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_ossen,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 have also 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

ACM Reference Format:

1 INTRODUCTION
Smart toys are gaining popularity in recent times with a rapid growth in sales every year. 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...
The US Federal Trade Commission (FTC) has conducted several various privacy aspects of smart toys. In particular, we define 17 More experimental validation is needed beyond our preliminary adherence to COPPA, strong security measures at the server-side (e.g., lack of collecting home addresses), or provide false information (e.g., these policies may omit important information (e.g., no mention of companions, strong security measures at the server-side).

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.

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.

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

<table>
<thead>
<tr>
<th>Devices and Sensors</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microphone</td>
<td>Speaker</td>
</tr>
<tr>
<td>Hello Barbie</td>
<td>✓</td>
</tr>
<tr>
<td>Toymail</td>
<td>✓</td>
</tr>
<tr>
<td>Sphero BB-8</td>
<td>✓</td>
</tr>
<tr>
<td>Wowwee Chip</td>
<td>✓</td>
</tr>
<tr>
<td>Smart Toy Monkey</td>
<td>✓</td>
</tr>
<tr>
<td>CogniToys Dino</td>
<td>✓</td>
</tr>
<tr>
<td>Edwin the Duck</td>
<td>✓</td>
</tr>
<tr>
<td>Anki Cozmo</td>
<td>✓</td>
</tr>
<tr>
<td>My Friend Cayla</td>
<td>✓</td>
</tr>
<tr>
<td>I-Que Robot</td>
<td>✓</td>
</tr>
<tr>
<td>Zenbo</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 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 Sadegh 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 as 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; see also EU e-Privacy Directive1 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


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 JANS 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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Barbie</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Toymail</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sphero BB-8</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Wowwee Chip</td>
<td>●</td>
<td>○</td>
<td>N/A</td>
<td>N/A</td>
<td>●</td>
<td>N/A</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Smart Toy Monkey</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>CogniToys Dino</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Edwin the Duck</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Anki Cozmo</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>My Friend Cayla</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>N/A</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>I-Que Robot</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
<td>N/A</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Zenbo</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>N/A</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>□</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

● = 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

<table>
<thead>
<tr>
<th>Product</th>
<th>Data Access</th>
<th>Communication</th>
<th>Functionalities</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Photos, Media, Files and Storage</td>
<td>USB storage</td>
<td>Contacts</td>
<td>View WiFi connections</td>
</tr>
<tr>
<td>Hello Barbie</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Toymail</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sphero BB-8</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wowwee Chip</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Smart Toy Monkey</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CogniToys Dino</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Edwin the Duck</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Anki Cozmo</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>My Friend Cayla</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>I-Que Robot</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Zenbo</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Hello Barbie 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-participat and prohibits any attempts for reverse engineering, decompiling, or discovering the source code.
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...
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 parties 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 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 collects 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. Zimeck 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
We present a comprehensive framework for evaluating privacy with microphone. Yankson et al. \cite{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 \cite{29} (part of \cite{32}). In addition to the general 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


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.

**Sphereo BB-8:** Inspired by the fictional droid set named BB-8 from Star Wars, Sphereo 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, making 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

<table>
<thead>
<tr>
<th>Product</th>
<th>Policy link</th>
<th>ToU link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toymail</td>
<td><a href="https://toymail.co/pages/privacy">https://toymail.co/pages/privacy</a></td>
<td><a href="https://toymail.co/pages/terms">https://toymail.co/pages/terms</a></td>
</tr>
<tr>
<td>My Friend Cayla</td>
<td><a href="https://www.myfriendcayla.com/privacy-policy">https://www.myfriendcayla.com/privacy-policy</a></td>
<td><a href="http://myfriendcayla.co.uk/terms">http://myfriendcayla.co.uk/terms</a></td>
</tr>
<tr>
<td>I-Que Robot</td>
<td><a href="http://ique-robot.co.uk/privacy">http://ique-robot.co.uk/privacy</a></td>
<td><a href="http://ique-robot.co.uk/terms-conditions">http://ique-robot.co.uk/terms-conditions</a></td>
</tr>
</tbody>
</table>