No Transparency for Smart Toys

Julika Feldbusch[0009−0002−0299−0602], Valentyna Pavliv[0009−0007−0342−350X], Nima Akbari[0009−0004−0962−903X], and Isabel Wagner[0000−0003−0242−6278]

University of Basel, Spiegelgasse 1, 4054 Basel, Switzerland
julika.feldbusch@stud.unibas.ch, valentyna.pavliv@unibas.ch, nima.akbari@unibas.ch, isabel.wagner@unibas.ch
https://pet.dmi.unibas.ch/en/

Abstract. Smart toys combine traditional playtime with modern technologies, integrating IoT features like communication, computation, and sensing to create interactive toys that respond to their environment, offering children new options for entertainment and playful education. However, despite well-documented privacy and security shortcomings of IoT devices, there are no recent studies on the privacy and security properties of smart toys. This is critical because children are a particularly vulnerable group whose personal data merits special protection. In this paper, we therefore examine 12 smart toys available in the EU market with regard to their security, privacy, and transparency. Our main findings include widespread behavioral profiling of children via toy analytics data and a lack of transparency due to insufficient and not easily accessible information about data collection and processing.

Keywords: Smart toys · Transparency · Privacy · Security · GDPR.

1 Introduction

In 2015, the Hello Barbie doll was released as the first toy that children could speak with in a meaningful way, thanks to a direct connection to a remote server running speech processing software [30]. The Hello Barbie servers stored each doll's conversation history, which enabled the doll to build conversations based on previous interactions. Hello Barbie was one of the first in a generation of *smart toys*: toys with communication, computation, and sensing capabilities similar to other Internet of Things (IoT) devices. Concerns by parents were followed by a series of academic studies that detailed the security and privacy issues with Hello Barbie [7, 23, 32]. Subsequently, Mattel discontinued Hello Barbie in 2017.

Since the scandals about Hello Barbie and a similar doll, My Friend Cayla, we are not aware of major public scandals involving other smart toys. One reason for this could be the adoption of the General Data Protection Regulation (GDPR) [17] in 2016, which set strict rules for data protection and privacy. However, questions remain about how rigorously these regulations are applied to children's toys.

Privacy and data protection are especially important for products aimed at children because children's play time is essential for development as a human

being [4, 56], and pervasive surveillance by cameras and microphones in toys is detrimental to this process. Importantly, the degree of surveillance that a child is exposed to should not depend on well-informed and privacy-conscious parents who are able to judge the implications of pervasive surveillance.

Although numerous smart toys are available on the market today, we are not aware of recent studies that investigate their privacy or security. In this paper, we close this gap by rigorously examining 12 smart toys, aiming to understand to what extent the security, privacy, and transparency properties of currently available toys have improved, following the European Telecommunications Standards Institute (ETSI) *Cybersecurity for Consumer IoT* [16] standard as guideline. We purchase a diverse selection of 12 toys and evaluate their *security properties* by examining encrypted and unencrypted traffic, cipher suites and TLS versions, as well as Wi-Fi security; *privacy properties* by analyzing the transmitted data and requested application permissions, by decrypting the traffic or inspecting the application's code; *transparency properties* by inspecting privacy policies and sending subject access requests as well as data deletion requests. We also briefly comment on the toys' likely *compliance* with the GDPR and the upcoming Cyber Resilience Act (CRA). Our main findings are:

1. *Security* is addressed well overall, even though most toys still use TLS 1.2 encryption and only some use forward-secrecy cipher suites. In local networks no data traffic is encrypted, resulting into an insecure Wi-Fi setup for toy devices without user interface. None of our toys specify a hardware/software support period, and some toys even state that they may discontinue service without notice.
2. *Privacy* protections are generally insufficient. Most toys collect extensive analytics data combined with unique identifiers, subjecting children to pervasive behavioral profiling. In addition, the required permissions of companion apps are often unnecessary and sensitive, such as access to location, contacts, or the microphone.
3. *Transparency* suffers from well-known usability issues of privacy policies. The process for sending a subject access request is often too complicated. In addition, only 43% of toys vendors respond to our subject access request within the one month period allowed by GDPR, with one providing incomplete information. None of the toys provide accessible information about security, security issues, or software updates in their user interface.
4. *Compliance* with the GDPR is only partial. At the very least, the availability and comprehensiveness of privacy policies are insufficient. Vendors are also not yet meeting the requirements of the recently approved CRA and may have to improve their processes before the act takes effect.

Based on these findings, we strongly recommend that toy makers prioritize privacy and security, following best practices in security and privacy engineering, to act responsibly towards their young target audience. Subject access requests and data deletion requests should be easier for users and their processing should ideally be automated. Consent should be acquired on an opt-in basis, instead

of the default opt-out. It should also be more fine-grained, allowing users to disagree selectively with parts of privacy policy.

The research community and regulators could also do more to support toy makers, for example by standardizing privacy/transparency labels for toy packages, similar to well-known nutrition labels [12, 44, 11].

2 Related Work

IoT security. Security approaches for IoT devices have to balance security, performance, and resource constraints. Achieving the right trade-off between these factors is a significant challenge, especially given that traditional security practices were optimized for desktop and server environments [33, 36].

The two most pressing concerns in IoT security are authentication and encryption. These aspects are essential for safeguarding sensitive data and ensuring secure communications within the IoT ecosystem [47]. Today, most traffic from IoT devices is encrypted, however, data is frequently sent to third-party services and to different geographic regions, which leads to information exposure [45]. Although the connection may be encrypted with the Transport Layer Security (TLS) protocol, the implementation needs to be secure, using strong cipher suites, certificates and protocols. Still, many consumer IoT products lack a secure implementation of TLS, for example by using outdated cipher suites, offering attack surfaces on the connection [41]. Companion apps are often used to control IoT devices or to provide internet connectivity via Wi-Fi or Bluetooth. These apps may also be a security risk, as they may expose user data without proper disclosure [34], use abandoned domains or hard-coded credentials [48]. To determine which data is sent, the TLS encryption of the companion apps to the services can be decrypted using Man-in-the-Middle (MitM) attacks [52] as many vendors have insufficient countermeasures in place [39].

Transparency. Current literature on transparency mainly addresses the lack of transparency in privacy requirements [6, 13, 57], but does not extend to broader cybersecurity metrics. Some studies have proposed the implementation of transparency labels on devices to provide users with a quick overview of basic privacy status [44, 12]. Extending this concept, the idea of labeling could include basic cybersecurity parameters. However, it is important that such labels strike a balance between providing sufficient information for informed decision-making and avoiding overwhelming consumers with excessive detail [37]. Therefore, transparency labels should be designed to be easily understood by non-technical users, while still providing meaningful information.

Children's rights. Children are a particularly vulnerable group that deserves special protection [53]. Especially in the context of online privacy, safeguards for children are being addressed by current legislation. For example, the GDPR in the European Union (EU) provides privacy protections with a focus on parental consent [29]. Recital 38 of the GDPR specifically states that "Children merit

specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned" [17].

Smart Toys security and privacy. Privacy and security of smart toys have been analyzed through both legislative and experimental approaches. Legal studies have found that privacy and security legislation in the EU as well as in North America [23, 21, 50] does not sufficiently ensure IT security and is difficult to enforce, as many vendors interpret the applicable laws as vaguely as possible. For users of toys, this often means that the toy manufacturers' privacy policies lack clarity or omit information regarding how their toys protect users' security and privacy [7].

Experimental studies have uncovered vulnerabilities primarily caused by a lack of encryption and authentication of Hypertext Transfer Protocol (HTTP) sessions, constant data storage and the disclosure of personal data to third-parties in crash reports [8]. These vulnerabilities lead to privacy policy violations and easily exploitable toys which expose children to various threats, whether through physical, nearby, or remote access to the toy [49]. The identified risks include manipulating a toy's movements or issuing instructions to a child, leading them into dangerous situations. Toys that are disclosing personal information could be turned into spies if exploited as passive sensitive data collectors.

These studies highlight significant shortcomings in cybersecurity and privacy of smart toys. However, it is worth noting that these studies focus mainly on toys which are no longer on the market. Notable examples include the Hello Barbie doll, which was discontinued due to numerous vulnerabilities leading to the potential disclosure of personal data [30, 49, 5], and the My Friend Cayla doll, which was banned by German authorities due to concerns about a hidden camera and microphone [3, 5].

Notably, these experimental studies have been published more than five years ago, with very little work in recent years. However, this most likely does not indicate that the privacy and security issues with smart toys have all been resolved. For example, a recent blog post revealed severe security issues on an educational robot, without disclosing the robot's brand [19]. The uncovered vulnerabilities included APIs that allow stealing of sensitive information, guessable robot identifiers that enable targeted calls to any robot, and remote code execution during the update process.

In this study, we aim to close this gap in research on smart toys and analyze the security, privacy, and transparency properties of toys available for purchase in late 2023.

3 Methodology

We follow a three-step methodology to evaluate smart toys with respect to their privacy and security. First, we select and purchase a number of smart toys (Section 3.1). Second, we develop a set of evaluation criteria based on the *ETSI Cybersecurity for Consumer IoT* standard (Section 3.2). Finally, we select and implement technical methods that allows to evaluate our criteria (Section 3.3).

3.1 Smart Toys Market and Selection

We select 12 smart toys from the *Toys* category on amazon.de, opting for this marketplace due to its large product range, position in the EU market, and availability of English language information on all toys. We aim for a diverse selection of toys based on their game mechanisms and *smart* features. Regarding connectivity, we only select toys equipped with Wi-Fi capabilities. Among these, eight toys come with built-in connectivity, while four toys use a companion app to access connectivity. Five of these toys are made by well-known toy companies and six by startups. In terms of location, five of the toy vendors are from Europe, four from the United States, and three from Asia. In Table 1 the purchased toys are presented. None of the toys are having artificial intelligence (AI) features because none were available on the EU market when we purchased the toys in October 2023. However, since then several new AI-powered smart toys have become available [27, 22, 10, 31] which we aim to study in future work.

3.2 Criteria

To evaluate the security, privacy and transparency properties of smart toys, we follow the *ETSI Cybersecurity for Consumer IoT* [16] standard as a reference. However, due to space constraints, we only present subset of these criteria which represent the key findings of our examination.

Cybersecurity. We evaluate the encryption of connections to external servers and on the local network. By capturing the traffic, we investigate whether the connection is encrypted, and if so, what TLS versions and cipher suites are being used. Then we look at the process of initializing a Wi-Fi connection. Since not all toy devices contain user interfaces and open their own local Wi-Fi network, we verify whether encryption is used, and if not, we try to eavesdrop on the connection to retrieve the transmitted data and Wi-Fi credentials. Moreover, we examine the vendor's website, user manual, and terms and conditions to find information about minimum hardware and software support periods.

Privacy. To assess the state of children's privacy on the toys, we first evaluate what personal data is sent to which service, by decrypting the data connections from the companion apps to external servers. We then assess the necessity of sending this data, check for the use of known trackers by reviewing the app's codebase and captured network traffic, and examine the destination countries of outgoing traffic. Additionally, we check whether the apps are sending the device's Google Ad ID. In a last step, we obtain the permissions requested by companion apps, by reviewing the app's manifest, and evaluate if the apps request only permissions that are required for their functionality.

Transparency. In order to assess adequate user transparency on data collection and use, we send subject data access requests to all vendors on which we have a user account with an e-mail address (7 of the 12 toys). In addition we evaluate the

Table 1. Overview of the 12 toys in our study.

Toy	Description	IoT	App	Vendor	Country	Size
Edurino	Learning app with figurine and pen	-	✓	Edurino	DE	●
Kidibuzz	Smartphone for children with parental control	✓	✓	VTech	HK	⬤
Moorebot	Moving and patroling robot with camera and microphone	✓	✓	Pilot Laboratories	US	●
Children's Camera	Camera with direct printing	✓	✓	unknown	CN	?
Osmo	Learning app with building blocks and camera reflector	-	✓	Tangible Play	US	●
Pictionary Air	Video-capturing drawing app with flashlight stylus	-	✓	Mattel	US	⬤
Tamagotchi Uni	Virtual pet which can be carried around on wrist	✓	-	Bandai Namco	JP	⬤
Tigerbox	Speaker with touchscreen	✓	✓	Tigermedia	DE	●
Tiptoi	Charging station + pen, with audio content for picture books	✓	-	Ravensburger	DE	⬤
Toniebox	Speaker with NFC figurine	✓	✓	Tonies	DE	●
Twister Air	Video-capturing dancing app with wrist bands	-	✓	Hasbro	US	⬤
Winky	Non-moving robot with gyroscope, program and play	✓	✓	Mainbot	FR	●

availability and comprehensiveness of privacy policies, focusing on information on data collection and transmission. We also evaluate the information presented in user interfaces, regarding software updates, version numbers, and consent and withdrawal options regarding data processing, storage and transmission.

Compliance. In the last category, we read the EU legislation regarding data protection (GDPR) and align our results with an assessment on compliance to this piece of legislation. Furthermore, we evaluate if the upcoming Cyber Resilience Act in the current version, would change the current state of smart toys, and preview the potential changes and improvements it could bring.

3.3 Technical Methodology

To assess the criteria presented above, we used a range of technical methods: decrypting and eavesdropping on network traffic, static analysis of the companion

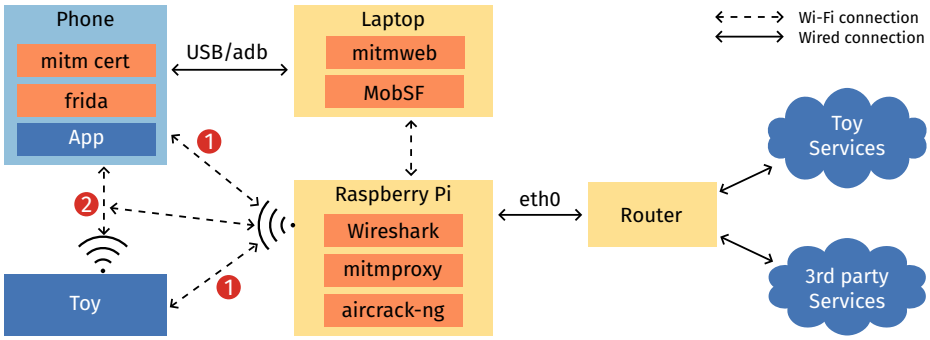

Fig. 1. Setup for network traffic analysis. The toy and its companion app connect to the Wi-Fi provided by the Raspberry Pi ❶, which forwards the traffic to the router via an Ethernet connection. Some toys also use a direct Wi-Fi connection to the phone ❷. The Raspberry Pi runs `Wireshark` to capture all traffic, `aircrack-ng` to sniff traffic between the toy and the phone, and `mitmproxy` to decrypt the traffic. The laptop connects to the phone with USB to install the `mitmproxy` certificate and the `Frida` server, and to perform static analysis with `MobSF`.

apps, network traffic evaluation, and Wi-Fi sniffing. Figure 1 gives an overview of our setup.

Wi-Fi Sniffing. Some toys communicate with their companion app or a local web server instead of (or in addition to) accessing the internet directly. To analyze this network traffic, we use a Raspberry Pi with `aircrack-ng` [35] and `Wireshark`. To filter out unrelated traffic, we specify the channel and BSSID of the local Wi-Fi. When the local Wi-Fi network uses WPA2 encryption with a password, `Wireshark` can decrypt the traffic after entering the raw WPA PSK key, which can be generated on the `Wireshark` website [62].

Decryption of network traffic. To intercept and decrypt TLS traffic between companion apps and the internet, we perform a Man-in-the-Middle (MitM) attack using `mitmproxy` [9]. To achieve this, the app must (1) trust the certificate of the MitM attacker and (2) not use a hardcoded certificate for the remote server (SSL pinning).

To ensure that apps trust the mitmproxy certificate, we install the certificate on the phone and transfer it from the user-trusted to the system-trusted certificates folder. We use a rooted phone to enable global installation of the mitmproxy certificate.

To bypass SSL pinning, we use `Frida`, a tool for dynamic code instrumentation [40]. Instead of injecting the `Frida` server into companion apps via app patching, we opted to run the `Frida` server directly on the phone. This approach allows us to easily execute scripts that modify the applications, to bypass their SSL pinning code [42]. Once more, we use our rooted phone to gain the superuser access necessary for this.

In the `mitmweb` user interface of `mitmproxy`, we can then examine the decrypted data and save it in an `har` (HTTP Archive) file for further analysis.

Static analysis. We used static analysis based on the Mobile Security Framework `MobSF` [1] to analyze the requested permissions and trackers embedded in the toys' companion apps. `MobSF` provides vulnerability assessment, evaluates trackers and permissions, and summarizes metadata.

In addition to the automated `MobSF` evaluation, we also conducted a manual assessment by inspecting the apps' `Java` code. To navigate the large code bases efficiently, we searched for strings that reveal information about encoding (*encode, decode, base64, utf-8, H264, H265, png, gif, jpeg*), encryption and hashing (*encrypt, decrypt, TLS, AES, hash, SHA, MD5*), authentication (*password, pwd*), and the Google Ad ID (*advertise, gaid, ad_id*).

Network Traffic Analysis. To capture the network traffic from companion apps and toys, we use `Wireshark` [61]. For each toy, we start `Wireshark` data capture, activate the device and/or launch the companion app, log in if required, start a game, and perform typical user interactions for 2–10 minutes. Finally, we shut down all processes and end the data capture. A `python` script is used to filter and summarize the captured traffic. First, we filter out any traffic that does not involve the phone or toy, based on their IP addresses. Then, we aggregate incoming and outgoing messages to specific servers. We resolve server IP addresses to server names, hosting providers and geolocations using the `geolocation-db` [54] API and manual lookups [24]. To assess encryption with TLS, we parse the `Client Hello` messages to extract available TLS cipher suites. We cross-reference these suites with cryptographic security evaluations provided by an Ciphersuite Info API [46] and evaluate the negotiated TLS cipher suite. On the server side, we list available cipher suites using `SSL Labs` [43].

4 Results

In this section we present our findings regarding the cybersecurity, privacy, transparency and compliance of the 12 selected toys. Table 2 summarizes the results.

4.1 Security

Communication. For connections outside the local network to the internet, most toys establish secure communication channels to servers via TLS and HTTPS using secure TLS cipher suites, even though most toys still use TLS 1.2 instead of TLS 1.3. Although the Tigerbox encrypts traffic for most servers, traffic to the firmware update server remains unencrypted. While the update itself is encrypted, reducing the risk of firmware exposure or malicious modification, it may allow for offline attacks against firmware updates or the encryption mechanism. Tiptoi also sends data over HTTP without encryption. Although the transmitted

Table 2. Overall results for each criterion and each toy. Red triangles (▲) indicate deficiencies, vulnerabilities, or inadequacies; yellow squares (■) indicate some improvements or partial fulfillment of the criterion; blue circles (●) indicate that the toy fulfills the criterion well. A dash (-) indicates that the criterion is not applicable to the toy.

	Edurino	Kidibuzz	Camera	Moorebot	Osmo	Pictionary	Tamagotchi	Tigerbox	Tiptoi	Toniebox	Twister	Winky
Security												
Global network traffic encrypted	●	●	-	■	●	●	●	●	▲	■	●	●
Local network encryption	-	-	▲	■	-	-	■	-	▲	▲	-	-
Wi-Fi setup	-	●	-	■	-	-	■	●	▲	▲	-	-
SW & HW support periods	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	▲
Privacy												
Processing minimum necessary	▲	■	●	■	▲	■	■	●	●	■	■	■
Number of trackers	1	-	0	2	1	3	-	1	-	4	2	0
Location of server	■	■	-	▲	■	■	■	■	●	■	▲	■
Only necessary app permissions	●	-	▲	▲	▲	■	-	●	-	▲	■	■
Transparency												
Subject data access requests	▲	▲	-	▲	■	-	-	●	-	●	-	▲
Privacy policy: Transparent info about data	●	■	▲	▲	■	■	■	■	■	●	●	■
Privacy policy: Consent and withdrawal	●	●	▲	▲	●	■	●	●	●	●	■	●
UI: Updates available	●	■	■	●	●	●	●	●	●	●	●	●
UI: Info about risks/disruptions	■	▲	■	■	■	■	▲	●	■	■	■	■
UI: Model and version designation	▲	●	▲	■	▲	●	●	●	■	●	●	■

data mainly involves audio file downloads and updates, which may not contain sensitive information, passive observers may be able to profile usage of the toy.

Communication from the Moorebot robot appears to be `RTMP` encoded rather than encrypted, though decoding attempts were unsuccessful. The Toniebox encrypts data to servers using TLS, but uses a weak TLS cipher suite (using SHA1 and the AES in the Cipher Block Chaining (CBC) mode, which are considered insecure in TLS 1.3). The Toniebox server only supports cipher suites which are classified as "weak", whereas the Toniebox device supports "weak" and even worse, "insecure" cipher suites.

All local network connections initiated by the toy devices themselves are unencrypted. The Children's camera transmits images only WPA2 encrypted with the default and unchangeable password "12345678", which offers only limited protection. During initialization, Toniebox and Tiptoi send the user's Wi-Fi credentials over unencrypted HTTP, creating a security risk for disclosure as they are not even WPA2 encrypted.

Wi-Fi setup. Some of the toys create their own Wi-Fi network for communication, while others ask for credentials to connect to an existing Wi-Fi network

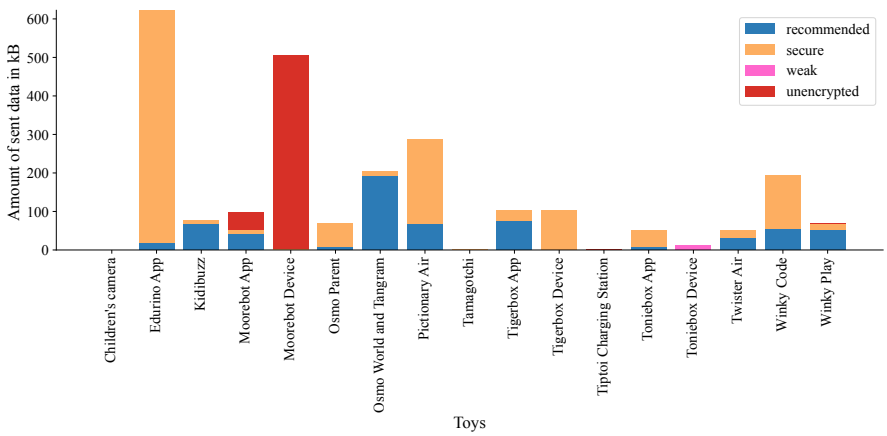

Fig. 2. Amount of data sent (in kB) for all toys, by security of the negotiated TLS cipher suite. Packets without payload (e.g. Acknowledgments) are excluded.

by the home's router. For IoT devices without a user interface, such as Moorebot, Tiptoi, Toniebox and the Children's camera, evaluation of the connection is more challenging. These toys set up their own local Wi-Fi network for sharing the Wi-Fi credentials to connect to the router.

Tiptoi and Toniebox have open Wi-Fi networks without password protection, allowing anyone to connect to the local network. Once connected, the user inputs their home Wi-Fi credentials on their phone or laptop, which are then transmitted to the device over HTTP without TLS encryption. With the Wi-Fi sniffing setup described earlier we are able to intercept the connection and can see the plaintext transmission of the given Wi-Fi credentials. This is concerning as it allows nearby attackers to retrieve the Wi-Fi credentials, especially since Tiptoi and Toniebox are popular toys in public libraries. The identified security vulnerabilities and proposed solutions were communicated to the respective vendors. Toniebox acknowledged the issue and stated that they are already working on a solution for future releases, whereas Tiptoi only indicated an intent to investigate the issue further.

The Moorebot robot provides its own WPA2 password-protected Wi-Fi network with the default password "r0123456". This password is the same for every robot. However, users can change the password when setting up the device. After connecting and entering the home Wi-Fi credentials, the credentials are transmitted to the device in encoded form. Then, users can choose to connect the robot to the companion app, via their home Wi-Fi or the device's Wi-Fi network.

The Tamagotchi toy offers two ways to connect to the user's home Wi-Fi. By entering the Wi-Fi credentials directly into the device using just three buttons, or by scanning a QR code. Through scanning the QR code, Tamagotchi opens a local network, to which the users connects to. The Wi-Fi password is

"596deccf4e1b1c979ae2af8e", and unique for each device, making it harder for an attacker to crack the WPA2 encryption. However, the traffic itself is not encrypted and if the password is known, it is also vulnerable to malicious interception and disclosure of the Wi-Fi credentials.

The Winky robot connects to the phone and companion app with Bluetooth 5 Low Energy. It uses Secure Connections for pairing which provides protection against passive eavesdropping, however, its use of the Just Works association method leaves the connection open to Man-in-the-Middle attacks.

HW/SW support periods. No toy manufacturer declares hardware or software support periods for their products. The terms of service declarations primarily outline standard return rights and warranty claims, without explicit mention of ongoing hardware or software support. The vendors of three toys – Tamagotchi, Twister Air and Winky – even declare that they may discontinue services and support without notice. The Kidibuzz phone comes with Android 10 (released in 2019), which Google stopped supporting in March 2023. Concerningly, we bought the phone in October 2023 and it is still available as of April 2024.

4.2 Privacy

Personal Data. To evaluate the users' privacy, we analyze the decrypted traffic to see which kind of personal data is transmitted to which service. We also examine whether the privacy policy explains this data collection and processing.

For many toys, we find that the privacy policies do not state clearly which specific data is collected and for what purpose the vendors are processing it.

By examining the transmitted data and evaluating their necessity (see Table 3), we find that especially Edurino and Osmo, the learning apps, perform poorly. Edurino sends data about the child's sex, the created avatar, and detailed game analytics. Osmo asks for the full name and the child's exact date of birth. Another case of unnecessary data collection is done by Toniebox as they describe in their privacy policy that they send the list of all SSIDs in the area to their server. This is not needed for the functionality and may allow the vendor to geolocate the Toniebox and identify which Toniebox owners live nearby.

Almost every toy sends device and unique identifiers together with analytics data such as detailed interaction logs, session lengths and device information such as model, OS version and CPU details. While much of this data is justified by the vendors as necessary for improving the app and user experience, it may not be essential for the app's functionality. Moreover, collecting such data could result in the creation of user profiles and identifiable fingerprints.

Interestingly, we find code in most of the apps to retrieve the Google Advertisement ID. As we do not see the Ad ID directly in the traffic, it is uncertain whether the identifier is actually being transmitted to vendors or third-parties. However, given the functionality exists, it is possible that the Ad ID is scrambled into the User ID, as described in the Twister Air privacy policy. Alternatively, the functionality may be inactive, but could be turned on in a future version.

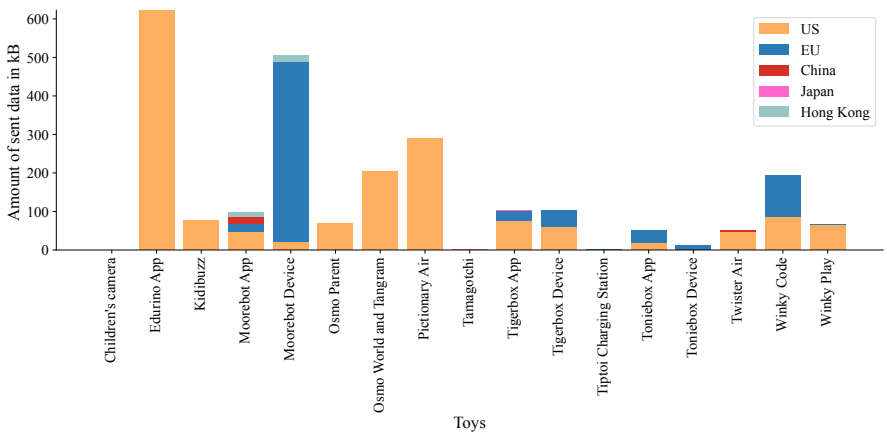

Fig. 3. Amount of sent data (in kB) for all toys, by location of the data destination. Packets without payload (e.g. Acknowledgments) are excluded.

We also find various services which are identified as trackers in the code and in the captured traffic. Seven out of nine companion apps use trackers, Toniebox being the leader by employing four tracking services. Moreover, users should be aware that simply using these applications will result in data being sent to Google Libraries which we can see in the captured traffic. In Figure 4, we provide a list of all contacted services, summing up all transmitted data by all toys.

An analysis of server locations shows that major hosting providers, such as Google Cloud and Amazon AWS, are mainly used, with servers primarily located in the United States. Two toys, the Moorebot and Twister Air, transmit data to servers located in China, specifically to the Alibaba Cloud. Only one toy, the Tiptoi pen, communicates entirely with servers in Europe. An overview of the server locations for each toy can be seen in Figure 3.

In addition, on local networks the Moorebot has an open Robot Operating System (ROS) version 1.4 interface. ROS employs a publisher and subscriber architecture, allowing anyone on the same network as the robot to subscribe to topics. As a result, we were able to access the live video stream, audio stream and other sensor data without any security layer such as authentication or encryption. Furthermore, by publishing topics, we could control the robot's movements to capture additional video data from the environment or improve audio quality of the audio stream.

App permissions. We extracted app permissions from the `AndroidManifest` file and evaluated them regarding necessity for the intended functionality (see Table 4). Positive examples are Edurino and Tigertones, the companion app for Tigerbox, that either require only minimal permissions overall or not very intrusive ones. Pictionary Air, Twister Air and both Winky companion apps perform overall well. However, permissions like the exact location, access to the phone status or the possibility to run at startup are seen unnecessary.

Table 3. Data types transmitted by each toy and assessment whether each data type is required to provide the toy's functionality. Cases where the evaluation is based on public data instead our traffic analysis are marked with an asterisk (*).

	Edurino	Kidibuzz	Camera	Moorebot	Osmo	Pictionary	Tamagotchi	Tigerbox	Tiptoi	Toniebox	Twister	Winky
Processing minimum necessary	▲	■	●	■	▲	■	■	●	●	■	■	■
Personal Information												
Email	●	●	-	●	●	-	-	●	-	●	-	●
Name/pseudonym	■	▲	-	-	▲	-	●	●	-	●	●	▲
Birthday/age	■	-	-	-	▲	-	■	●	-	●	-	-
Avatar	▲	-	-	-	●	-	▲	■	-	●	-	-
Sex	▲	-	-	-	-	-	-	●	-	-	-	-
Region/location	●	●	●	-	-	●	●	●	-	■	■	●
Wi-Fi credentials	-	●*	-	●*	-	-	●*	-	●	▲	-	-
Identifiers												
User ID	●	-	-	●	-	●	-	-	-	●	●	●
Ad ID	■*	-	-	■*	■*	■*	-	-	-	■*	■*	-
Device ID	■	■	-	■	■	■	●	-	-	■	■	■
Game Analytics												
Device Data	■	●	-	●	●	■	●	-	-	●	●	■
Game Data	■	●*	-	●*	■	■	■	■	-	■	■	■
Interactions	■	●*	-	●*	■	■	-	-	-	■	■	■
Image data	-	●*	-	■*	-	●	-	-	-	-	●	■
Audio data	-	●*	-	■*	-	●	-	●	-	●	●	■
Product Analytics												
Purchase information	▲	-	-	-	▲	-	-	-	-	-	-	-

In contrast, the Children's camera, Moorebot, Osmo Parent and the Toniebox app request extensive permissions beyond what is necessary for their operation. This includes the phone status to see the device ID and call information, location status, reading external storage, accessing contact information, and the ability to run at startup.

4.3 Transparency

Subject Data Access Requests. We sent subject data access and deletion requests to all toy vendors for which we have a user account. Only three of seven vendors replied within the one-month period mandated by the GDPR.

Osmo answered quickly and confirmed deletion of the data. However, they indicated that they had only stored the e-mail address, even though we observed transmissions of birth dates and game data to their servers and synchronization with the Osmo parent app, indicating that more data is stored on their side.

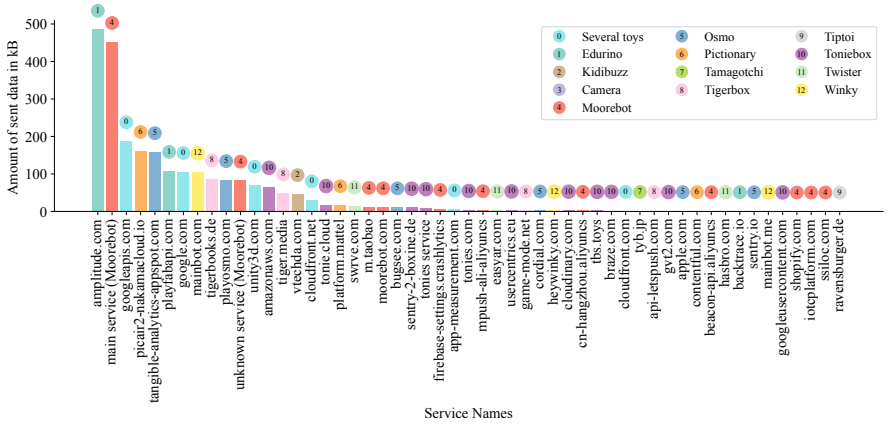

Fig. 4. Amount of data sent (in kB) across all services, by toy. Packets without payload (e.g. Acknowledgments) are excluded.

The data access process for the Toniebox is unnecessarily complicated: users have to provide either PGP keys for the e-mail address associated with their account, or their real-world home address. We requested the digital form and received an encrypted e-mail with a PDF containing the list of data they claim to have stored. However, the list does not contain scanned SSIDs or behavioral analytics, which are processed according to their privacy policy and confirmed to be linkable to user accounts [51]. Tigerbox responded with a list of all personal data, a history of stories and songs we listened to, as well as a breakdown of sent e-mails and whether they were opened or not.

Privacy Policies. In line with prior work on privacy policies [58], the privacy policies for our toys are on average too vague and unspecific, especially regarding transparent information about detail of user data processing, storage and transmission (see Table 5). Most toys have easily accessible privacy policies. The Twister Air app stands out for its detailed list of data and purposes, while others, such as Pictionary Air, Children's camera, or Tigerbox, have generic privacy policies that mention the processing of personal data without specifying purposes and recipients.

The Moorebot robot lacks a privacy policy for its device entirely. Its user manual mentions data being sent to AWS servers in the US without specifying the data or its use. Finding a privacy policy for the Children's camera is challenging for users, as no mention is provided in the app or user manual. Only the link on the Apple App Store (but not the Google Play Store) leads to the privacy policy, which is very generic. While a privacy policy is missing from both the Winky Play app and the website, the Winky Code app has a good privacy policy that users have to consent to. Tiptoi provides a privacy policy during the setup of Wi-Fi credentials. Due to their lack of data collection, the policy is brief.

Table 4. App permissions requested by companion apps and evaluation whether the permissions are necessary for the intended functionality. Permissions with a ⚠ sign are "dangerous" permissions according to Google [20]. Permission marked with an asterisk (*) are required for some features but not the main functionality of the app.

	Edurino	Kidibuzz	Camera	Moorebot	Osmo	Pictionary	Tamagotchi	Tigerbox	Tiptoi	Toniebox	Twister	Winky
Only necessary app permissions	●	-	▲	▲	▲	■	-	●	-	▲	■	■
Number of permissions	3	-	10	19	15	18	-	21	-	32	14	8
Location ⚠	-	-	▲	-	-	▲	-	-	-	▲	-	▲
Phone status ⚠	-	-	▲	▲	-	-	-	-	-	▲	▲	-
Contacts ⚠	-	-	-	▲	-	-	-	-	-	-	-	-
Run at startup	-	-	-	▲	-	-	-	-	-	-	▲	-
Camera ⚠	-	-	●	-	▲	●	-	-	-	▲	●	-
Microphone ⚠	-	-	▲	▲	-	●*	-	●*	-	●*	-	-
Read storage ⚠	-	-	●*	▲	▲	▲	-	●*	-	●*	▲	-
Write storage ⚠	-	-	●*	●*	▲	●*	-	●*	-	●*	●*	-
Post notifications ⚠	-	-	-	▲	▲	▲	-	▲	-	▲	▲	-
Network connections	●	-	■	●	-	-	-	-	-	●	●	●
Wi-Fi	-	-	●	●	-	-	-	-	-	●	-	-
Bluetooth ⚠	-	-	-	-	-	●*	-	●*	-	●*	-	●
NFC	-	-	-	-	-	-	-	●*	-	-	-	-

Obtaining consent for most apps and toys involves displaying the privacy policy and sometimes the terms of service during the initial setup process. In some cases, users may need to actively check a consent box. Tigerbox and Toniebox offer options for users to opt-in to receive advertisements via email, while Edurino allows users to decide whether their data should be stored in the Edurino cloud. However, Edurino does not provide any information about the location or hosting service of the stored data.

User Interface Information. The presentation of privacy- and security-relevant information to users could be improved. For example, none of the toys offer a password strength indicator that would help users create stronger passwords. In addition, the Kidibuzz fails to explain all password requirements when rejecting passwords, such as the prohibition of using names or dictionary words.

The provision of information about software updates is also inadequate. Most IoT devices either lack descriptions of updates or provide vague details, often omitting descriptions of security fixes. One exception is the Tigerbox, which provides a changelog for updates to both device and its companion app.

Table 5. Evaluation of the availability of privacy policies and their quality regarding specific information on what data is collected/shared, and for which purpose.

	Edurino	Kidibuzz	Camera	Moorebot	Osmo	Pictionary	Tamagotchi	Tigerbox	Tiptoi	Toniebox	Twister	Winky
Transparent info about data protection	●	■	▲	▲	■	■	■	■	■	●	●	■
Availability of privacy policy	●	●	■	▲	●	●	●	●	■	●	●	■
Which data	●	●	■	▲	■	▲	●	■	●	●	●	●
How used	■	■	▲	▲	■	▲	■	▲	-	■	●	●
By whom	●	▲	▲	▲	■	▲	■	▲	-	●	●	●

Furthermore, not all version and model numbers are available to users. While app versions can be viewed in the settings of an Android phone, firmware version information is provided by the toy manufacturer. Unfortunately, this information is not available for the Toniebox, and model numbers are missing for the Tiptoi pen and the Moorebot.

4.4 Compliance

General Data Protection Regulation (GDPR). The GDPR mandates vendors to ensure a basic level of protection mechanism for user's data and control mechanisms such as the availability of privacy policies, data minimization, provision of secure storage, and data retention rules. With a lens of technical, but not legal, expertise, we estimate that not all toys are compliant with the GDPR. In particular, we find shortcomings in the availability of the privacy policy (three vendors) and in the detail provided in these policies about specific data processing practices. Many vendors do not list the data items they are processing, or omit information about which parties the data is shared with.

Consumers also have the right to access their data, ask for correction and for deletion. Most vendors mention this right in their privacy policy, however, the response rate of 43% for our subject access requests is disappointing.

Cyber Resilience Act (CRA). The Cyber Resilience Act [18], approved by the European Parliament in March 2024, seeks to establish a standardized cybersecurity framework for products and software with digital components. The CRA, in the current version, mandates for software updates and vulnerability disclosure rules, requiring regular updates with transparent documentation of mitigated vulnerabilities and detailed software bills, listing the history of all detected and patched vulnerabilities. In addition, the CRA asks for basic cybersecurity requirements such as secure authentication or to minimize the attack surface. It will also ask vendors to publish vulnerability disclosure policies, offering security researchers or attentive users a guideline how to disclose found vulnerabilities.

In our examination, we see that only three of 12 vendors provide this information: Tonies (Toniebox), Hasbro (Pictionary Air) and VTech (Kidibuzz). Furthermore, regarding information on software updates, no vendor with the exception of Tigerbox provides detailed information on updates or a history log. This means that most vendors will need to update their processes to comply with the CRA, once it comes into effect.

5 Discussion and Recommendations

In this section we discuss the limitations of our study, put our findings regarding cybersecurity, privacy, transparency and compliance to EU legislation in a broader context, and give specific recommendations for improving smart toys.

Limitations of this work include the small sample size of only 12 toys selected from a much larger smart toy market, which may not be representative for the whole product range.

We did not conduct a longitudinal study, which prevents us from observations of any potential changes in data collection practices over time, and restricts us in assessing long-term effects.

Furthermore, we did not attempt to extract or reverse engineering device firmwares. Thus, plaintext traffic between toys and internet could not be analyzed as we could not install trusted certificates for Man-in-the-Middle attacks.

5.1 Security

In our examination of current communication practices, we see the widespread use of TLS 1.2 encryption for connections to external servers. While some cipher suites within TLS 1.2 offer forward secrecy, their use in our examination, as well as not using the newer TLS 1.3, is not best practice. Most toys as well as the corresponding servers support the stronger, forward secrecy enabling algorithms, such that an upgrade is theoretically possible. Only Toniebox relies on a weak cipher suite for communication, which offers an attack surface to decrypt the traffic.

We also identified some instances of unencrypted connections, which compromises data confidentiality and undermines the integrity and authenticity of transmitted information. We see plaintext traffic mostly in local networks, for example in the Wi-Fi setup procedure, where Wi-Fi credentials can be easily obtained by eavesdropping on the connection. Although the probability of an external attack on the local network is low, these devices are popular in public libraries, which creates a scenario where attackers could exploit the setup process by following users home to capture their Wi-Fi credentials. As this issue is present for all IoT devices without a user interface, the new Wi-Fi Device Provisioning Protocol (DPP, or "Easy Connect") offers a secure solution for connecting IoT devices to Wi-Fi networks [60]. In that solution, devices can be onboarded to a network through QR codes, NFC tags or user-chosen configurators, with strong encryption. None of our toys has deployed this protocol.

Additionally, vendors fail in disclosing information on their device's support periods. This is concerning because users are not informed when security updates are discontinued, and devices may cease functioning entirely.

5.2 Privacy

Personal data has become a prime target for both commercial interests and malicious actors. Children represent an even more vulnerable group in the digital landscape, particularly due to their limited understanding of the implications of sharing personal information online. Moreover, unauthorized access to children's personal data creates a number of potential risks, including exposure to inappropriate content, manipulation through targeted advertising and creating digital footprints, potentially influencing the child's future.

We observe extensive collection of game analytics and behavioral data, including time spent on games, hints/errors, and toy interactions. This data has the potential to generate user-specific profiles, reflecting children's intelligence, problem-solving abilities, and even daily behavioral patterns like playtime and bedtime routines.

Another concerning observation is the widespread use of data tracking mechanisms. These trackers collect user data to create profiles for targeted advertising or for sale to third-party data brokers [25].

Furthermore, we observe network traffic directed to servers in the US, Europe, Japan and China. Although the European Union has established privacy treaties with the US and Japan [14] to protect the data of European citizens [15], data protection concerns remain about the adequacy of privacy measures outside of the EU and to the US [2, 38]. In particular, China is not regarded as having an adequate level of data protection [15], which means that children's interactions with their toys may be disclosed to Chinese authorities and other third parties.

Not all apps comply with the best-practice to only request minimum necessary app permissions. Modern Android apps often ask users to grant permissions during runtime, including for access to location, Bluetooth, camera, and microphone. However, not all users – which may well be children, in the case of toy companion apps – may understand which permissions are really needed, and therefore may not be able to make informed security and privacy choices [28].

5.3 Transparency

The process and responses of the accessing the own personal data stored by the vendor is insufficiently implemented, which is in line with prior work on subject access requests [55]. Only 43% of vendors responded within the one-month period, and their responses did not include all transmitted data that we could see in our data collection. Furthermore, the process of requesting data is too cumbersome: users need to write emails, send PGP keys, or provide their home address. In the latter case, many users may not have PGP keys (or may be unable to use PGP, which is a well-known issue [59]), and would be left with a paper-based process that requires them to reveal additional data (their address)

to the vendor. This is clearly not ideal. A better solution would be to allow users to download their data directly in the app. This would not only be more user friendly, but the transmission could also be encrypted with TLS. However, this approach is not implemented by any of the vendors in our study.

Our analysis finds that many toy companies fail to provide clear, transparent and easily accessible privacy policies. The inconsistency in the availability and detail of privacy policies is evident, with some toys providing detailed lists of data and purposes, while others offer only generic statements. This leaves users unaware regarding the use of their personal information, which is particularly concerning given that sensitive data of children may be processed.

The process for providing and withdrawing consent is insufficient overall. While some toys offer check boxes for proactive consent in the set-up process, others may not present the privacy policy at all, or only refer to it in the settings menu. In addition, the ability to revoke consent is limited. Providers typically do not offer granular choices for data processing, resulting in a binary "all or nothing" scenario. This lack of flexibility may force users to consent to data processing practices that they would otherwise prefer to avoid [26].

5.4 Compliance

Our results show that some vendors fall short of full GDPR compliance. In particular, we find shortcomings in the availability and comprehensiveness of privacy policies. Even when provided, these policies often lack the detailed information necessary to adequately inform users about their data processing practices. Furthermore, we see that not all vendors apply data minimization practices as we observe large amounts of game analytics and device information data. Moreover, the right to access user data and the right to data deletion is ignored by 57% of vendors, resulting in non-compliance with the GDPR.

The CRA aims to improve cyber resilience for products with digital components. Thus, a focus lies on other cybersecurity metrics, primarily regarding patching of vulnerabilities. The act will enforce vulnerability disclosure policies and better information on software updates, such as providing a software bill with the update history. Currently, only one vendor provides a changelog of software updates, and three vendors provide vulnerability disclosure policies, indicating that most vendors need to catch up on the requirements of the CRA. This means that in terms of transparency on patched security vulnerabilities users can hope for better information after the adoption of the CRA. However, the success of this legislation also relies on the enforcement practices, as the descriptions and requirements are held very general.

5.5 Recommendations

Upon the discussion of our findings we want to provide some recommendations regarding the cybersecurity, privacy and transparency of children's smart toys.

Prioritizing privacy and security. Toy vendors have a particular responsibility, due to their young target audience, to implement security-by-design and privacy-by-design best practices throughout their development lifecycle. This includes strong encryption, proper authentication mechanisms, data minimization, and the provision of transparent information and choices to users.

Use of a label system. The creation of a unified label inspired by the nutrition label model [12] could inform users on first glance about basic security, privacy and transparency features of the toy. This label should be placed on the packaging and in online stores for easy accessibility. Possibly, this label could motivate vendors to invest and develop more secure and privacy-preserving smart toys.

Enhance User Control. User interfaces should provide more easily accessible information about the data collected by the vendor. This should be combined with options to withdraw consent and delete specific data as desired.

Easier subject data access requests Users should be able to submit subject data access requests by means of a simple button press within the app. Automated processing of these requests on the vendor-side, i.e., giving users a direct download, would significantly improve the user experience.

Opt-in Consent. Toys should rely more on opt-in rather than opt-out approaches to gain consent from users. This ensures that users need to actively choose to share data and avoids excessive data collection from users who did not change the default settings.

Enable Fine-Grained Consent. Users should be able to selectively disagree with specific aspects of a privacy policy, giving users more granular control. For example, this should include options for users to refuse collection of behavioral and game analytics data.

6 Conclusion and Future Work

We examined 12 children's smart toys with respect to cybersecurity, privacy, transparency and compliance to EU legislation and formulated recommendations aimed at improving security and privacy for smart toys.

Our investigation of security issues uncovered that some connections especially in local networks are inadequately encrypted, leaving vulnerabilities to data disclosures. Furthermore, while the data transmitted is not excessively intrusive, the substantial volume of data, particularly toy analytics data combined with unique identifiers, raises privacy concerns, because it allows pervasive behavioral profiling and fingerprinting of children.

In addition, the toys do not provide sufficient transparency regarding the data being transmitted and its recipients because the privacy policies lack the desired detail. The process for accessing information through subject data access

requests requires more user effort than necessary, and the low response rate indicates that not all toys are compliant with the GDPR.

Looking ahead, the CRA may address some of our security concerns, particularly in areas such as vulnerability patching. However, the effectiveness of this legislation will depend on its enforcement and the cooperation of toy vendors.

Future Work. In the future, we plan to deepen our study of smart toys, including data from the IoT devices themselves rather than just the companion apps. This includes a comprehensive examination of the types of data collected and transmitted, with a particular focus on understanding the implications of AI-powered and medical smart toys which have recently become available. These efforts may not only inform future regulatory frameworks, but may also be helpful for parents who decide whether or not to purchase a smart toy.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abraham, A., Magofei, Dobrushin, M., Nadal, V.: Mobile Security Framework - Documentation. https://mobsf.github.io/docs/, accessed: Dec 2023
2. Batlle, S., van Waeyenberge, A.: EU–US Data Privacy Framework: A First Legal Assessment. European Journal of Risk Regulation **15**(1), 191–200 (2024)
3. Bundesnetzagentur: Bundesnetzagentur zieht Kinderpuppe Cayla aus dem Verkehr. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html (Feb 2017), accessed: Oct 2023
4. Buttarelli, G.: Privacy Matters: Updating Human Rights for the Digital Society. Health and Technology **7**(4), 325–328 (Dec 2017). https://doi.org/10.1007/s12553-017-0198-y
5. de Carvalho, L.G., Eler, M.M.: Security Tests for Smart Toys. In: ICEIS (2). pp. 111–120 (2018)
6. Castelluccia, C., Cunche, M., Le Métayer, D., Morel, V.: Enhancing transparency and consent in the IoT. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 116–119. IEEE (2018)
7. Chowdhury, W.: Toys that talk to strangers: a look at the privacy policies of connected toys. In: Proceedings of the Future Technologies Conference (FTC) 2018: Volume 1. pp. 152–158. Springer (2019)
8. Chu, G., Apthorpe, N., Feamster, N.: Security and privacy analyses of internet of things childrens toys. IEEE Internet of Things Journal **6**(1), 978–985 (2018)
9. cortesi, maximilianhils, raumfresser: mitmproxy - an interactive HTTPS proxy. https://mitmproxy.org/, accessed: Oct 2024
10. Curio Interactive Inc: Homepage of the curio AI toy. https://heycurio.com (2024), accessed: Mar 2024
11. Emami-Naeini, P., Agarwal, Y., Cranor, L.F., Hibshi, H.: Ask the experts: What should be on an IoT privacy and security label? In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 447–464. IEEE (2020)

12. Emami-Naeini, P., Dheenadhayalan, J., Agarwal, Y., Cranor, L.F.: An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices. IEEE Security & Privacy **20**(2), 31–39 (Mar 2022). https://doi.org/10.1109/MSEC.2021.3132398
13. Escher, S., Weller, B., Köpsell, S., Strufe, T.: Towards transparency in the Internet of Things. In: Privacy Technologies and Policy: 8th Annual Privacy Forum, APF 2020, Lisbon, Portugal, October 22–23, 2020, Proceedings 8. pp. 186–200. Springer (2020)
14. European Commission: EU and Japan conclude landmark deal on cross-border data flows at High-Level Economic Dialogue. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5378 (2023), accessed: Apr 2024
15. European Commission: Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (2024), accessed: Apr 2024
16. European Telecommunications Standards Institute: ETSI EN 303 645 V2.1: Cyber Security for Consumer Internet of Things: Baseline Requirements. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (2020), accessed: Oct 2023
17. European Union: General Data Protection Regulation. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (2016), accessed: Oct 2023
18. European Union: Cyber Resilience Act, preliminary version. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0454 (2022), accessed: Mar 2024
19. Frolov, N.: An educational robot security research. https://securelist.com/smart-robot-security-research/111938/ (Feb 2024), accessed: Mar 2024
20. Google for Developers: Manifest.permission. https://developer.android.com/reference/android/Manifest.permission, accessed: Apr 2024
21. Hessel, S., Rebmann, A.: Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children. International Cybersecurity Law Review **1**, 27–37 (2020). https://doi.org/https://doi.org/10.1365/s43439-020-00006-3, https://link.springer.com/article/10.1365/s43439-020-00006-3
22. Holland, M.: ChatGPT & Co.: In fünf Jahren personalisierte Gutenachtgeschichten vom KI-Teddy? https://www.heise.de/news/ChatGPT-Co-Tedybaeren-koennten-personalisierte-Gutenachtgeschichten-erzaehlen-9191143.html (2023), accessed: Mar 2024
23. Hung, P., Fantinato, M., Rafferty, L.: A Study of Privacy Requirements for Smart Toys. In: PACIS 2016 Proceedings. Chiayi, Taiwan (Jun 2016), https://aisel.aisnet.org/pacis2016/71
24. IPSHU: IP Address Lookup Tools. https://en.ipshu.com/, accessed: Feb 2024
25. Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C., Shadbolt, N.: Before and after GDPR: tracking in mobile apps. arXiv preprint arXiv:2112.11117 (2021)
26. Kollnig, K., Dewitte, P., Van Kleek, M., Wang, G., Omeiza, D., Webb, H., Shadbolt, N.: A Fait Accompli? An Empirical Study into the Absence of Consent to {Third-Party} Tracking in Android Apps. In: Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021). pp. 181–196 (2021)
27. Kotrba, K.: Alternative zu Tonies & Co: Lösen Startups mit KI-generierten Geschichten jetzt die Platzhirsche ab? https://www.businessinsider.de/gruen-

derszene/technologie/alternative-zu-tonies-co-loesen-startups-mit-ki-generierten-geschichten-jetzt-die-platzhirsche-ab/ (2024), accessed: Mar 2024
28. Kreuter, F., Haas, G.C., Keusch, F., Bähr, S., Trappmann, M.: Collecting survey and smartphone sensor data with an app: Opportunities and challenges around privacy and informed consent. Social Science Computer Review **38**(5), 533–549 (2020)
29. Macenaite, M.: From universal towards child-specific protection of the right to privacy online: Dilemmas in the eu general data protection regulation. New media & society **19**(5), 765–779 (2017)
30. Manta, I.D., Olson, D.S.: Hello Barbie: First They Will Monitor You, Then They Will Discriminate against You - Perfectly. Alabama Law Review **67**(1), 135–188 (2015/2016), https://heinonline.org/HOL/P?h=hein.journals/bamalr67&i=145
31. Mattel: Shoppingpage Pictionary vs KI. https://shopping.mattel.com/de-de/products/pictionary-vs-ki-hyh74-de-de (2024), accessed: Mar 2024
32. McReynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., Roesner, F.: Toys that listen: A study of parents, children, and internet-connected toys. In: Proceedings of the 2017 CHI conference on human factors in computing systems. pp. 5197–5207 (2017)
33. Mosenia, A., Jha, N.K.: A comprehensive study of security of internet-of-things. IEEE Transactions on emerging topics in computing **5**(4), 586–602 (2016)
34. Nan, Y., Wang, X., Xing, L., Liao, X., Wu, R., Wu, J., Zhang, Y., Wang, X.: Are You Spying on Me?{Large-Scale} Analysis on {IoT} Data Exposure through Companion Apps. In: 32nd USENIX Security Symposium (USENIX Security 23). pp. 6665–6682 (2023)
35. aircrack ng: Aircrack-ng. https://github.com/aircrack-ng/aircrack-ng, accessed: Feb 2024
36. NIST: Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process (2018), https://csrc.nist.gov/projects/lightweight-cryptography
37. Norval, C., Singh, J.: A Room With an Overview: Towards Meaningful Transparency for the Consumer Internet of Things. IEEE Internet of Things Journal (2023)
38. NOYB – European Center for Digital Rights: New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (2023), accessed: Apr 2024
39. OConnor, T., Jessee, D., Campos, D.: Through the spyglass: Towards iot companion app man-in-the-middle attacks. In: Proceedings of the 14th Cyber Security Experimentation and Test Workshop. pp. 58–62 (2021)
40. oleavr: frida, Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers. https://frida.re/docs/android/, accessed: Oct 2023
41. Paracha, M.T., Dubois, D.J., Vallina-Rodriguez, N., Choffnes, D.: IoTLS: understanding TLS usage in consumer IoT devices. In: Proceedings of the 21st ACM Internet Measurement Conference. pp. 165–178 (2021)
42. pcipolloni: Frida Codeshare - Universal Android SSL Pinning Bypass with Frida. https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/, accessed: Mar 2024
43. Qualys Inc: Qualys SSL Lab. https://www.ssllabs.com/ssltest/index.html, accessed: Feb 2024
44. Railean, A., Reinhardt, D.: OnLITE: on-line label for iot transparency enhancement. In: Secure IT Systems: 25th Nordic Conference, NordSec 2020, Virtual Event, November 23–24, 2020, Proceedings 25. pp. 229–245. Springer (2021)

45. Ren, J., Dubois, D.J., Choffnes, D., Mandalari, A.M., Kolcun, R., Haddadi, H.: Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In: Proceedings of the Internet Measurement Conference. pp. 267–279 (2019)
46. Rudolph, H.C., Grundmann, N.: TLS Ciphersuite Search. https://ciphersuite.info/, accessed: Jan 2024
47. Sadeeq, M.A., Zeebaree, S.R., Qashi, R., Ahmed, S.H., Jacksi, K.: Internet of Things security: a survey. In: 2018 International Conference on Advanced Science and Engineering (ICOASE). pp. 162–166. IEEE (2018)
48. Schmidt, D., Tagliaro, C., Borgolte, K., Lindorfer, M.: IoTFlow: Inferring IoT Device Behavior at Scale through Static Mobile Companion App Analysis. In: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. pp. 681–695 (2023)
49. Shasha, S., Mahmoud, M., Mannan, M., Youssef, A.: Playing with danger: a taxonomy and evaluation of threats to smart toys. ieee internet things j. 6, 2986–3002 (2018)
50. Streiff, J., Noah, N., Das, S.: A Call for a New Privacy & Security Regime for IoT Smart Toys. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC). pp. 1–8. IEEE (2022)
51. Team RevvoX: Toniebox Reverse Engineering. https://github.com/toniebox-reverse-engineering/talks/blob/master/2023-12-27%20-%2037C3%20-%20Toniebox%20Reverse%20Engineering.pdf and https://media.ccc.de/v/37c3-11993-toniebox_reverse_engineering#t=3609, accessed: Jan 2024
52. Trimananda, R., Le, H., Cui, H., Ho, J.T., Shuba, A., Markopoulou, A.: {OVRseen}: Auditing network traffic and privacy policies in oculus {VR}. In: 31st USENIX security symposium (USENIX security 22). pp. 3789–3806 (2022)
53. United Nations, G.: Convention on the Rights of the Child. https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (1989), accessed: Mar 2024
54. Unknown: Geolocation DB. https://geolocation-db.com/jsonp/, accessed: Feb 2024
55. Urban, T., Tatang, D., Degeling, M., Holz, T., Pohlmann, N.: A Study on Subject Data Access in Online Advertising After the GDPR. In: Pérez-Solà, C., Navarro-Arribas, G., Biryukov, A., Garcia-Alfaro, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology. pp. 61–79. Lecture Notes in Computer Science, Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-31500-9_5
56. Wachter, S.: Privacy: Primus Inter Pares - Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights. SSRN Scholarly Paper ID 2903514, Social Science Research Network, Rochester, NY (Jan 2017)
57. Wachter, S.: The GDPR and the Internet of Things: a three-step transparency model. Law, Innovation and Technology **10**(2), 266–294 (2018)
58. Wagner, I.: Privacy Policies across the Ages: Content of Privacy Policies 1996–2021. ACM Transactions on Privacy and Security **26**(3), 32:1–32:32 (May 2023). https://doi.org/10.1145/3590152
59. Whitten, A., Tygar, J.D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: Usenix Security (1999)
60. Wi-Fi Alliance, Harkins, D.: Wi-Fi Easy Connect: Simple and secure onboarding for IoT. https://www.wi-fi.org/beacon/dan-harkins/wi-fi-easy-connect-simple-and-secure-onboarding-for-iot (2023)

61. Wireshark Foundation: Wireshark - Network Protocol Analyzer. https://www.wireshark.org/, accessed: Dec 2023
62. Wireshark Foundation: WPA PSK (Raw Key) Generator. https://www.wireshark.org/tools/wpa-psk.html, accessed: Feb 2024