over-privilege as having permissions in the Manifest that are not utilized in the app code. Such over-privilege does not necessarily imply hidden intents, as there could be several benign reasons (e.g., developer mistake). Moreover, in newer versions of Android (6.0 and later), the app will not be granted the dangerous permissions during installation, rather it would ask for permissions during runtime and the user may choose to grant or deny them. However, the app may still ask the users for permissions that they do not need or use at the moment, but once granted can utilize them in later versions of the app.

We use another static analysis tool Androwarn [24] to identify potential misbehaviors and information collection. In contrast to RiskInDroid, Androwarn uses a combination of structural and data-flow analysis to identify suspicious behaviors including exfiltration of sensitive information (e.g., device unique identifiers and geolocation via GPS/WiFi), and abuse of functionality (e.g., making phone calls, sending SMSes, and recording audio/video).

We choose RiskInDroid as it is one of the most recent tools of its kind (published in 2017). In contrast, Androwarn is an open source tool available since 2013 (used in other app analysis studies). The accuracy of the results of our analysis is tied to the tools we use. We encountered only one mismatch in outcomes from the tools (for Toymail, RiskInDroid labels READ_CONTACTS as unused, but Androwarn's data flow analysis finds its use for reading the contact list); we acknowledge the fact that using different tools may yield somewhat different results.

3 ANALYSIS AND RESULTS

We now use our criteria to evaluate a representative set of 11 smart toys. We manually examine the privacy policies and ToU documentation to check whether the proposed privacy criteria are fulfilled by the toys or not (between June 2017 to July 2017, see Table 7 in the Appendix for links to the documents). We also statically analyze the companion apps to identify over-privileged apps, personal/device identifier leakage, and suspicious behaviors. Below, we elaborate how each toy is rated in our framework; note that, for brevity, we discuss a feature in the text if it requires some explanation. For a quick summary of our results and an overall picture, see Table 2 and Section 4. Table 3 list permissions declared in the app Manifests, and Figure 1 shows permission utilization. Tables 4, 5, and 6 summarize PII collection, device information collection, and toy/app usage collection, respectively.

3.1 Hello Barbie

Hello Barbie's companion app does not satisfy *Reasonable-permissions* as it declares seven permissions in the Manifest but uses only four. The unused permissions include write access to the internal storage and read/write access to the external storage. Hello Barbie provides *Store-app-website-links* to the privacy policy, and satisfies *Update-info-notification*. It also mentions that in some cases, it obtains the user's prior verifiable approval before updating the policy (no explicit mention of approval mechanisms).

Hello Barbie is *Legal-compliant* with COPPA. It does not satisfy *Reasonable-PII-collection*: from the user, it collects email address, voice recordings, and child birthday (Table 4); from the device, it collects device model and name, IP address, operating system, browser type, mobile network information (Table 5). It also collects service usage information including information about how the app features and speech processing services are used, and information about the number, frequency and length of each session (Table 6). In addition, the toy does not satisfy *No-website-data-collection* as it sets cookies and web beacons.

Hello Barbie does not satisfy *No-third-party-PII-sharing* as it shares personal information with vendors, consultants, and other service providers. Hello Barbie provides *Parental-PII-control* through the parent's account. The toy also provides *PII-protection* through secure encrypted data transmission (TLS). In addition, the child's voice recordings are not stored locally on the toy (WiFi credentials are stored). However, a recent study [33] shows that Hello Barbie suffers from many vulnerabilities including using weak passwords, no password brute force protection, using unencrypted WiFi network to configure the toy, and not requiring unique authentication to modify the configuration of the toy. As our analysis is based on the information obtained from the documentation, we grant *PII-protection* to Hello Barbie. We follow the same principle for other toys, assuming any reported vulnerabilities will be promptly fixed.

Hello Barbie is *Protection-program-participant*: the user can directly submit a complaint to JAMS to resolve a dispute. In addition, Hello Barbie states that its server, ToyTalk, is subject to the investigatory and enforcement powers of the US FTC. It is *Bug-bounty-participant* according to HackerOne [17]; however, Hello Barbie mentions in the ToU document that attempts of reverse engineering, decompiling, or discovering the source code are disallowed. The toy does not clearly state the *Data-storage-location*: it states that the location can be in the USA or other countries.

3.2 Toymail

Toymail does not satisfy *Reasonable-permissions* as it declares 14 permissions in the Manifest but does not use six, including get accounts, access the camera and read/write external storage. In addition, our static analysis shows that the companion app can abuse the telephony service to make phone calls without user consent, and it can read and edit contacts.

Toymail partially satisfies *Store-app-website-links* (P1); it includes some privacy information in the ToU document, including collection of personal information (e.g., voice recordings), service usage information, and sharing policy of personal information. It also partially satisfies *Update-info-notification* (P2) since it fails to notify the user with any update details to the privacy policy, although it indicates the update date (similar rating for ToU T2).

Toymail is *Legal-compliant* with COPPA, and the federal courts in Michigan have exclusive jurisdiction. It does not satisfy *Reasonable-PII-collection* as it collects email address, child's name, image, and birthday, time zone, sound bite of the child's name (see Tables 4, 5, and 6). Moreover, our data flow analysis for the companion app reveals that it also collects the unique device ID that can be used

Table 2: Comparative evaluation of the representative smart toys

Product	A1: App-website-links	A2: Reasonable-permissions	P1: Store-app-website-links	P2: Update-info-notification	T1: Store-app-website-links	T2: Update-info-notification	C1: Legal-compliant	C2: Reasonable-PII-collection	C3: No-website-data-collection	S1: Data-storage-location	S2: No-third-party-PII-sharing	S3: Parental-PII-control	S4: PII-protection	S5: Dedicated-privacy-support	S6: Protection-program-participant	S7: Bug-bounty-participant	S8: Do-not-track-support
Hello Barbie	●		●	●	●	●	●					●	●	●	●	●	N/A
Toymail	●		○	○	●	○	●					●	●				N/A
Sphero BB-8	●		●	○	●	○	●						●				○
Wowwee Chip	●		○		N/A	N/A	●			N/A		○	N/A				N/A
Smart Toy Monkey	●		●	○	○	○	●					●	N/A	●			N/A
CogniToys Dino	○		○	○	●	○	●					●	○				N/A
Edwin the Duck	○		○	○	●		●					●	○				N/A
Anki Cozmo	○		●	●	○	○	●	N/A		●		●	●	●	●		
My Friend Cayla	●		○	○	N/A	N/A	●						●				N/A
I-Que Robot	●		●	○	●	○	●						●				N/A
Zenbo	○		○	○	●	○							●	●			N/A

● = offers the feature; ○ = Partially offers the feature; no circle = does not offer the feature; N/A = information unavailable.

Table 3: Permissions requested by companion apps

	Data Access			Communication						Functionalities														Control					
Product	Photos, Media, Files and Storage	USB storage	Contacts	View WiFi connections	Full network access	WiFi multicast reception	Control WiFi	Pair with bluetooth devices	Access bluetooth settings	Take pictures and videos	Record audio	Receive data from Internet	Approximate location	Precise location	Read phone status and identity	Use accounts on the device	Google Play license check	Send sticky broadcast	Retrieve running apps	Disable screen lock	Control flashlight	Run at startup	Audio settings	Display settings	Control vibration	Prevent device from sleeping	Modify system settings	Control accounts	Create accounts
Hello Barbie	✓	✓		✓	✓																			✓	✓	✓			
Toymail		✓	✓	✓	✓					✓	✓	✓																	
Sphero BB-8	✓	✓		✓	✓			✓	✓	✓	✓	✓	✓		✓	✓	✓							✓	✓				
Wowwee Chip	✓	✓			✓			✓	✓		✓														✓				
Smart Toy Monkey				✓	✓		✓	✓	✓			✓																	
CogniToys Dino				✓	✓								✓												✓				
Edwin the Duck	✓	✓			✓			✓	✓			✓	✓										✓						
Anki Cozmo	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓				✓								✓	✓				
My Friend Cayla	✓	✓		✓	✓			✓	✓		✓					✓	✓						✓	✓					
I-Que Robot	✓	✓		✓	✓			✓	✓		✓					✓	✓						✓	✓					
Zenbo	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓			✓	✓		✓	✓	✓	✓		✓		✓	✓	✓	✓	✓

to fingerprint the user's device and can allow tracking the user across different services [23]. In addition, it collects information from users when they use the toy's website, including IP address, browser type and version, and cookies. It also uses Google analytics service, hence it does not satisfy *No-website-data-collection*.

Toymail does not satisfy *Data-storage-location* as it states that data can be stored in the USA or other countries. It does not satisfy *No-third-party-PII-sharing* as it shares personal information with "Electric Imp", service technicians, other Toymail employees, and provides users' personal information in case of a law or court order, or if third-party entities audit its system for security vulnerabilities. Toymail satisfies *PII-protection* (uses TLS). It uses Amazon cloud service to store personal data, and thus it depends on Amazon's security measures to prevent the unauthorized access to its data. Toymail also performs automated deployments and security upgrades, and it uses independent third-party services to audit the system for security vulnerabilities. It is not *Bug-bounty-participant* and prohibits any attempts for reverse engineering, decompiling, or discovering the source code.

Table 4: Personal information collected by smart toys via the toys and companion apps

Product	Name (parent)	Name (child)	Gender	Physical address	Country	Postal code	Email address	Social media profile	Telephone number	Child image	Voice recordings	Child birthday	Child's interests	Payment info	Demographic info
Hello Barbie							✓			✓	✓				
Toymail		✓					✓		✓		✓				
Sphero BB-8	✓		✓	✓			✓							✓	✓
Smart Toy Monkey	✓	✓					✓		✓						✓
CogniToys Dino	✓	✓	✓	✓			✓		✓		✓	✓	✓		
Edwin the Duck	✓			✓			✓		✓					✓	
My Friend Cayla	✓					✓	✓			✓	✓				
I-Que Robot	✓					✓	✓			✓	✓				
Zenbo	✓		✓	✓	✓	✓	✓	✓						✓	

Table 5: Device information collected by smart toys (from user devices e.g., smartphone)

Product	Device Unique ID	Serial Number	Mac address	IP address	Device type	Device name and model	Device activation time	WiFi SSID and password	Operating system	Browser type	Device carrier	Internet service provider	Network status	WiFi nearby APs	GPS info
Hello Barbie	×			✓		✓			✓	✓	✓		×		
Toymail	×			✓				✓					×		
Sphero BB-8	×			✓	×	✓			✓	✓	✓	✓			
Wowwee Chip	×										×				
Smart Toy Monkey						✓			✓	✓	✓		×		
CogniToys Dino	×										×		×		
Edwin the Duck	✓			✓	✓				✓	✓	×		×		
Anki Cozmo					×								×		
My Friend Cayla				✓	×						×		×		
I-Que Robot				✓							×		×		
Zenbo	✓	✓	✓	✓	×	✓	✓		✓		✓		✓	✓	✓

✓ refers to information collected by the companion apps as declared in the privacy policy
× refers to information collected by the companion apps but not declared in the privacy policy
blank means no information is collected

3.3 Sphero BB-8

Sphero BB-8 does not satisfy *Reasonable-permissions* as it declares 18 permissions but uses 13. It requires location access, which is not necessary for the toy; it requires access to device status and identity, allowing it to collect user's personal information including phone number and device ID. Moreover, the static analysis for the companion app reveals that it can make phone calls without the user's consent.

Sphero BB-8 partially satisfies *Update-info-notification* for ToU (T2) as the toy only notifies users with 'important' changes in the ToU without defining what is considered as important.

Sphero BB-8 is *Legal-compliant* with EU safe harbor agreement [14], which is an agreement between the European Union and USA to protect user information; it is also governed by the laws and courts

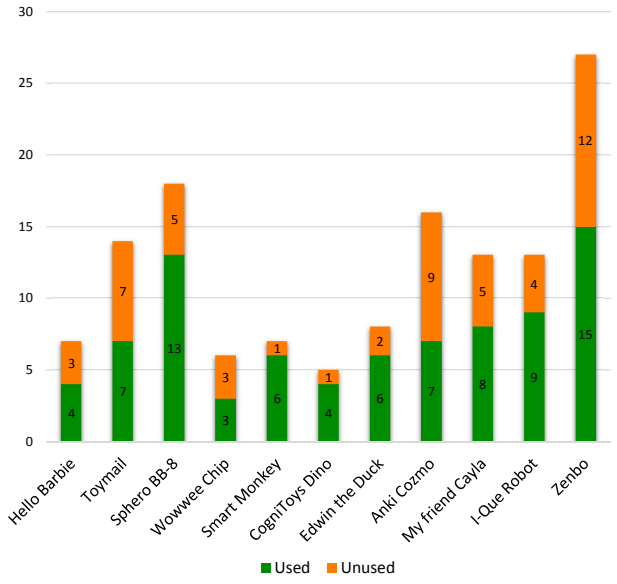

Figure 1: Permissions requested (used vs. unused) by the companion apps

of Colorado (USA). On the other hand, Sphero BB-8 does not satisfy *Reasonable-PII-collection* as the toy collects excessive information from users; see Tables 4, 5, and 6. Moreover, our static analysis reveals that the toy also collects the unique device ID. Sphero BB-8 does not satisfy *No-website-data-collection* as it gathers information including browser/OS type, IP addresses, referring URL, date/time stamps for the visits, cookies, web beacons. It also indicates that third parities including advertisers, ad measurement services, and ad networks may collect device information and information about the users' online activities over time and across different websites.

Sphero BB-8 does not satisfy *Data-storage-location* as it may store the information in the USA or any other country. It lacks *No-third-party-PII-sharing*: it shares personal information with third-party services who may work for the company, and in the case of corporate restructuring or court order. The toy lacks *Parental-PII-control* as it does not provide an explicit facility for PII-deletion, though it provides an email address, which parents can use to contact the company for deleting personal information; however, it mentions that the information will be deleted from their active server but not from the archive servers. It provides *PII-protection* as it uses encrypted traffic and it hires third-party security experts to audit the network infrastructure. It partially provides *Do-not-track-support* feature because Sphero BB-8 discusses about DNT in their documentation but acknowledges that they may not be able to recognize such requests.

3.4 Wowwee Chip

Wowwee Chip lacks *Reasonable-permissions* as only three out of the six requested permissions are used. Wowwee Chip partially provides *Store-app-website-links* (P1) to the privacy policy as there is no link from Google Play to the privacy policy. Wowwee Chip

Table 6: Toy usage information collected by smart toy companies

Product	Toy's ID	Firmware version	App install and uninstall time	Toy features used	Toy features usage frequency	Session length	Crash history
Hello Barbie				✓	✓	✓	
Toymail	✓	✓					
Sphero BB-8		✓		✓	✓	✓	
Smart Toy Monkey				✓	✓	✓	
My Friend Cayla			✓				✓
I-Que Robot			✓				✓
Zenbo				✓	✓	✓	✓

does not provide ToU document, hence *Store-app-website-links* (T1) and *Update-info-notification* (T2) features are inapplicable.

Wowwee Chip is *Legal-compliant* with COPPA. It collects personal information from users when they sign up for email newsletters, or register a product; however, Wowwee Chip does not mention exactly which personal information it collects. Our static analysis reveals that the companion app collects the unique device ID, and thus not satisfying *Reasonable-PII-collection*. Wowwee Chip sets cookies through its website, hence it does not satisfy *No-website-data-collection*.

Wowwee Chip fails to achieve all the features of *Information Storage, Sharing and Protection* except *Parental-PII-control* (partial). Wowwee Chip mentions that users can delete their accounts, though it does not mention whether or not the personal information will be permanently deleted.

3.5 Smart Toy Monkey

Smart Toy Monkey lacks *Reasonable-permissions* as it requests location permission in the Manifest, which remains unused in the app. It partially satisfies *Update-info-notification* (P1) as it does not include the last update date in the privacy policy, and states that it may notify users about important changes. Smart Toy Monkey partially satisfies *Store-app-website-links* (T1) for ToU because in Google Play, Smart Toy Monkey mistakenly names the ToU as privacy policy, which can mislead users, although it provides a direct link to the ToU in the companion app and the website. It also partially achieves *Update-info-notification* (T2) because it does not indicate the last update date in the ToU (but notifies users).

Smart Toy Monkey is *Legal-compliant* with US laws, implying COPPA compliance. It lacks *Reasonable-PII-collection* as it collects unique device ID (revealed by the static analysis). Smart Toy Monkey also states that it optionally collects names, email, telephone number, demographic and other personal information. It does not satisfy *No-website-data-collection* (uses cookies and web beacons).

Smart Toy Monkey does not provide *No-third-party-PII-sharing*: it may use third parties to provide analytics and advertising services, implying that it can share personal information with them. It does not clearly state the *Data-storage-location* as it may store information in the USA or any other country. It is not *Bug-bounty-participant* and it states clearly that it prohibits any attempts for reverse engineering, decompiling, or discovering the source code.

3.6 CogniToys Dino

CogniToys Dino partially achieves *App-Website-links*, as it does not provide a link from website to the app. It lacks *Reasonable-permissions* as the companion app requires location access permission (also another unused permission). CogniToys Dino partially satisfies *Store-app-website-links* (P1) as it has no direct link to the privacy policy from the Google Playpage; the policy is reachable through its app interface. It partially satisfies *Update-info-notification* (P2) because it does not notify users with updates in the privacy policy. For ToU, CogniToys Dino partially provides *Update-info-notification* (T2) because it states that users must check back the ToU for any changes, implying that CogniToys Dino does not notify the user with changes.

CogniToys Dino is *Legal-compliant* with US laws, implying COPPA compliance. It lacks *Reasonable-PII-collection* as it collects name, address, mobile phone number, email address, payment information, and child's name, date of birth, and gender. Static analysis reveals that the companion app also collects unique device ID. It does not satisfy *No-website-data-collection* as it collects information about web browser, OS, ISP, IP addresses, device type, viewed pages, the time and duration of visits to the site, and it sets cookies uses Google Analytics services.

CogniToys Dino lacks *Data-storage-location*: it can store user information in the USA or any other country. It does not satisfy *No-third-party-PII-sharing* because it shares information with third-party service providers who work for the company. It also shares personal information in case of corporate restructuring, or in case of a law or court order. We rate CogniToys Dino as partially providing *PII-protection* since it does not mention exactly which kind of measures it takes to protect data, although CogniToys Dino states that it takes physical, electronic, and procedural safeguards to protect the information. It is not a *Bug-bounty-participant*, and prohibits any attempts for reverse engineering, decompiling, or discovering the source code.

3.7 Edwin the Duck

Edwin the Duck is labeled as partially satisfying *App-website-links* as its companion app contains a link to its official website but the link from the website to its Google Play page is missing. Static analysis of the app reveals two unused permissions (read/write external storage), making it over-privileged and not satisfying *Reasonable-permissions*. In spite of containing links to the privacy policy from its website, companion app and Google Play page, Edwin the Duck is partially granted *Store-app-website-links* (P1) as the later two link to different documents. *Update-info-notification* (P2) is partially satisfied as both versions of the privacy policy state the last date of update but fail to mention whether they will keep the users updated with any changes in the policy. For ToU, it lacks *Update-info-notification* (T2).

Edwin the Duck does not satisfy *Reasonable-PII-collection* because it collects name, address, email address, type of device, device unique ID, IP address, OS, and browser information. It does not satisfy *No-website-data-collection* as it sets cookies, and collects name, email address, mailing address, phone number, and credit card information.

Edwin the Duck lacks *No-third-party-PII-sharing* as it shares information with third-parties who assist the company in operating and developing the service. It states that non-personally identifiable visitor information may be provided to other parties for marketing, advertising, or for other uses. We rate Edwin the Duck as providing *Parental-PII-control* as it allows parents to delete PII by contacting the company through "Contact us" link in the website. It partially provides *PII-protection*: Edwin the Duck mentions that all sensitive information is transmitted over SSL (but does not clarify what is considered as sensitive, except credit card numbers); at the server-side, Edwin the Duck does not store a user's private information such as credit card and financial information. Edwin the Duck is not *Bug-bounty-participant*, and it prohibits any attempts for reverse engineering, decompiling, or discovering the source code.

3.8 Anki Cozmo

Anki Cozmo partly achieves *App-website-links* as the link to the Google Play page of the companion app from its website is unavailable. It lacks *Reasonable-permissions*: the app uses 7 out of 16 requested permissions. The unused permissions include read/write access to the external storage of the device, access to bluetooth settings. We grant the toy a partial *Store-app-website-links* as the ToU is unavailable in its Google Play page. The toy is granted a partial *Update-info-notification* as there is no mention of how they will report updates in ToU to users. *Reasonable-PII-collection* is not granted as there is no clear explanation of what data they collect from users. *No-third-party-PII-sharing* is not granted as it shares collected information with third party ad networks. The toy achieves *Protection-program-participant* as users can contact TRUSTe [37] and JAMS in case of a dispute.

3.9 My Friend Cayla

My Friend Cayla fails to satisfy *Reasonable-permissions*: 5 out of 13 requested permissions are unused, including read/write access to external storage. Moreover, static analysis shows that the app can make phone calls without users' consent. We could not find a link to the privacy policy from the app, therefore, granting a partial *Store-app-website-links*. There is no mention of how it will notify users of any policy changes, although, it contains the last date of update in the privacy policy, thus partially fulfilling *Update-info-notification* (P2).

The toy does not offer *Reasonable-PII-collection* as it collects IP address, zip code, date of birth and voice messages. Furthermore, the static analysis for the companion app shows that it collects the unique device ID. The toy fails to satisfy *No-third-party-PII-sharing* as it shares data with partner organizations. It lacks *Parental-PII-control* as according to its privacy policy, there is some information that cannot be removed completely.

3.10 I-Que Robot

I-Que Robot does not satisfy *Reasonable-permissions* as four out of thirteen declared permissions remain unused, including write access to the external storage. Data flow analysis for the app also shows that it can make phone calls. Although the last date of update is mentioned, there is no specific statement in the privacy policy on notifying users about changes in the document, thus partly satisfying *Update-info-notification* (P2); it is similarly rated for T2 (ToU). I-Que Robot collects the same PII as My Friend Cayla, and thus lacks *Reasonable-PII-collection*. The toy shares information with other parties and fails to satisfy *No-third-party-PII-sharing*. The toy uses firewalls and secure databases to achieve *PII-protection*.

3.11 Zenbo

Zenbo is partially granted *App-website-links* as the official website does not contain any link to the companion app's Google Play page. The app is also highly over-privileged; it requests 27 permissions, but uses only 15 (unused permissions include: flashlight, recording audio, using camera and modifying system settings). The app requires the permission to retrieve running apps information and to manage accounts on the device. Static analysis also reveals that the companion app can be involved in telephony service abuse by making phone calls without users' consent. Thus Zenbo is not granted *Reasonable-permissions*.

The toy partially achieves *Store-app-website-links* because its Google Play page provides a link to the Mandarin version of the privacy policy and there is no way to switch to the English version, though the website and the app provide links to the English version. The toy is also partially granted *Update-info-notification*: it will notify users if there is any important/big update in the policy. *Update-info-notification* is achieved partly as the procedure of notifying users is not mentioned. We do not grant *Reasonable-PII-collection*: it collects a wide range of PII including name, email, gender and date of birth, if the user decides to login using social media profiles; otherwise, it only requires email address and country.

4 OVERALL RESULTS

None of the toy companion apps achieve *Reasonable-permissions*. Our static analysis reveals different levels of over-privileges (i.e., more permissions declared in the Manifest than the app needed or used). For example, Smart Toy Monkey and CogniToys Dino declare only one unused permission, but Zenbo has 12 unused permissions. Among the declared and used permissions, there are multiple instances where the requested permissions are not necessary for the toys' intended functioning. For example, Sphero BB-8 requires access to the approximate location; Zenbo requests permissions to allow managing users' accounts on the device. Static analysis also shows that some toys may perform unwanted/suspicious activities surreptitiously. For example, My friend Cayla, I-Que Robot, and Zenbo companion apps can make phone calls without user consent.

Most toys perform poorly in *Information Collection* features. All except Anki Cozmo collect PII that appear unreasonable, and Anki Cozmo fails to declare which PII it collects. Collected PII includes: email address, voice recordings, address, phone number, child's name, image and birthday; device information including device model and name, IP address, OS/browser version, and mobile network information. Collected service usage information includes: information about how the features of the app and speech processing services are used, and information about the number, frequency and length of each session. Moreover, static analysis reveals that some toys may collect personal information that is not mentioned in their privacy policies. For example, Toymail, Sphero BB-8, Wowwee Chip, CogniToys Dino companion apps collect the unique device ID (e.g., IMEI) that can be used to fingerprint the user's device and can allow tracking the user across different services. All the toys fail to achieve *No-website-data-collection* as they at least set cookies and web beacons (which can be used for tracking and serving targeted ads; see e.g., [3]).

Except Wowwee Chip all the toys share PII with third parties. Hello Barbie, Toymail, Smart Toy Monkey, CogniToys Dino, Edwin the Duck, and Anki Cozmo provide full *Parental-PII-control*. Seven toys claim to take security measures for *PII-protection*, two toys do not state exactly which measures they take to protect PII, and two others do not provide any information. Four toys provide a dedicated webform/email address to contact the company in case of any privacy concern about their toys; two of those are *Protection-program-participant* in TRUSTe or JAMS. Hello Barbie is the only toy that is *Bug-bounty-participant*, which may help discover security and privacy flaws in the toy. None of the toys' websites (except Sphero BB-8 partially) respect DNT.

5 RELATED WORK

Natural language privacy policies have long been the standard form of notification to users about privacy implications of a service. However, their length and complexity put extra burden on the users' who rarely read and understand them. Identifying the best format to represent privacy implications is non-trivial. Earlier work in this domain has largely been focused on proposing alternatives, or quantifying data practices from legacy privacy policies. Several studies (e.g., [1, 32]) utilize Natural Language Processing (NLP) techniques to identify important data collection practices from privacy policies. Sadeh et al. [32] leverage advances in NLP and machine learning techniques in combination with crowd-sourcing to extract key privacy information from privacy policies, and then present the policies in a user-friendly manner.

Costante et al. [8] propose a solution using Information Extraction (IE) techniques to analyze website privacy policies regarding what data about a visitor is collected. Zimmeck et al. [41] propose a system to automatically examine compliance of Android apps with their privacy policies, by performing static analysis of Android apps and extracting privacy information from their policies. They found that 71% of the apps that do not provide a privacy policy, but collect at least one PII item, and the ones with privacy policies show significant inconsistencies between policies and actual app (code) behavior. Our work is based on careful manual analysis of available privacy policy and terms of use documentation as the number of toys/apps we analyze is limited.

Earlier research analyzed privacy policies to infer data practices in more generic cases, without taking the target user base into consideration. The Explore Privacy Policies project [29] highlights privacy practices of websites. Hoke et al. [18] study privacy

policies of 75 tracking companies to examine compliance with self-regulatory guidelines. Costante et al. [9] assess the completeness of privacy policies by comparing them against a set of privacy categories. Cranor et al. [10] utilize web crawling and document parsing to analyze *model* privacy forms of a large number of financial institutions, and found many instances where users' right to control the sharing of information was violated. Various studies focus on privacy of Android apps in general. Kong et al. [22] propose a system called AUTOREB that maps reviews of Android apps to security and privacy behaviors. Zhang et al. [40] attempt to generate security related app description by analyzing the app code.

Another line of work explores the design of user-friendly privacy policy interfaces and formats that would facilitate users' understanding of data practices (e.g., [19, 21, 30, 38]). Kelley et al. [21] develop a solution inspired by nutrition labels that represents the information collection practices in a grid view. Holtz et al. [19] propose the use of privacy icons in addition to the written policies to express data practices in a more effective way.

Several studies have found serious privacy and security issues in connected toys (see e.g., [12, 33]). Security analysis of Hello Barbie reveals several loopholes in its security mechanism [33], including an unencrypted WiFi network used to configure the toy. McReynolds et al. [25] study the expectations and concerns of both parents and children regarding the use of connected smart toys. A report from Future Privacy Forum [16] explores privacy concerns related to microphone-enabled devices, including smart toys such as Hello Barbie, and suggests best practices for devices equipped with microphone. Yankson et al. [39] discuss privacy implications of connected smart toys and propose some best practices that could be embraced by both parents and toy companies.

In our framework, we complement existing research and highlight key privacy features that reflect the privacy practices in smart toys. We adapt several privacy features from the Explore Privacy Policies website [29] (part of [32]). In addition to the generic privacy features, we define several criteria in our framework that are tailored for smart toys. In contrast to privacy studies targeting the general population, we focus on privacy implications of a very sensitive user base, i.e., children.

6 CONCLUSION AND FUTURE WORK

We present a comprehensive framework for evaluating privacy practices of smart toys – to help us better understand their policies and to be able to compare them. We use our framework to analyze a representative set of 11 smart toys and their companion apps. We believe it can help evaluate other smart toys in the market (with possible extension and refinement). We found several issues in the privacy practices of these smart toys, especially in regards to PII collection, third-party data sharing, web tracking, and data storage location. We augment our policy analysis by statically analyzing the toys' companion apps to determine over-privileges, sensitive PII collection and suspicious behaviors. We found that all the companion apps are over-privileged and collect unnecessary personal information. Our static analysis provides evidence of potential suspicious activities of the companion apps, such as abusing the telephony service. We believe that our framework can facilitate quick and effective comparison of smart toys privacy practices in future, and be useful to parents, law-makers and toy manufacturers.

We emphasize that our evaluation here is mostly analytical, based on available privacy policies and terms of use documents. A toy may appear to conform to privacy best practices according to its documentation, but may fail to implement necessary technical measures. For validation of stated privacy practices, more experimental evaluation is necessary (e.g., perform dynamic analysis of apps, analyze behaviors of toys when in actual use). Such evaluation also need to be automated for better scalability (as opposed to our current manual static analysis).

ACKNOWLEDGMENTS

We are grateful to anonymous STAST 2017 reviewers for their comments and suggestions. This work is supported by a grant from the Office of the Privacy Commissioner of Canada (OPC) Contributions Program.

REFERENCES

[1] Manar Alohaly and Hassan Takabi. 2016. Better privacy indicators: a new approach to quantification of privacy policies. In *Symposium on Usable Privacy and Security (SOUPS'16)*. Denver, CO, USA.
[2] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie. 2012. PScout: analyzing the Android permission specification. In *ACM conference on Computer and Communications Security (CCS'12)*. Raleigh, NC, USA.
[3] Justin Brookman, Phoebe Rouge, Aaron Alva, and Christina Yeung. 2017. Cross-device tracking: measurement and disclosures. *Privacy Enhancing Technologies* (2017).
[4] Federal Trade Commission. 2012. Mobile apps for kids: current privacy disclosures are disappointing. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf. (Feb. 2012).
[5] Federal Trade Commission. 2012. Mobile apps for kids: disclosures still not making the grade. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf. (Dec. 2012).
[6] Federal Trade Commission. 2015. Children's Online Privacy Protection Rule ("COPPA"). (2015). https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[7] Federal Trade Commission. 2015. Kids' apps disclosures revisited. https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited. (Sept. 2015).
[8] Elisa Costante, Jerry den Hartog, and Milan Petković. 2013. What websites know about you. In *Data Privacy Management and Autonomous Spontaneous Security*. Lecture Notes in Computer Science, vol 7731.
[9] Elisa Costante, Yuanhao Sun, Milan Petković, and Jerry den Hartog. 2012. A machine learning solution to assess privacy policy completeness (short paper). In *ACM Workshop on Privacy in the Electronic Society (WPES'12)*. Raleigh, NC, USA.
[10] Lorrie Faith Cranor, Kelly Idouchi, Pedro Giovanni Leon, Manya Sleeper, and Blase Ur. 2013. Are they actually any different? Comparing thousands of financial institutions' privacy practices. In *Workshop on the Economics of Information Security (WEIS'13)*. Washington, DC, USA.
[11] CTVNews. 2014. Children becoming targets of identity theft. (2014). News article (Mar. 26, 2014). http://www.ctvnews.ca/canada/children-becoming-targets-of-identity-theft-1.1748056.
[12] Danielle L Dobbins. 2015. *Analysis of security concerns and privacy risks of children's smart toys*. Ph.D. Dissertation. Washington University St. Louis, St. Louis, MO, USA.
[13] European Union. 2016. General data protection regulation. http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. (April 2016).
[14] Export.gov. 2017. U.S.-EU & U.S.-Swiss safe harbor frameworks. (2017). https://www.export.gov/safeharbor
[15] Campaign for a Commercial Free Childhood. 2015. Hell no Barbie: 8 reasons to leave Hello Barbie on the shelf. http://www.commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf. (2015).
[16] Stacy Gray. 2016. Always on: privacy implications of microphone-enabled devices. In *Future of privacy forum*. https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf

[17] HackerOne. 2017. ToyTalk: bug bounty program - get rewards through HackerOne. (2017). https://hackerone.com/toytalk
[18] Candice Hoke, Lorrie Faith Cranor, Pedro Giovanni Leon, and Alyssa Au. 2015. Are they worth reading? An in-depth analysis of online trackers' privacy policies. *I/S: a journal of law and policy for the information society* (2015). http://engagedscholarship.csuohio.edu/fac_articles/783/
[19] Leif-Erik Holtz, Katharina Nocun, and Marit Hansen. 2010. Towards displaying privacy information with icons. In *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life*.
[20] JAMS. 2017. JAMS mediation, arbitration, ADR services. https://www.jamsadr.com/. (2017).
[21] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. 2009. A nutrition label for privacy. In *Symposium on Usable Privacy and Security (SOUPS'09)*. Mountain View, CA, USA.
[22] Deguang Kong, Lei Cen, and Hongxia Jin. 2015. AUTOREB: Automatically understanding the review-to-behavior fidelity in Android applications. In *ACM Conference on Computer and Communications Security (CCS'15)*. Denver, CO, USA.
[23] Andreas Kurtz, Hugo Gascon, Tobias Becker, Konrad Rieck, and Felix Freiling. 2016. Fingerprinting mobile devices using personalized configurations. *Privacy Enhancing Technologies* (2016).
[24] Maaaaz. 2013. Androwarn. (Mar 2013). https://github.com/maaaaz/androwarn
[25] Emily McReynolds, Sarah Hubbard, Timothy Lau, Aditya Saraf, Maya Cakmak, and Franziska Roesner. 2017. Toys that listen: a study of parents, children, and internet-connected toys. In *ACM Conference on Human Factors in Computing Systems (CHI'17)*. Denver, CO, USA.
[26] Alessio Merlo and Gabriel Claudiu Georgiu. 2017. RiskInDroid: machine learning-based risk analysis on Android. In *IFIP International Conference on ICT Systems Security and Privacy Protection*.
[27] Motherboard.Vice.com. 2015. One of the largest hacks yet exposes data on hundreds of thousands of kids. (2015). News article (Nov. 27, 2015). https://motherboard.vice.com/en_us/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids.
[28] Bill Nelson. 2016. Children's connected toys: data security and privacy concerns. (2016). Technical report (Dec. 14, 2016). US Senate Committee on Commerce, Science, and Transportation. https://www.hsdl.org/?view&did=797394.
[29] The Usable Privacy Policy Research Project. 2016. Usable privacy. (2016). https://explore.usableprivacy.org/
[30] Robert W Reeder, Patrick Gage Kelley, Aleecia M McDonald, and Lorrie Faith Cranor. 2008. A user study of the expandable grid applied to P3P privacy policy visualization. In *ACM Workshop on Privacy in the Electronic Society (WPES'08)*. Alexandria, VA, USA.
[31] Juniper Research. 2017. Smart toy sales to grow threefold to exceed $15.5 billion by 2022. (2017). https://www.juniperresearch.com/press/press-releases/smart-toy-sales-to-grow-threefold
[32] Norman Sadeh, Alessandro Acquisti, Travis D. Breaux, Lorrie Faith Cranor, Aleecia M. McDonald, Joel R. Reidenberg, Noah A. Smith, Fei Liu, N. Cameron Russell, Florian Schaub, and Shomir Wilson. 2013. *The usable privacy policy project*. Technical Report CMU-ISR-13-119. Carnegie Mellon University. http://reports-archive.adm.cs.cmu.edu/anon/isr2013/CMU-ISR-13-119.pdf
[33] Somerset Recon, Inc. 2016. Hello barbie security analysis. https://static1.squarespace.com/static/543effd8e4b095fba39dfe59/t/56a66d424bf1187ad34383b2/1453747529070/HelloBarbieSecurityAnalysis.pdf. (Jan. 2016).
[34] Emmeline Taylor and Katina Michael. 2016. Smart toys that are the stuff of nightmares. *IEEE Technology and Society Magazine* (2016).
[35] TheGuardian.com. 2017. CloudPets stuffed toys leak details of half a million users. (2017). News article (Feb. 28, 2017). https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults.
[36] TheGuardian.com. 2017. German parents told to destroy doll that can spy on children. (2017). News article (Feb. 17, 2017). https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children.
[37] TRUSTe. 2017. Submit a report - watchdog. (2017). https://feedback-form.truste.com/watchdog/request
[38] World Wide Web Consortium (W3C). 2007. P3P: The platform for privacy preferences. (2007). https://www.w3.org/P3P/
[39] Benjamin Yankson, Farkhund Iqbal, and Patrick CK Hung. 2017. Privacy preservation framework for smart connected toys. In *Computing in Smart Toys*.
[40] Mu Zhang, Yue Duan, Qian Feng, and Heng Yin. 2015. Towards automatic generation of security-centric descriptions for Android apps. In *ACM Conference on Computer and Communications Security (CCS'15)*. Denver, CO, USA.
[41] Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven M Bellovin, and Joel Reidenberg. 2017. Automated analysis of privacy requirements for mobile apps. In *Network and Distributed System Security Symposium (NDSS'17)*. San Diego, CA, USA.

A SELECTED SMART TOYS AND POLICY LINKS

We briefly describe the smart toys analyzed in our study. Most of these toys are equipped with several hardware sensors that enable them to observe and record their surroundings, especially their interactions with children. They are also accompanied by a mobile application that can be used to configure or control their activities.

Hello Barbie: An interactive toy that tells stories and engages in real-time conversations with children.

Toymail: A toy that enables parents and children to exchange voice messages in a playful manner.

Sphero BB-8: Inspired by the fictional droid set named BB-8 from Star Wars, Sphero BB-8 can move around on its own in patrol mode or be controlled by a companion app.

Wowwee Chip: A robot dog equipped with advanced sensors that allow it to adapt its behavior based on its surroundings.

Smart Toy Monkey: An interactive learning toy that adapts itself to develop new adventures for the children as they continue to play with it. *CogniToys Dino:* Powered by IBM Watson and Friendgine technology, CogniToys Dino can interact with children by telling stories, make them laugh by cracking jokes and playing games.

Edwin the Duck: A toy duck that tells interactive stories, sings and plays stimulating games via the companion app.

Anki Cozmo: An interactive robot that sings, plays games and observes its surroundings. This Artificial Intelligence (AI) powered toy offers new features as it interacts more with the children.

My Friend Cayla: A doll that utilizes speech recognition technology and Internet connectivity to answer questions on various topics.

I-Que Robot: An intelligent robot that responds to queries, dances on music and allows children to have real-time conversations with the toy.

Zenbo: A smart robot that can roam around the house taking photos, making video calls and playing songs. It can tell entertaining stories to children.

Table 7: Links to toys' privacy policies and terms of use

Product	Policy link	ToU link
Hello Barbie	https://www.toytalk.com/hellobarbie/privacy	https://www.toytalk.com/hellobarbie/terms
Toymail	https://toymail.co/pages/privacy	https://toymail.co/pages/terms
Sphero BB-8	http://www.sphero.com/privacy	http://www.sphero.com/terms
Wowwee Chip	http://wowwee.com/information/privacy	http://wowwee.com/information/warranty
Smart Toy Monkey	http://www.smarttoy.com/privacy	http://www.smarttoy.com/terms
CogniToys Dino	https://cognitoys.com/pages/privacy	https://cognitoys.com/pages/terms
Edwin the Duck	http://www.edwintheduck.com/privacy-policy	http://www.edwintheduck.com/terms-and-conditions
Anki Cozmo	https://www.anki.com/en-ca/company/privacy	https://www.anki.com/en-ca/company/terms-and-conditions
My Friend Cayla	https://www.myfriendcayla.com/privacy-policy	http://myfriendcayla.co.uk/terms
I-Que Robot	http://ique-robot.co.uk/privacy	http://ique-robot.co.uk/terms-conditions
Zenbo	https://www.asus.com/Terms_of_Use_Notice_Privacy_Policy/Privacy_Policy	https://www.asus.com/Terms_of_Use_Notice_Privacy_Policy/Privacy_Policy