Journal of Cybersecurity and Privacy

MDPI

Article

Assessing the Security and Privacy of Baby Monitor Apps

Lukas Schmidt *, Henry Hosseini and Thomas Hupperich

European Research Center for Information Systems, University of Münster, 48149 Münster, Germany; henry.hosseini@wi.uni-muenster.de (H.H.); thomas.hupperich@wi.uni-muenster.de (T.H.)
* Correspondence: lukas.schmidt@wi.uni-muenster.de

Abstract: Emerging technologies in video monitoring solutions seriously threaten personal privacy, as current technologies hold the potential for total surveillance. These concerns apply in particular to baby monitor solutions incorporating mobile applications due to the potential privacy impact of combining sensitive video recordings with access to the vast amount of private data on a cell phone. Therefore, this study extends the state of privacy research by assessing the security and privacy of popular baby monitor apps. We analyze network security measures that aim to protect baby monitoring streams, evaluate the corresponding privacy policies, and identify privacy leaks by performing network traffic analysis. Our results point to several problems that may compromise user privacy. We conclude that our methods can support the evaluation of the security and privacy of video surveillance solutions and discuss how to improve the protection of user data.

Keywords: privacy; dynamic analysis; monitor apps; home surveillance

check for updates

Citation: Schmidt, L.; Hosseini, H.; Hupperich, T. Assessing the Security and Privacy of Baby Monitor Apps. *J. Cybersecur. Priv.* **2023**, *3*, 303–326. https://doi.org/10.3390/jcp3030016

Academic Editor: Giorgio Giacinto

Received: 28 April 2023
Revised: 19 June 2023
Accepted: 23 June 2023
Published: 29 June 2023

1. Introduction

Advances in digitalization have been affecting our lifestyles in recent decades. While the effects provide various benefits to ease our daily life tasks, their utilization introduces challenges for users' privacy. The consumer use of digital products, such as mobile applications (apps) and the Internet of Things (IoT), inevitably leads to the production and process of user data. Blanket access to these private data and opaque data flows between endpoints, servers, and cloud infrastructures eases privacy leaks and opens the door for abusive data collection. This concern holds especially true for video surveillance systems due to the privacy implications of recording live videos. The combination of digitalization and rising technologies in video monitoring solutions poses a serious threat to personal privacy, as current technology has the potential for total surveillance [1]. Thus, exploring the usage and protection of private data, especially in closed-source proprietary surveillance systems, represents a focal point of privacy research.

Adequate surveillance systems must cover both security and privacy, stemming privacy violations holistically. From a technical perspective, this requires the implementation of security mechanisms to ensure confidentiality and data protection, complemented by privacy measures, such as transparent system architecture, privacy-aware data exchange, and informing their users [1]. Previous work has explored the security and privacy mechanisms of various video surveillance solutions targeting the consumer market [2–4], which generally consist of ecosystems built around network cameras reachable through the internet. Unfortunately, the results indicate that these systems often suffer from serious flaws and security vulnerabilities, threatening user privacy for sensitive tasks, such as home security [5]. Analyzing and reporting these weaknesses improves the security and privacy levels of video surveillance solutions built for consumer use, e.g., by encouraging manufacturers to fix security weaknesses or informing users about their use of insecure systems. However, previous studies seemingly overlooked a whole category of video monitoring solutions: baby monitor apps on mobile phones. Often referred to as "baby monitors", these apps usually combine two mobile phones to constitute a surveillance solution, where one phone serves as a camera that transmits a video stream to the second paired smartphone. The most popular apps of this kind have been downloaded millions of times. Despite their large user base and the use of video and audio recording capabilities in conjunction with access to personal information on a mobile phone, we are unaware of any previous work investigating the privacy implications of baby monitor app usage. Moreover, as most baby monitor apps are proprietary, their communication and security mechanisms are opaque, narrowing the possibilities for privacy evaluation and thus indicating a knowledge gap. This study aims to examine the current state of the art in regards to the security and privacy of popular baby monitor apps by answering the following research questions:

RQ1 How is the confidentiality of the video streams of the baby monitor applications ensured?

RQ2 How compliant are the data practices of the baby monitor applications with the respective privacy policies?

In doing so, we investigate the privacy exposure of users during the sensitive task of monitoring babies with mobile phones. More detailed, the contributions of this study are listed as follows:

- Considering that the confidentiality of private video footage is an integral part of privacy protection, we evaluated the security measures used to protect the monitoring streams and identified several security issues that threaten their confidentiality.
- By analyzing network connections and transferred data during baby monitoring sessions, we compared the apps' behavior with the declared data practices of their privacy policies. We examined the statements and transparency of the privacy policies and assessed the privacy implications of the use of the baby monitor app in the real world.
- We conducted the first in-depth analysis of network communications and corresponding network security measures implemented by popular baby monitor apps in the Android ecosystem.

In the remainder of this work, we review related work in Section 2, providing an overview of the state-of-the-art video surveillance analysis and mobile app privacy research. We describe our assessment methodology in Section 3 and detail the steps we used for privacy and security analysis. We present the results of our study in Sections 4 and 5, followed by a discussion of our findings and a conclusion, including an outline of future work in Section 6.

2. Related Work

Compared to other user systems, the usage of mobile devices appears to pose more serious risks in terms of security and data protection [6], resulting in high compliance requirements. However, despite the strict regulations for mobile devices, many mobile applications seem not to comply with current demands.

Data practices in mobile applications are often found to be different from declared policies, omitting or incorrectly handling private information [7], collecting personal data, e.g., location profiles, without declaration or consent [8], or suffering from other inconsistencies [9]. At the same time, users often do not realize that their data are being collected and used by mobile applications [10]. In this area of conflict, further investigation is required to gain insight into how personal data is collected and how these data practices are declared in the applications' privacy policies. Therefore, a focal point of privacy research is evaluating existing mobile applications, especially those that process sensitive user data.

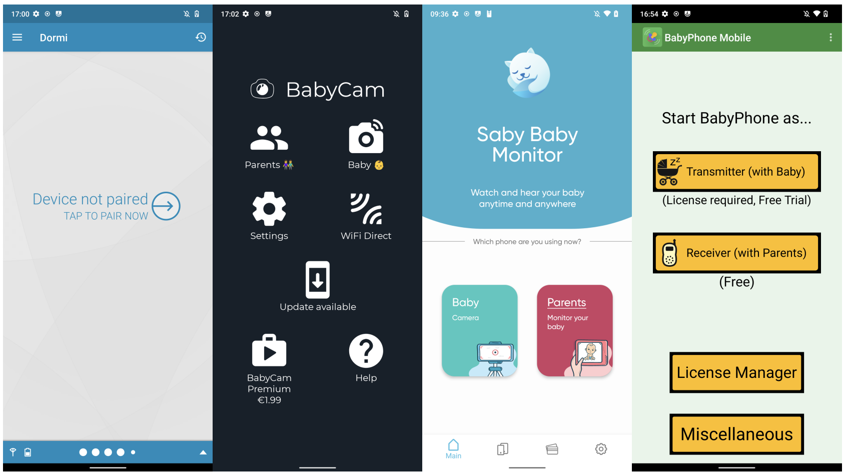
Previous work investigated mobile applications supporting healthcare [11], warning about the alarming state of security and privacy in this area. Similar results were presented by a study of mobile apps targeting individuals suffering from depression. The study reported that most of the apps lacked transparency about the security of personal data and were found to be insecure and unsafe to use [12].

It has been shown that it is relatively easy for app developers to hide their data practices from automated analysis [13]. Therefore, manual analysis of apps that record and process personal data is essential, as work in areas other than mobile health has also been suggested. One domain processing sensitive data is childcare, and devices and software designed to interact with and survey children have been found to pose high security and privacy risks [14]. Another study examines childcare mobile apps, showing that their privacy policies may not be clear about data practices. Additionally, some of the solutions examined rely on insecure cloud storage for the collected data [15], threatening the privacy of children's data.

In this context, we found baby monitoring applications to be a unique category of interest whose security and privacy implications remain to be researched. Baby monitoring apps are designed to observe, and thus, apply methods similar to video surveillance solutions, such as recording and processing pictures, videos, and audio material. Although privacy consent for such actions is abdicated to children's guardians, there is the potential to use the data collected by such apps illegally [16]. In addition to the challenges of mobile app security and privacy, video surveillance systems have their own difficulties. In the context of IoT surveillance devices, researchers demonstrated that machine-in-the-middle attacks might allow reconstruction of visual material recorded by IP cameras by eavesdropping on network traffic or deploying a multichannel attack [2,17]. Valente et al. have conducted similar experiments, revealing activities captured by cameras even if the device's communication is encrypted [4]. Moreover, with the growing diversity and number of IoT devices and camera surveillance, attack vectors increase, putting the security and privacy of personal information at risk [18]. Therefore, this paper extends previous work in the field of security and privacy analysis of surveillance applications by examining the security and privacy implications of baby monitor mobile applications, running on off-the-shelf smartphones.

3. Materials and Methods

The focus of this study is to investigate the current state of privacy and security of baby monitoring applications, i.e., applications that allow parents to monitor their babies remotely. To achieve this, we searched for apps in the Google Play Store using the phrase "baby monitor", and identified those that could stream video from a local Wi-Fi network to remote parental devices over the Internet. We chose to evaluate freely available apps with a significant user base, i.e., apps that had been downloaded more than 500,000 times by mid-February 2023. We identified four apps that meet these requirements and downloaded their software packages and their respective privacy policies (Table 1). Figure 1 shows the overview of the welcome screens in these applications.



(**a**) (**b**) (**c**) (**d**)

Figure 1. Overview of the analyzed baby monitor apps that can be used to combine two cell phones into a video surveillance solution: (**a**) Dormi (**b**) BabyCam (**c**) Saby (**d**) Babyphone Mobile.

Table 1. Investigated baby monitor apps. All apps were accessed on 30 March 2023.

Abbreviated Name	APK id@version	Installs	Rating
Dormi	com.sleekbit.dormi@3.4.3	1 Mio.+	4.1/5
BabyCam	com.arjonasoftware.babycam@2.24	1 Mio.+	4.5/5
Saby	com.saby.babymonitor3g@2.133	1 Mio.+	3.9/5
Babyphone Mobile	com.babyphonemobile@3.00.1	100.000+	3.9/5

The creators of Babyphone Mobile have split the functionality into two different apps, one for Wi-Fi-only monitoring and one for baby monitoring using remote parental devices accessible via the Internet. Combining the installation numbers of both apps, the developers reached a total of 600,000+ installs, wherefore we chose to consider the app as well. As part of our study, we focused on investigating the data practices of each monitoring app and checking compliance with its respective privacy policy. Furthermore, we examined how these monitoring applications ensure the confidentiality of transmitted video streams by analyzing the implemented network security measures.

3.1. Privacy Assessment Methodology

Multiple privacy regulations have been enforced over the last decade, including prominent instances such as the General Data Protection Regulation (GDPR) [19] and the California Consumer Privacy Act (CCPA). Its amendment, the California Privacy Rights Act (CPRA) [20], went into effect in January 2023, along with the Virginia Consumer Data Protection Act (VCDPA) [21]. These privacy regulations require processors and collectors of personal data to inform affected users about these data practices, such as collection, use, and sharing. The means of informing users about these data practices are privacy policies. Consequently, the rights of affected individuals must be listed in privacy policies along with the contact details of a person for privacy-related questions. This provides individuals with the ability to self-determine information. Fair and transparent handling of personal data builds trust in companies and, in our case, the worry-free usage of baby monitor apps.

In line with previous studies exploring the privacy of mobile applications containing sensitive data, such as COVID-19 contact tracing apps [22], mHealth apps [11], or child-care apps [15], we utilized several measures to evaluate the privacy implications of baby monitoring apps. Adapting from the different methodologies of previous work, we carried out the following steps to assess the privacy impact of each baby monitor app:

1. We reviewed the data practices declared in the app's privacy policy and categorized the collected and shared personal data and the security level of confidential data transmission. To perform these assessments, we used the established taxonomy used for the annotation of the OPP-115 privacy policy corpus by Wilson et al. [23], as well as its refined and updated taxonomy as used for the annotation of the bilingual English and German MAPP privacy policy corpus by Arora et al. [24]. The updated taxonomy captures the introduced EU GDPR regulations and California's CCPA/CPRA for first-party and third-party data collection. Furthermore, we did not consider the defined "Do Not Track" category in [23], as it is no longer supported by the major browsers and is considered a retired specification by the former Tracking Protection Working Group [25]. Table 2 illustrates the categories and attributes of the resulting taxonomy, accompanied by their descriptions.
2. We evaluated the dangerous permissions that each app stated in the Android manifest and identified valid permissions necessary to build a video surveillance solution. Extending previously used methodology [11], we investigated possible misuse of permissions by combining dynamic and static code analysis.
3. We performed a dynamic analysis of the app's communication behavior by capturing and decrypting all network connections using a transparent proxy. In this way, we got insight into the communication destinations, the transport security mechanisms implemented, and the actual data transmitted during a baby monitoring session.

4. Finally, we checked the results of the dynamic analysis for exposure of personal information and compliance with the respective privacy policy.

3.2. Reviewing the Confidentiality of Monitoring Video Streams

Considering that the confidentiality of video stream monitoring is an integral part of privacy protection, we found that evaluating the use of appropriate security measures is of particular interest. By evaluating the utilized network security measures, we examined how each application protects the confidentiality of the transmitted baby monitoring video streams.

3.2.1. Threat Model

Based on user feedback on the Google Play Store, baby monitor apps are used in potentially insecure networks, such as wireless networks in hotels during vacations. As such, we assume a threat model where a potential attacker can eavesdrop and intercept network traffic between the two cell phones in use, which is similar to the attack scenarios described in related work [11,23]. These attacks are also known as MitM (machine-in-the-middle) [26] attacks. In the case of baby monitoring apps, MitM-attacks become easily possible if the phone monitoring the child uses a Wi-Fi network and the parental device communicates over the Internet via cellular or other Wi-Fi networks. In such a scenario, the confidentiality of protected data is usually ensured by encryption as a network security measure.

3.2.2. Methodology

Even in the case of properly set-up transport encryption of video streams, MitM attacks may compromise the monitoring streams' confidentiality by allowing eavesdropping or recording of the transmitted video footage. Therefore, next to evaluating the implemented encryption mechanisms intended to protect transmitted video streams, we checked each application for security issues in the applied network protocols and software implementations:

1. Using the results of a traffic capture performed during a baby monitoring session (see Section 3.1), we evaluated the collected data regarding utilized network security measures and potential clear text transmissions.
2. By statically analyzing the app using the Mobile Security Framework (MobSF) [27], we evaluated the overall security state of each app. We obtained an overview of potential security issues and verified these issues by performing a code review using JADX [28].
3. We performed an additional security analysis for each application to identify security issues that were not detected by automatic static analysis. The analysis consisted of a manual review of the source code using JADX [28], where we focused on identifying potential issues that compromise the confidentiality of transmitted video streams.

3.3. Analysis Environment

Baby monitoring apps constitute a video surveillance solution by combining the capabilities of two different smartphones. This surveillance solution uses one monitoring device, which transmits live video streams to the second device, the parental control device. Therefore, a fundamental requirement for investigating baby monitoring apps is running instances of the same monitoring app on two smartphones. Our experiments were carried out using two physical mobile devices running the Android 12 operating system. We chose physical devices to create a realistic analysis environment, which means, among other things, establishing connections to Wi-Fi and cellular networks. The parent device was connected to a separate Wi-Fi network only accessible through the Internet to emulate a remote parent device. We pre-installed each investigated app on both devices.

Table 2. Applied taxonomy to identify data practices in the privacy policies adapted from Wilson et al. [23] and Arora et al. [24].

Categories	Category Description	Attributes	Attribute Description
First-Party Collection/Use	Privacy practices describing data collection or data use by the company/organization owning the website or mobile app.	Information Type	What category of information is collected or tracked by the company/organization?
		Purpose	What is the purpose of collecting or using user information?
		Collection Process	How does the first party collect, track, or obtain user information?
		Does/Does Not (opt)	Use to denote if the policy explicitly states that something is NOT done.
		Collection Mode (opt)	Use to denote if the data collection performed by the first party is implicit (e.g., the company/organization collects the information without the user's explicit awareness) or explicit (e.g., the user provides the information)
		Anonymization (opt)	Use if it is explicitly stated whether the information or data practice is linked to the user's identity or if it is anonymous.
		User Type (opt)	Use if a practice applies specifically to users with an account or users without an account.
		Choice Type (opt)	Use if user choices are explicitly offered for this practice.
		Choice Scope (opt)	Use to indicate the scope of user choices. In some cases, even if user choices are not clear or specific, this attribute can be selected.
		Legal Basis for Processing	The GDPR prohibits the collection and processing of personal data without a proper legal basis. Therefore, every category of personal data requires the legal basis to be clear and specific.
Third-Party Collection/Use	Privacy practices describing data sharing with third parties or data collection by third parties. A third party is a company/organization other than the first-party company/organization that owns the website or mobile app.	Information Type	What category of information is shared with, collected by, or otherwise obtained by the third party?
		Purpose	What is the purpose of a third party receiving or collecting user information?
		Entity	The third parties involved in the data practice.
		Collection Process	How does the third party receive, collect, track, or see user information?
		Does/Does Not (opt)	Use to denote if the policy explicitly states that something is NOT done.
		Anonymization (opt)	Use if it is explicitly stated whether the information or data practice is linked to the user's identity or if it is anonymous.
		User Type (opt)	Use if this practice applies specifically to users with an account or users without an account.
		User Choice (opt)	Use if user choices are explicitly offered for this practice.
		Choice Scope (opt)	Use to indicate the scope of user choices. In some cases, even if user choices are not clear or specific, this attribute can be selected.
User Access, Edit and Deletion	Privacy practice that allows users to access, edit or delete the data that the company/ organization has about them.	Access Type	Options offered for users to access, edit, delete information that the company/organization has about them.
		Access Scope	If access is offered, what data does it apply to.
		User Type	Use if this practice applies specifically to users with or without an account.
Data Retention	Privacy practice specifying the retention period for collected user information.	Retention Period	Description of the retention period, i.e., how long data are stored.
		Retention Purpose	The purpose to which the retention practice applies (may be "unspecified").
		Personal Information Type	The information type for which the retention period is specified (may be "unspecified").

Table 2. *Cont.*

Categories	Category Description	Attributes	Attribute Description
Data Security	Practice that describes how users' information is secured and protected, e.g., from confidentiality, integrity, or availability breaches. Common practices include the encryption of stored data and online communications.	Security Measure	Policy statements that describe the type of security that the website/app implements to protect users' information.
Policy Change	The company/organization's practices concerning if and how users will be informed of changes to its privacy policy, including any choices offered to users.	Change Type Notification Type User Choice	For what type of changes to the website/app's policy are users notified? How is the user notified when the privacy policy changes? What choices/options are offered to the user when the policy changes?
International and Specific Audiences	Specific audiences mentioned in the company/organization's privacy policy, such as children or international users, for which the company/organization may provide special provisions.	Audience Type	Which audience does the policy segment refer to?
Other	Another aspect not covered in the other categories is discussed in the text segment.	Privacy Contact Information	The paragraph describes how to contact the company with questions, concerns, or complaints about the privacy policy.

We connected the baby monitoring device to a configured Wi-Fi access point for network and security analysis (Figure 2), which functioned as a router that forwards packets to the Internet. On top, a transparent proxy was run [29]. Using this transparent proxy, we intercepted all TCP and HTTP(S) connections and were further able to decrypt TLS-based transport encryption by performing MitM attacks. This method allowed us to inspect and capture transmitted data, providing us with the same capabilities an attacker has in our proposed threat model (see Section 3.2). Since MitM attacks on properly secured TLS connections result in connection errors due to failed certificate checks, we disabled certificate checks for the privacy analysis part. We did so by dynamically patching the instances of the monitoring application running using Objection [30], setting the certificate check results to always return "true".

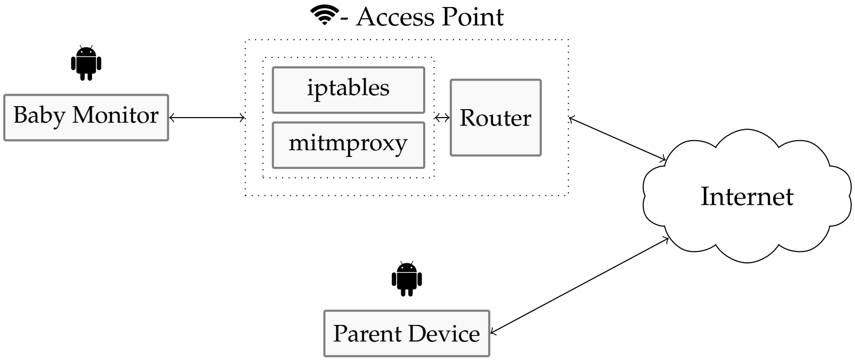


Figure 2. Methodology—analysis environment.

We captured and analyzed the network traffic from a monitoring session for each initially chosen baby monitoring app. A monitoring session consisted of the subsequent execution of the child and parent apps, pairing the mobile phones, performing a video transmission with default settings, and closings on both devices.

4. Evaluation of the Privacy Policies

In Section 3.1, we described the assessment method of the apps' privacy policies based on established taxonomies that comply with GDPR and CCPA/CPRA. In this section, we first describe the findings of analyzing the privacy policies collected. The analysis is followed by a description of the privacy-risking permissions requested by each application and our observations on the monitored network traffic. Our assessment reveals a mixed picture in terms of the quality and completeness of the privacy policies. Table 3 depicts all the observed data practices based on the taxonomies described above in the privacy policies. In the following, we elaborate on these observations.

4.1. First-Party Collection/Use

Article 13 of the GDPR requires affected users (data subjects) to be informed about the direct collection and processing of their personal data [31]. All inspected apps state in their privacy policies that they collect personal data implicitly. These implicitly collected personal data include common data types, such as IP address, device ID and device information, cookies, and tracking elements. The Dormi and Babyphone Mobile apps essentially require these data to provide services, while the other apps use collected information to provide optional services or for analytical purposes. In particular, the BabyCam app generically states at the beginning of the privacy policy that it neither collects personal information nor uses cookies. However, it controversially alludes in a later section to the use of first-party cookies for advertising purposes. In terms of user choice, the Dorm and BabyCam apps explicitly state not to use the app in case of objection to the collection and use of the specified personal data. While Article 6 of the GDPR requires providing a valid legal basis for data processing and collection, none of the inspected apps' privacy policies explicitly state such a legal basis.

Table 3. Identified data practices in the privacy policies, as illustrated in Table 2. Empty cells denote that the data practice could not be identified in the respective privacy policy.

Category	Attributes	Dormi	BabyCam	Saby	Babyphone Mobile
First-Party Collection/Use	Information Type	IP address and device IDs	Cookies and tracking elements	IP address and device IDs Computer information	IP address and device IDs
	Purpose	Essential service or feature	Advertising or marketing	Optional service or feature	Essential service or feature
	Collection Process	Collected on a first-party app	Collected on first-party website/app		Collected on a first-party app
	Does/Does Not	Does not share PI with any third party	Does not collect (personal) information Does not use cookies	Does not collect PI of children	Does not analyze personal data
	Collection Mode (opt)	Implicit	Implicit	Implicit	Implicit
	Anonymization (opt)				Identifiable
	User Type (opt)				Unspecified
	Choice Type (opt)	Do not use service	Do not use service		
	Choice Scope (opt)	Collection and Use	Collection and Use		
	Legal Basis for Processing				
Third-Party Collection/Use	Information Type		Cookies and tracking elements	IP address and device ID Computer information User online activities Cookies Unspecified	Unspecified
	Purpose		Advertisement or Marketing	Analytics or research Essential service or feature	Unspecified
	Entity		Google AdSense	Google Play Services AdMob Firebase Analytics Facebook Fabric Crashlytics	App Store
	Collection Process		Tracked on first-party website/app by third party	Tracked on first-party website/app by third party	Unspecified
	Does/Does Not (opt)		Does not sell, trade, or transfer PI		
	Anonymization (opt)				
	User Type (opt)		Unspecified		
	Choice Type (opt)		Opt-out link	Opt-in Do not use service	
	Choice Scope (opt)		Use	Collect and Use	
User Access, Edit, and Deletion	Access Type	Unspecified			Unspecified
	Access Scope	Unspecified			Unspecified
	User Type (opt)				
Data Retention	Retention Period	Limited Indefinitely		Unspecified	Limited
	Retention Purpose	Perform service			Perform Service
	Personal Information Type	IP address and device IDs			IP address and device IDs User online activities Other
Data Security	Security Measure	Secure data transfer		Generic	Secure data transfer
Policy Change	Change Type	Unspecified Privacy relevant change	Unspecified	Unspecified	Other
	Notification Type	General notice in privacy policy Personal notice	General notice in privacy policy	General notice in privacy policy	General notice in privacy policy
	User Choice	Opt-in	Unspecified	None	None
Intl. and Specific Audiences	Audience Type	Europeans		Children	
Other	Privacy contact information	Yes	Yes	Yes	Yes

4.2. Third-Party Collection/Use

Article 14 of the GDPR requires affected users to be informed about the collection of personal user data through third-party sources i.e., without the user's knowledge [32]. Based on the information provided in the privacy policies, third parties collect personal data in all applications, except the Dormi app. These personal data include cookies and tracking elements, but also more extensive personal information, such as IP address and device ID, further device information, and user online activities. The purpose of the collection ranges between advertisement or marketing, analytics and research, and essential features. The applications with third-party collection list the entities that collect data on their app. The Saby app does not provide any option to object to third-party data collection, while BabyCam and Babyphone Mobile provide choice types such as an opt-in and an opt-out link, or not using part of the service.

4.3. User Access, Edit, and Deletion

The GDPR grants users the right to access and seek a copy of their collected personal data on request (Article 15) [33], the right to rectification in order to correct and complete their personal data (Article 16), and the right to erasure also known as "the right to be forgotten" (Article 17) [34]. While users have the right to be informed about these control rights (Articles 13 and 14), two of the inspected apps did not provide such information. The Dormi app merely offers users the opportunity to contact them in case of queries or complaints about the collected data. Babyphone Mobile informs users of their rights regarding their stored personal data, i.e., the rights of access, rectification, and deletion in its general website privacy policy. This app offers users the ability to contact the developers of the app by email to exercise these rights.

4.4. Data Retention

Article 5(1)(e) of the GDPR requires that personal data are stored for no longer than necessary. Additionally, recital 39 invites data controllers to limit the storage time of personal data [31]. In their privacy policies, three of the inspected apps (Dormi, Saby, and Babyphone Mobile) state that they store personal data, mainly to perform services. The Babyphone Mobile app stores users' IP addresses while permanently storing unique identifiers. This app also describes the need to temporarily store encrypted audiovisual data in a data cluster to transfer them between two devices. BabyCam explicitly states not to store any personal data on their servers, while none of the remaining apps describe whether audiovisual data is stored temporarily for audiovisual transmission.

4.5. Data Security

Article 32 of the GDPR requires data controllers and processors to take appropriate data protection measures to ensure the security of collecting and processing personal data based on existing risks [35]. Dormi and Babyphone Mobile state to take concrete security measures by encrypting transmitted audiovisual data. More concretely, the Babyphone mobile app offers end-to-end encryption as an additional option by asking the user to set a password as the encryption key. The Dormi app offers end-to-end encryption by default. The Saby app generically states to take security measures and apply commercial security products to protect collected personal data. The BabyCam app does not provide any explicit statements about security measures.

4.6. Policy Change

The Guidelines for Transparency under Regulation 2016/679 published by the Article 29 Working Party explicitly require data processors and controllers to inform data subjects about changes in the privacy statement so that most affected users become aware of the changes [36]. All inspected privacy policies contain a statement on informing users in the event of changes in their privacy policies. The Dormi app aims to inform users of significant changes and seek consent if required by law. The other apps intend to inform users by updating their respective privacy policies and asking users to review them from time to time. Not all analyzed privacy policies include the date of their update. However, those that had included a date were last updated around the GDPR enforcement date in 2018.

4.7. International and Specific Audiences

We inspected the privacy policies for declared special provisions aimed at international or specific audiences, e.g., children. The privacy policy of the Dormi app contains a short segment addressing European residents, due to the application of the GDPR, about the collection of unique identifiers only after acquiring consent. A section of the privacy policy of the Saby app states that it does not offer services to children. We could not find any privacy declaration aimed at Californian residents, i.e., a CCPA/CPRA notice.

4.8. Contact Details for Privacy-Related Questions

Article 13(1)(a) of the GDPR requires the identity and contact data of data controllers, i.e., collectors of personal data, to be available to affected users [31]. All privacy policies include the possibility to ask an individual about privacy-related questions. Only Babyphone Mobile includes full contact details, such as providing a telephone number and address. The other apps were content with providing an email address. BabyCam provides a Gmail address, while the other observed email addresses are company or app domains.

5. Mobile App Analysis

Baby monitoring apps form a video surveillance solution using commercially available mobile devices and mobile applications. In this monitoring solution, one device is used to transmit live video streams to the second device, the parental control device. However, the proprietary nature of common baby monitoring apps makes it difficult to analyze their security and privacy status. By dynamically analyzing the behavior of the apps in combination with code inspection, we aim to lower the opacity that hinders analysis. In the following, we elaborate on the knowledge gained during our analysis, offering insight into the inner workings of baby monitor apps. This allows us to assess baby monitor app usage's security and privacy implications. We analyze the permissions each app uses, how device authorization is performed, and how each app uses network communication to transfer monitor video footage over the Internet. Based on these insights, we review the network security measures deployed to protect this video footage and identify several privacy leaks and security issues that threaten user privacy.

5.1. App Permissions

The permission system in the Android operating system regulates an application's access to the phone hardware, settings, and user data [37]. Based on the criticality of the access granted, the Android permissions are divided into different categories, with dangerous permissions allowing access to sensitive data, settings or potentially risky features. Since the release of Android 6.0, Android requires app users to explicitly grant dangerous permissions to an app at runtime [38]. Accordingly, those permissions are called runtime permissions. The user must confirm access for privacy protection reasons, but the time at which runtime permissions are requested depends on the app being used. This complicates the evaluation of permissions because the app could only request permissions when the user triggers the corresponding functionality. However, runtime permissions should be declared in the app's manifest file, a configuration file that is meant to contain all the permissions that an app might request. Therefore, we evaluated the dangerous permissions listed in each app's Android manifest to check whether the app requests more than the required permissions.

As the evaluation of manifest permissions in Table 4 illustrates, there are ultimately two dangerous permissions required to provide baby monitoring functionality: (a) the CAMERA permission, which allows recording video and taking pictures using the built-in camera, and (b) the RECORD_AUDIO permission, which controls the usage of the device microphone. These permissions are clearly necessary for an app to perform the baby monitoring task and are requested by every app at runtime. However, Table 4 indicates that both the BabyCam and Saby apps may request to write the external storage. Moreover, the Dormi app may want to read the phone state or to write phone settings, and the Saby app may ask to read to external storage. The purpose is unclear in each of these cases, as these permissions are not tied to functionalities in addition to the baby monitoring task. This may indicate excessive use of permissions, which could open the door for potential privacy violations.

Table 4. Dangerous permissions listed in the Android Manifest of baby monitor apps.

Permission	Dormi	BabyCam	Saby	Babyphone Mobile
ACCESS_COARSE_LOCATION	○	●	○	○
ACCESS_FINE_LOCATION	○	●	○	○
CAMERA	●	●	●	●
RECORD_AUDIO	●	●	●	●
READ_EXTERNAL_STORAGE	○	○	●	○
READ_PHONE_STATE	●	○	○	○
WRITE_EXTERNAL_STORAGE	○	●	●	○
WRITE_SETTINGS	●	○	○	○
NEARBY_WIFI_DEVICES	○	●	○	○
POST_NOTIFICATIONS	○	●	●	○

●: Permission listed. ○: Permission not listed.

Therefore, we further investigated additional permissions to identify potential misuse. To investigate suspicious permissions not requested during regular app usage, we associated run-time permission requests with their corresponding functionality (Table 5). If an application did not make a run-time request, the corresponding permission was not required for the functions used. Since this could indicate suspicious usage elsewhere in the execution path and could also be associated with proper functionality that we did not trigger during execution, we examined the decompiled code to rule out misuse.

Table 5. Linkage of suspicious, dangerous permissions, and app functionality.

App	Permission	Requests		Purpose	Required
		Runtime	Code		(Android 12)
Dormi	READ_PHONE_STATE	○	○	-	○
Dormi	WRITE_SETTINGS	○	○	-	○
BabyCam	ACCESS_COARSE_LOCATION	●	●	Wi-Fi Direct	●
BabyCam	ACCESS_FINE_LOCATION	●	●	Wi-Fi Direct	●
BabyCam	WRITE_EXTERNAL_STORAGE	○	●	Image Capture	○
BabyCam	NEARBY_WIFI_DEVICES	○	●	Wi-Fi Direct	○
BabyCam	POST_NOTIFICATIONS	○	●	Push Notifications	○
Saby	WRITE_EXTERNAL_STORAGE	○	●	Image Capture	○
Saby	READ_EXTERNAL_STORAGE	●	●	Image Crop, Bug Report	●
Saby	POST_NOTIFICATIONS	○	●	Push Notifications	○

●: Permission request performed during runtime/Code contains permission request capabilities. ○: Does not exist.

Due to ongoing changes in the Android permission model [39,40], not all permissions specified in an app's manifest are required when running an app on a specific Android version. Therefore, we document whether permission is required to implement a feature in Android 12, the OS version we used during our analysis. As our evaluation shows (Table 5), there is no evidence of misuse of any of the potentially suspicious permissions. The Dormi app does not contain any code at all to query the additionally listed runtime permissions. Although the other apps contain code for requesting additional dangerous permissions, we could associate them with legitimate app functions during code analysis. However, our results were obtained with the caveat that evaluating all possible code paths was not feasible. Therefore, hidden or obfuscated usage may have been missed.

5.2. Device Pairing

Protecting surveillance sessions from unauthorized access should be a key concern for video surveillance solutions. Therefore, the Dormi, Saby, and Babyphone Mobile apps use a pairing workflow to authorize a parent device before accessing a surveillance session. This workflow consists of two to three steps, depending on the application's implementation (Table 6). In the first step, the monitoring device creates a pairing code. In the second step, this code must be entered on the parent device, which then connects back to the child device using the pairing code. By entering the correct pairing code, a monitoring session is established.

Table 6. Pairing mechanisms utilized by the inspected apps when transferring video footage over the Internet.

App	Pairing	Type of Pairing	Confirmation Required
Dormi	●	5-digit code, valid for 120 s.	●
BabyCam	○	-	○
Saby	●	QR-Code, Link, 4-digit code.	●
Babyphone Mobile	●	5-digit code, valid for 30 min.	○

●: Exists. ○: Does not exist.

Although the Babyphone Mobile app does not require additional confirmation of connection requests on the monitoring device, both the Saby and Dormi apps do. Separate confirmation of incoming connections is advantageous, as potential brute-force attacks on the pairing code and the corresponding monitor sessions are effectively mitigated. We propose further investigating how brute-force attacks on pairing codes can lead to session theft and suggest investigating potential attacks in future work. The Babycam app does not use a pairing workflow and grants access to anyone who knows the connection parameters.

5.3. Network Communication

To conduct a privacy assessment and examine the ways in which the selected baby monitoring apps secure their video transmissions, we needed to understand the underlying communication mechanisms. The baby monitor, the device responsible for recording and transmitting video footage, must be placed near the child. Therefore, we assume that the mobile phone used for monitoring purposes is connected to a local Wi-Fi network, e.g., at home or at the hotel. In contradiction, a parental device is expected to be moved around using an Internet connection provided by cellular networks or another Wi-Fi access point. In such a scenario, a direct connection between mobile devices is not feasible. Consequently, before transmitting the monitoring footage, a connection between the baby monitor and the parent device must be established over the Internet. However, since the selected baby monitoring apps are proprietary, their communication mechanisms are opaque, hindering privacy and security evaluation. Therefore, a part of this study explored how app instances communicate with their respective peers. During our analysis, we discovered that in our analysis environment, the baby monitoring apps make use of mainly two different communication mechanisms to transfer video streams. In the following, we describe these two communication mechanisms.

The first communication variant is used by the apps Dormi, Saby, and Babyphone Mobile. Although implemented using different technologies and protocols, the overall communication scheme stays the same. Figure 3 shows this communication scheme.

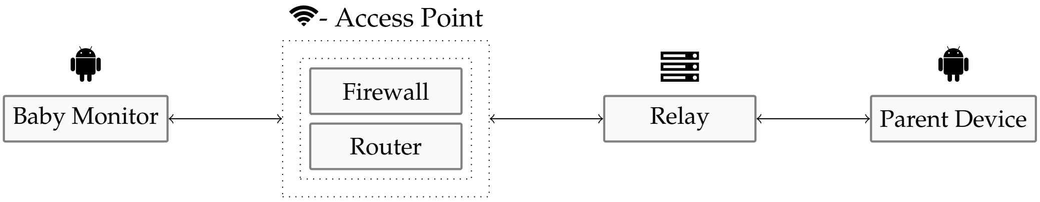


Figure 3. Network communication of the Dormi, Saby, and Babyphone mobile apps.

For each of these applications, the monitoring device and the parent device connect to a relay instance that is reachable via a public IP address. The relay uses the established connections to forward data between mobile devices, allowing data exchange between the monitor and the parent instance. As all data are routed through the relays, the relay operators can access the transmitted video data. However, this privacy threat is mainly mitigated by encryption (see Section 5.5). While the Babyphone Mobile app relies on proprietary binary protocols transported over its servers, the Dormi app exchanges data using servers owned by Google LLC, utilizing a custom protocol to establish a data channel and using the Secure-RTP protocol for video transmission (Table 7). The Saby app uses WebRTC [41] in conjunction with TURN relays [42] operated by Xirsys.

In contrast, the BabyCam app establishes connections between mobile phones differently, favoring a direct connection between the monitoring device and the parental endpoint. The app sets up a server on the child device, which provides the monitoring video streams via HTTP. As the monitoring device is part of the local Wi-Fi network, it is typically secured by a firewall and hidden by NAT techniques. This means that the communication scheme has to overcome complexities such as network address translation (NAT) and security mechanisms in local networks, e.g., the firewall has to allow the corresponding connections and provide port forwarding to the monitoring device. Figure 4 demonstrates this communication mechanism.

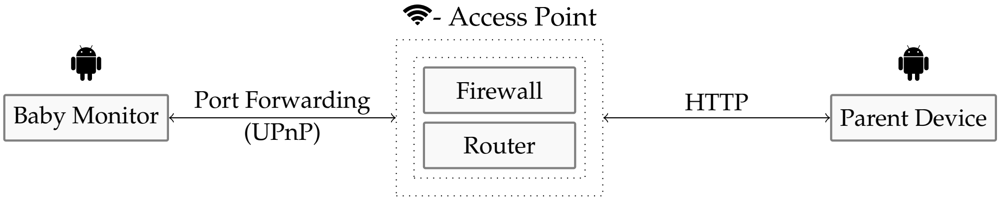


Figure 4. Network communication of the BabyCam app.

During the operation, the BabyCam app checks if it is externally reachable via TCP on port 6060 or port 50002. If it is not reachable, the default settings configure the BabyCam app to send a UPnP query to the firewall, requesting that connections be allowed on these ports, and establishing port forwarding to the own device. We documented the network infrastructure utilized by each application (Table 7); however, the data may be considered volatile.

Table 7. Network infrastructure used for exchanging video footage over the internet.

App	Video Exchange	Domain/IP	Server Owner
Dormi	Relay	34.68.30.36	Google LLC
BabyCam	Client/Server	Local Router	User (App)
Saby	Relay	47.242.47.214	Xirsys
Babyphone Mobile	Relay	bpsvr01.papenmeier.com (194.55.15.124)	Papenmeier Software UG

5.4. Privacy Leaks

By intercepting and decrypting all network connections during a baby monitoring session using a transparent proxy, we got insights into the communication destinations and the actual transmitted data of each monitoring app. In the following, we analyze the data collected for privacy leaks, i.e., the transmission of personal data without providing a legal basis in the privacy policy [7]. For this purpose, we performed a two-step network analysis. First, we evaluated all network connections by collecting communication destinations and the type of personal information transmitted. Second, we matched the identified destinations to companies by using DNS lookups of the domain names so that we were able to compare the collected data with the statements in the respective privacy policy. Since we did not attempt to reverse-engineer encoding or obfuscation attempts of data transmission, which we were unable to interpret, we did not consider those data in our evaluation. However, we identified multiple privacy leaks, which aligns with the results of previous research exploring mobile applications for mHealth or childcare [11,15].

As indicated in Figure 5, there are immense differences in the number of domains and companies contacted and data exchanged between the apps. The Dormi app transfers personal data using Google server infrastructure, but does not mention this in the privacy policy, which we consider a privacy fault. More severely, the BabyCam app states that it collects cookies and tracking elements for use with Google AdSense, but exchanges more than the declared data with numerous advertising companies (see Table 8). Similarly, the Saby app does not mention data exchange with the AppsFlyer Inc. company. The only app without identified privacy leaks is the Babyphone Mobile app.

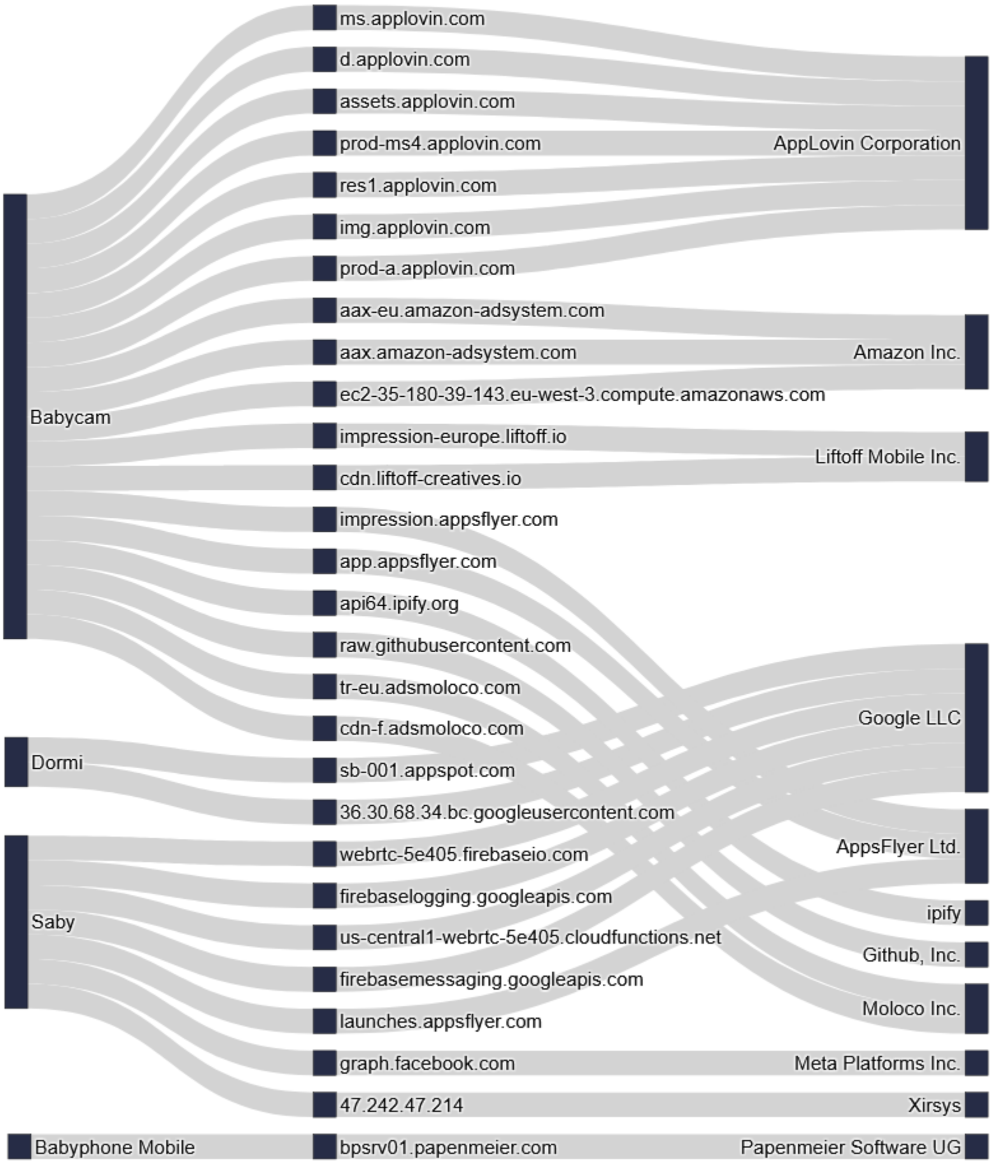


Figure 5. Captured network connections.

Table 8. Exchange of personal information and privacy leaks.

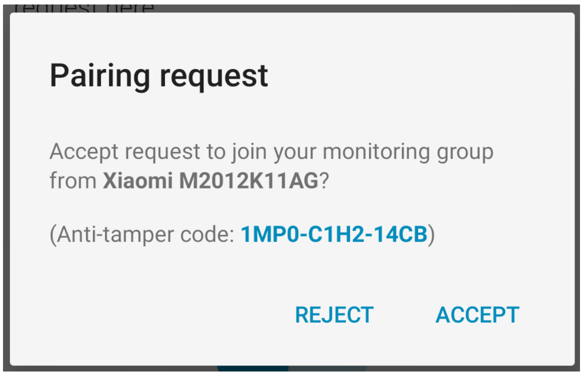
App	**Destination**	**Personal Information**													**Leak**
		IP Address	**Device Name**	**Device UUID**	**Hardware Type**	**Parental Device Name**	**Parental Device UUID**	**User Agent**	**Operating System**	**Country/Language**	**Android Package**	**Ad Id**	**Child Id**	**Monitoring Time**	
Dormi	Google	●	●	●	○	●	●	○	○	○	○	○	○	○	●
BabyCam	Amazon	●	●	○	●	○	○	●	●	●	●	○	○	○	●
	AppLovin	●	○	○	○	○	●	○	○	●	○	○	○	○	●
	AppsFlyer	●	○	○	○	○	○	○	○	○	●	●	○	○	●
	Github	●	○	○	○	○	○	●	○	○	○	○	○	○	●
	ipify	●	○	○	○	○	○	○	○	○	○	○	○	○	●
	Liftoff	●	○	○	○	○	○	●	○	○	●	●	○	○	●
	Moloco	●	○	○	○	○	○	●	○	○	●	○	○	○	●
Saby	Google	●	●	●	○	●	●	○	○	○	○	○	●	●	○
	Meta Platforms	●	●	○	○	○	○	○	○	●	●	●	○	○	○
	AppsFlyer	●	○	○	○	○	●	○	○	○	○	○	○	○	●
	Xirsys	●	○	○	○	○	○	○	○	○	○	○	○	○	●
Babyphone Mobile	Papenmeier Software	●	○	●	○	○	○	○	○	○	○	○	○	○	○

●: Information transferred. ○: Information not transferred.

5.5. Deployed Network Security Measures

As detailed in Section 5.3, we studied a scenario in which baby monitoring apps exchange video footage over untrusted networks, which makes ensuring the confidentiality of the transmitted data significantly relevant. In untrusted networks, ensuring the confidentiality of sensitive data is usually achieved by using transport encryption. Given the sensitive nature of baby monitoring video, video streams should be protected by the approach promising the highest level of confidentiality, which we consider to be end-to-end encryption. End-to-end encryption allows only the intended parties to decrypt the transmitted data, effectively protecting confidentiality against any potential eavesdroppers on the communication path. We aimed to investigate in which way the chosen baby monitoring apps fulfill the demands on video footage protection. To identify the network security measures set up to protect the monitoring video streams, we performed a baby monitoring session using each of the investigated applications and evaluated the created network traffic, supported by insights from manual security analysis. Surprisingly, the BabyCam app does not use any encryption at all, leaving the transferred video footage unprotected against potential eavesdroppers. The Dormi and Saby applications rely on encrypted SRTP data streams to securely transfer video streams, for which an encryption key must be exchanged between the communication parties. While the Saby app utilizes the DTLS protocol mechanisms for key exchange, the Dormi app relies on a proprietary key exchange protocol, which is also based on asymmetric cryptography and public keys. For both key exchange protocols, the identity of the remote peer must be verified to protect it from MitM attacks. The Dormi app uses additional anti-tamper codes that are exchanged during pairing, which the app user verifies in case of a valid connection request (Figure 6), so the remote device can get correctly authenticated.

The Saby app exchanges a hash of the remote peer's certificate over a secured communication path to a signaling server, in this way effectively verifying the identity of the remote peer. Using TLS-secured connections to its relay, the Babyphone Mobile app protects video footage against potential eavesdroppers on the communication path, but not the relay server operators. To hide video footage from server operators, Babyphone Mobile offers optional password-based end-to-end encryption of video data, which requires the user to enter the same password in both app instances. However, the use of encryption is not mandatory. Table 9 summarizes the described network security measures of the applications.



Pairing request

Accept request to join your monitoring group from **Xiaomi M2012K11AG**?

(Anti-tamper code: **1MP0-C1H2-14CB**)

Figure 6. Dormi app: identify verification using an anti-tamper code exchanged during pairing.

Table 9. Identified network security measures in the inspected apps.

App	Data Encryption	Key Exchange	Peer Authentication
Dormi	End-to-End (SRTP)	Proprietary	Anti-tamper code
BabyCam	-	-	Password (optional)
Saby	End-to-End (SRTP)	DTLS	Certificate hash
Babyphone Mobile	TLS End-to-End (optional)	TLS User (Password)	TLS Certificate -

5.6. Assessing the Confidentiality of Video Streams

As mentioned earlier, the audiovisual footage recorded and transmitted by baby monitoring applications is sensitive. As a consequence, ensuring the confidentiality of audiovisual data should be a key concern for baby monitoring applications. However, only two baby monitoring apps state in their privacy policy that they secure their data transmissions without specifying how the data are ultimately secured. For the other apps, the use of security measures remains uncertain. Therefore, we investigated how baby monitoring apps aimed to transmit video footage securely and evaluated these mechanisms for security weaknesses (Section 3). As a result, we identified several security issues that may affect the confidentiality of the video streams, in some cases severely threatening the user's privacy.

5.6.1. Static Code Analysis

Performing automated static code analysis supports security evaluation by providing an overview of possible security issues, guiding further analysis, and identifying evident flaws. We performed the static analysis using MobSF [27] and investigated the issues found by performing a manual code review. The results produced by MobSF indicate a broad surface of possible issues, which are listed in Table 10. However, only a few of them could impact the confidentiality of video streams. The most relevant security issue threatening video confidentiality is the Insecure Implementation of SSL issue in the Saby app. However, we could not confirm this security issue during manual code analysis, so we assume a false-positive report. The same holds true for insecure random number generator issues as well as hard-coded passwords.

In contradiction, findings indicating the use of further vulnerable cryptographic primitives, e.g., the usage of MD5 or SHA1 hash functions or PKCS5 padding, are true-positive security issues. As they do not have a negative impact on video confidentiality, we leave the investigation of their impact open for future work. Our code review shows similar findings for the execution of raw SQL queries and the enabling of code execution in WebView implementations, which are not in the scope of this study. We document our results in Table 10, which shows that none of the issues identified during the static analysis threatens the confidentiality of the monitor streams.

Table 10. Security issues identified in baby monitor apps using MobSF.

Security Issue	Dormi	BabyCam	Saby	Babyphone Mobile
Files may contain hard-coded sensitive information, such as usernames, passwords, keys, etc.	○	○	○	
The app uses SQLite Database and executes raw SQL queries.			◑	
The app uses an insecure random number generator.	○	○	○	○
SHA-1 is a weak hash known to have hash collisions.	◑	◑	◑	
MD5 is a weak hash known to have hash collisions.	◑		◑	◑
Insecure implementation of SSL. Trusting all the certificates or accepting self-signed certificates is a critical Security Hole.			○	
The app can read/write to external storage. Any app can read data written to external storage.		◑	◑	
The app uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	◑			
Insecure WebView implementation. Execution of user-controlled code in WebView is a critical security hole.		◑		
Remote WebView debugging is enabled.		◑		
IP address disclosure.		○		○

◑ : Security issue without impact on video confidentiality. ○: False Positive.

5.6.2. Security Issues Threatening the Confidentiality of Video Streams

Since implementation flaws of network security measures can severely impact the confidentiality of video streams, we conducted a manual security analysis of each baby monitor app, consisting of a code review to identify security issues (Section 3). We uncovered several issues and classified them according to the types of CWE weakness [43]. Where appropriate, we also incorporated our analysis results from previous Sections 5.3, 5.5 and 5.6.1. As Table 11 illustrates, we identified multiple security issues that threaten the confidentiality of video transmissions.

Security Issue #1—Cleartext Transmission of Sensitive Information (CWE-319): As the BabyCam app uses unencrypted HTTP messages to transfer video monitoring streams, sensitive information is transmitted in clear text. It is evident that an eavesdropping attacker can capture the video footage. Moreover, by simply connecting to the app's web server, it is possible to gain access to live video footage directly.

In order to exchange control messages with the relay server, the Dormi app relies on unencrypted messages using the TCP protocol. Therefore, an attacker can eavesdrop on exchanged control-channel messages, including sensitive information, such as mobile device names and unique identifiers.

Security Issue #2—Insufficiently Protected Credentials (CWE-522): The BabyCam app allows configuring password-protected access to the video web server, whereas the password is transferred as a base64-encoded HTTP header value. However, as the utilized HTTP connections transport payloads in clear text, the encoded password is accessible to existing eavesdroppers in the communication channel. This also holds true for an attacker in our threat model, and as the password is base64-encoded, it can be decoded to clear text. Therefore, in our setting, the password feature provides no security benefits at all.

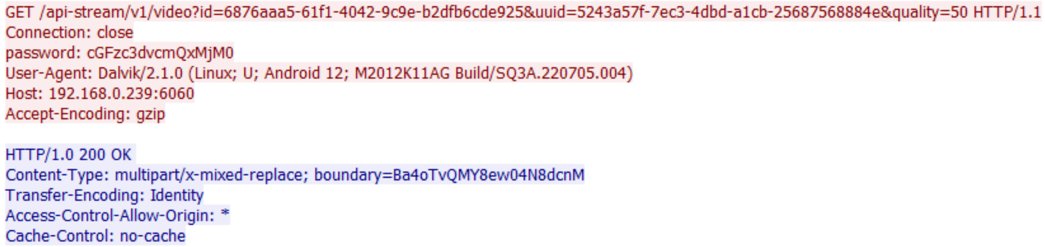
Security Issue #3—Channel Accessible by Non-Endpoint (CWE-300): Security issues of this type occur when the identity of parties at both ends of a communication channel is not correctly verified. This opens up for interception and alteration of exchanged communication, which may result in an attacker masquerading as the original entity, successfully breaking otherwise secure communication channels (MitM attacks).

Although the BabyCam app offers rudimentary password authentication, we previously showed the password is transmitted in clear text, effectively compromising the authentication mechanism and identity verification in a MitM attack. Figure 7 demonstrates this observation.

Similarly, the Dormi app uses an unencrypted control channel to the relay, which is also used for key exchange using a proprietary public key protocol. While the protocol relies on an anti-tamper code for public key verification, the user must manually verify the code. Again, this holds the potential for unnoticed compromise of the key exchange protocol by performing a MitM attack. Furthermore, we found the Dormi app contacts a web server to obtain the relay server IP address; while the connection is TLS-secured, the web server's certificate is not correctly verified. This allows an attacker to perform an unnoticed MitM attack, which may result in the redirection of relay server connections.

Security Issue #4—Weak Password Requirements (CWE-521): Although the Babyphone Mobile app offers optional end-to-end encryption of video streams, it does not mandate the use of end-to-end encryption. In case the user does not set up end-to-end encryption, anyone with access to the HTTPS server can view the monitoring stream.

We elaborated before that password protection in the BabyCam application does not provide any security benefits in our threat model. However, we still consider waiving the use of passwords in the default settings to be a security issue, as potential adversaries not in a MitM position have to overcome the basic authentication mechanism to be able to access the video footage.



```
GET /api-stream/v1/video?id=6876aaa5-61f1-4042-9c9e-b2dfb6cde925&uuid=5243a57f-7ec3-4dbd-a1cb-25687568884e&quality=50 HTTP/1.1
Connection: close
password: cGFzc3dvcmQxMjM0
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; M2012K11AG Build/SQ3A.220705.004)
Host: 192.168.0.239:6060
Accept-Encoding: gzip

HTTP/1.0 200 OK
Content-Type: multipart/x-mixed-replace; boundary=Ba4oTvQMY8ew04N8dcnM
Transfer-Encoding: Identity
Access-Control-Allow-Origin: *
Cache-Control: no-cache
```

Figure 7. BabyCam — unencrypted communication and weak password encoding. The asterisk indicates that the app is allowed to accept cross-origin HTTP requests from all origins.

Based on our results, we evaluated the confidentiality of video footage transmissions for each investigated baby monitoring app (see Table 11), categorizing the apps into three categories depending on the identified security issues: the confidentiality of video footage is fully ensured, the confidentiality may be compromised in certain circumstances, and the confidentiality is not ensured.

Table 11. Confidentiality of Monitoring Streams.

App	Confidentiality	Security issues
Dormi	◑	Clear text transmission of sensitive information (CWE-319). Channel accessible by non-endpoint (CWE-300).
BabyCam	○	Clear text transmission of sensitive information (CWE-319). Insufficiently protected credentials (CWE-522). Channel accessible by non-endpoint (CWE-300). Weak password requirements (CWE-521).
Saby	●	-
Babyphone Mobile	◑	Weak password requirements (CWE-521).

●: Appropriate security measures ensure confidentiality. ◑: Confidentiality may be compromised under some circumstances. ○: Confidentiality of the video footage is not guaranteed.

6. Discussion & Conclusions

Previous work has shown that mobile applications and various video surveillance solutions show deficiencies in the security measures and privacy protections implemented. Analyzing and reporting these weaknesses improves the security and privacy levels of these solutions, e.g., by encouraging manufacturers to fix security weaknesses or informing users about their use of insecure systems. Unfortunately, little work has been performed investigating the security and privacy implications of applications built for video surveillance utilizing mobile phones. Therefore, this study extends previous work in the field of mobile app video surveillance by analyzing the security and privacy implications of the usage of baby monitor apps.

6.1. Security Issues and Their Impact on Video Confidentiality

Our security analysis covered threats to the privacy of the app users, mainly focusing on identifying security issues threatening the confidentiality of monitoring video streams. We reviewed utilized network security measures and performed an automated static code analysis using the MobSF framework, supplemented by a manual code inspection of the investigated app's source code. The most impactful security issue was uncovered during dynamic network analysis. The Babycam app does not encrypt video streams when transferring video footage over the Internet. In contrast, all the other apps examined encrypt video streams, ensuring that potential eavesdroppers cannot compromise confidentiality. Using automated static analysis, we found no security issues directly threatening the confidentiality of video streams. However, the usage of cryptographic primitives should be improved, e.g., MD5 and SHA1 hash functions, as well as PKCBS5 padding, are long known to be vulnerable. Furthermore, issues such as raw SQL queries and user-controlled code in WebView implementations should be inspected and fixed to close potential attack vectors. Our additional manual code review was valuable, as several security issues threatening the users' privacy could be identified. As Table 11 shows, we mainly identified security issues in the establishment of secure channels, correct peer authentication, and authorization. Although we focused on investigating the network security measures that protect sensitive video streams, future work may explore different attack vectors. The proprietary Dormi protocol may be susceptible to downgrade attacks, as legacy app versions that do not use encryption are supported. Due to the proprietary nature of the protocol, flaws may be revealed when fully reverse engineering the protocol. Furthermore, attacks on device pairing that allow for session hijacking may be possible, particularly when there is no user confirmation during the device pairing workflow.

6.2. Privacy Implications of Baby Monitor App Usage

As our security analysis has shown, the confidentiality of transmitted monitor video streams may be compromised, which seriously threatens user privacy. On the contrary, the privacy status of baby monitor apps appears to be overall acceptable. Each app offers a privacy policy, although with differences in completeness and compliance. Interestingly, our analysis of requested permissions indicated that permissions were used correctly, with no excessive or suspicious use. However, a closer look at the privacy policies in conjunction with the analysis of the data exchanged reveals several privacy leaks from baby monitor apps. While the reasons are difficult to determine, we made two observations. First, although it is a valid business model to exchange app features to display ads, identified privacy leaks show that privacy policies do not sufficiently explain the transfer of personal data to advertising partners. Second, the use of (cloud) services is often not sufficiently mentioned in the respective privacy policies.

6.3. Recommendations for Developers

In Section 4, we identified shortcomings in the privacy policies of the apps considered in this study, e.g., the lack of statements on the legal basis of collection and processing of personal data. Recent studies have indicated that app developers are concerned about the strictness of existing privacy regulations that lead to fewer app revenues [44,45], as well as having to compromise when it comes to the use of tracking and advertising services [46]. Furthermore, studies reported that app developers seek help in developer forums on privacy topics primarily when required by legal obligations to understand privacy regulations and communicate their concerns and questions about the collection of personal data or privacy-sensitive permissions [45,47]. While the existing skill set of app developers could lead to the implementation of privacy-friendly practices in apps, disclosing the apps' compliance with existing privacy regulations by writing a privacy policy is not an easy task and requires knowledge about existing often complex and vast privacy regulations. To the best of our knowledge, there exists no study on developers being asked to write a privacy policy for their app, followed by an assessment of its correctness and compliance. A recent study proposed to facilitate the creation of compliant privacy policies for developers by introducing a privacy policy generator [48] called PrivacyFlash Pro, which automatically generates privacy policies based on static code analysis and questionnaires. Since a recent study indicates that common privacy policy generators for mobile apps have shortcomings in, e.g., detecting requested permissions [49], we suggest that app developers use reviewed and tested privacy policy generators, such as PrivacyFlash Pro, but also verify the completeness of the automatically generated privacy policy themselves.

Our security analysis has shown that there are mainly security issues with essential security features, such as building secure channels, proper peer authentication, and authorization. We suggest that developers follow a guide for secure product development offered by the Open Web Application Security Project (OWASP) [50]. This would increase the chances that the developed application would conform to generally accepted security design best practices. Almost all security issues found could be solved by using secure communication in combination with a secure default configuration and adherence to the zero trust principle. Zero trust includes authentication and authorization mechanisms that ensure that only authorized users can access sensitive data and resources.

6.4. Limitations

A relevant part of the presented results was obtained by intercepting and decrypting protected network communication using a proxy. Since MitM attacks on properly secured TLS connections result in connection errors due to failed certificate checks, we disabled certificate checks for the privacy analysis part. We did so by patching app instances using Objection, which alters the application. Alteration of the application may threaten the validity of our investigation, as the behavior of the application may change in response. We compared patched and non-patched monitoring sessions, and to the best of our knowledge, no negative influence could be determined. Moreover, patching Android applications is a widely used technique that has also been used in previous similar work [51].

A weak point of our methodology is the small sample size of only four Android applications. However, published studies of niche applications with few alternatives offered also used a sample of similar size [22], and therefore, we see the fact that all apps have more than 500,000 downloads as a mitigating factor.

Since we did not attempt to reverse engineer encoded or obfuscated data transmissions, we did not consider this data exchange in our evaluation. Therefore, we may have missed registering privacy leaks in these circumstances.

6.5. Conclusions

In addition to offering information on network communication and security measures of proprietary, and therefore, hard-to-assess video surveillance apps, we conducted a security analysis of the network protocols used to monitor video transmission over the Internet, as well as their implementation. For privacy analysis, we evaluated privacy policies and investigated the transfer of personal data regarding privacy leaks. We examined the data practices and compared them to the statements of the respective privacy policies. Although we expected a high level of security and privacy protection due to the privacy-sensitive domain of baby monitoring, this study discloses several security and privacy issues in the most popular baby monitor apps on the Google Play Store. Consistent with previous research results [7–9,11], the identified issues may be considered alarming, as there are no essential security mechanisms in some of the mobile apps examined, threatening user privacy. We responsibly disclosed the issues to the vendors and sent a complete report of our findings to each company, waiting for responses to discuss possible fixes. When evaluating the results of the related work and this study, it becomes evident that further research is needed to improve the state of mobile app privacy. The broad applicability of privacy and security assessments to a wide range of mobile applications would benefit consumers and developers, thus improving the overall level of privacy protection. Future research is required to develop automated security and privacy analysis tools that address the same issues as those examined during this study, focusing on scalability and ease of integration. In the future, additional laborious tasks that currently hinder privacy analysis should be automated, including interpreting encoded or obfuscated data transmissions without the need to reverse engineer proprietary formats manually. We expect that investigations that interpret these data will potentially uncover even more privacy leaks, making any advances in this area fruitful for future studies.

Author Contributions: Conceptualization, L.S. and H.H.; methodology, L.S. and H.H.; software, L.S.; validation, L.S. and H.H.; formal analysis, L.S. and H.H.; investigation, L.S. and H.H.; resources, L.S. and T.H.; data curation, L.S. and H.H.; writing—original draft preparation, L.S., H.H. and T.H.; writing—review and editing, L.S., H.H. and T.H.; visualization, L.S. and H.H.; supervision, T.H.; project administration, T.H.; funding acquisition, T.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the research project "North-Rhine Westphalian Experts in Research on Digitalization (NERD II)", sponsored by the state of North Rhine-Westfalia, Germany–NERD II 005-2201-0014.

Data Availability Statement: A snapshot of the analyzed privacy policies is available at https://github.com/ITSec-WWU-Munster/Security-and-Privacy-of-Baby-Monitor-Apps, accessed on 27 April 2023.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Vagts, H.; Beyerer, J. Security and Privacy Challenges in Modern Surveillance Systems. 2009. Available online: https://www.researchgate.net/publication/41193325_Security_and_privacy_challenges_in_modern_surveillance_systems (accessed on 13 June 2023).
2. Tekeoglu, A.; Tosun, A. Investigating Security and Privacy of a Cloud-Based Wireless IP Camera: NetCam. In Proceedings of the 2015 24th International Conference on Computer Communication and Networks (ICCCN), Las Vegas, NV, USA, 3–6 August 2015; pp. 1–6. [CrossRef]
3. Obermaier, J.; Hutle, M. Analyzing the Security and Privacy of Cloud-based Video Surveillance Systems. In Proceedings of the 2nd ACM International Workshop, Virtual, 18 July 2016; pp. 22–28. [CrossRef]
4. Valente, J.; Koneru, K.; Cardenas, A. Privacy and Security in Internet-Connected Cameras. In Proceedings of the 2019 IEEE International Congress on Internet of Things (ICIOT), Milan, Italy, 8–13 July 2019; pp. 173–180. [CrossRef]
5. Albrecht, K.; Mcintyre, L. Privacy Nightmare: When Baby Monitors Go Bad [Opinion]. *IEEE Technol. Soc. Mag.* **2015**, *34*, 14–19. [CrossRef]
6. Vlachos, V.; Stamatiou, Y.C.; Nikoletseas, S. The Privacy Flag Observatory: A Crowdsourcing Tool for Real Time Privacy Threats Evaluation. *J. Cybersecur. Priv.* **2023**, *3*, 26–43. [CrossRef]
7. Andow, B.; Mahmud, S.Y.; Whitaker, J.; Enck, W.; Reaves, B.; Singh, K.; Egelman, S. Actions speak louder than words: Entity-sensitive privacy policy and data flow analysis with policheck. In Proceedings of the 29th USENIX Security Symposium (USENIX Security'20), Boston, MA, USA, 12–14 August 2020.
8. Zimmeck, S.; Wang, Z.; Zou, L.; Iyengar, R.; Liu, B.; Schaub, F.; Wilson, S.; Sadeh, N.; Bellovin, S.; Reidenberg, J. Automated analysis of privacy requirements for mobile apps. In Proceedings of the 2016 AAAI Fall Symposium Series, Arlington, VA, USA, 17–19 November 2016.
9. Bui, D.; Yao, Y.; Shin, K.G.; Choi, J.M.; Shin, J. Consistency analysis of data-usage purposes in mobile apps. In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual, 15–19 November 2021; pp. 2824–2843.
10. Hussain, M.; Zaidan, A.A.; Zidan, B.B.; Iqbal, S.; Ahmed, M.M.; Albahri, O.S.; Albahri, A.S. Conceptual framework for the security of mobile health applications on android platform. *Telemat. Inform.* **2018**, *35*, 1335–1354. [CrossRef]
11. Papageorgiou, A.; Strigkos, M.; Politou, E.; Alepis, E.; Solanas, A.; Patsakis, C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* **2018**, *6*, 9390–9403. [CrossRef]
12. O'Loughlin, K.; Neary, M.; Adkins, E.C.; Schueller, S.M. Reviewing the data security and privacy policies of mobile apps for depression. *Internet Interv.* **2019**, *15*, 110–115. [CrossRef] [PubMed]
13. Continella, A.; Fratantonio, Y.; Lindorfer, M.; Puccetti, A.; Zand, A.; Kruegel, C.; Vigna, G. Obfuscation-Resilient Privacy Leak Detection for Mobile Apps Through Differential Analysis. In Proceedings of the NDSS, San Diego, CA, USA, 1 March 2017; Volume 17.
14. Valente, J.; Cardenas, A.A. Security & privacy in smart toys. In Proceedings of the 2017 Workshop on Internet of Things Security and Privacy, Dallas, TX, USA, 3 November 2017; pp. 19–24.
15. Gruber, M.; Höfig, C.; Golla, M.; Urban, T.; Große-Kampmann, M. "We may share the number of diaper changes ": A Privacy and Security Analysis of Mobile Child Care Applications. *Proc. Priv. Enhancing Technol.* **2022**, *3*, 394–414. [CrossRef]

16. Liu, E.; Rao, S.; Havron, S.; Ho, G.; Savage, S.; Voelker, G.M.; McCoy, D. No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. *Proc. Priv. Enhancing Technol.* **2023**, *1*, 1–18. [CrossRef]
17. Thankappan, M.; Rifà-Pous, H.; Garrigues, C. Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. *Expert Syst. Appl.* **2022**, *210* , 118401. [CrossRef]
18. Sivaraman, V.; Gharakheili, H.H.; Vishwanath, A.; Boreli, R.; Mehani, O. Network-level security and privacy control for smart-home IoT devices. In Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Milan, Italy, 19–21 October 2015; pp. 163–167.
19. European Parliament, Regulation (EU) 2016/679 (General Data Protection Regulation). 2016. Available online: https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed on 13 June 2023).
20. State of California Department of Justice. California Consumer Privacy Act (CCPA). 2020. Available online: https://oag.ca.gov/privacy/ccpa (accessed on 13 June 2023).
21. Law, V. Consumer Data Protection Act. 2021. Available online: https://law.lis.virginia.gov/vacode/title59.1/chapter53/ (accessed on 13 June 2023).
22. Krehling, L.; Essex, A. A Security and Privacy Scoring System for Contact Tracing Apps. *J. Cybersecur. Priv.* **2021**, *1*, 597–614. [CrossRef]
23. Wilson, S.; Schaub, F.; Dara, A.A.; Liu, F.; Cherivirala, S.; Leon, P.G.; Andersen, M.S.; Zimmeck, S.; Sathyendra, K.M.; Russell, N.C.; et al. The Creation and Analysis of a Website Privacy Policy Corpus. In Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), Berlin, Germany, 7–12 August 2016; pp. 1330–1340.
24. Arora, S.; Hosseini, H.; Utz, C.; Kumar, V.B.; Dhellemmes, T.; Ravichander, A.; Story, P.; Mangat, J.; Chen, R.; Degeling, M.; et al. A Tale of Two Regulatory Regimes: Creation and Analysis of a Bilingual Privacy Policy Corpus. In Proceedings of the 13th Conference on Language Resources and Evaluation, ELRA, LREC 2022, Paris, France, 20–25 June 2022; pp. 5460–5472.
25. Tracking Protection Working Group. Do Not Track. World Wide Web Consortium(W3C). 2012. Available online: http://www.w3.org/2011/tracking-protection (accessed on 13 June 2023).
26. Callegati, F.; Cerroni, W.; Ramilli, M. Man-in-the-middle attack to the HTTPS protocol. *Secur. Privacy IEEE* **2009**, *7*, 78–81. [CrossRef]
27. Abraham, A. Mobile Security Framework (MobSF). 2023. Available online: https://github.com/MobSF/Mobile-Security-Framework-MobSF (accessed on 13 June 2023).
28. Skylot. jadx-Dex to Java Decompiler. 2023. Available online: https://github.com/skylot/jadx (accessed on 13 June 2023).
29. Cortesi, A.; Hils, M.; Kriechbaumer, T. (contributors) *Mitmproxy: A Free and Open Source Interactive HTTPS Proxy*, version 9.0. Available online: https://github.com/mitmproxy/mitmproxy (accessed on 13 June 2023).
30. Sensepost, O.C. Objection-Runtime Mobile Exploration. 2023. Available online: https://github.com/sensepost/objection (accessed on 13 June 2023).
31. Kuner, C.; Bygrave, L.; Docksey, C.; Drechsler, L. *The EU General Data Protection Regulation (GDPR): A Commentary*; Oxford University Press: Oxford, UK, 2020.
32. Kazemi, R. *General Data Protection Regulation (GDPR)*; Tredition: Hamburg, Germany, 2018.
33. O'Kane, P. *A Practical Guide to Managing GDPR Data Subject Access Requests*, 2nd ed.; Law Brief Publishing: Somerset, UK, 2022.
34. Vrabec, H.; Uršič, H. *Data Subject Rights under the GDPR: With a Commentary through the Lens of the Data-Driven Economy*; Oxford University Press: Oxford, UK, 2021.
35. Voigt, P.; von dem Bussche, A. *The EU General Data Protection Regulation (GDPR): A Practical Guide*; Springer International Publishing: Berlin/Heidelberg, Germany, 2017.
36. Party, A.W. Guidelines on Transparency under Regulation 2016/679. 2018. Available online: https://ec.europa.eu/newsroom/article29/items/622227/en (accessed on 20 April 2023).
37. Alepis, E.; Patsakis, C. Hey doc, is this normal?: Exploring android permissions in the post marshmallow era. In Proceedings of the Security, Privacy, and Applied Cryptography Engineering: 7th International Conference, SPACE 2017, Proceedings 7, Goa, India, 13–17 December 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 53–73.
38. Android Open Source Project Request Runtime Permissions. Available online: https://developer.android.com/training/permissions/requesting (accessed on 13 June 2023).
39. Android Open Source Project Storage updates in Android 11. 2023. Available online: https://developer.android.com/about/versions/11/privacy/storage (accessed on 13 June 2023).
40. Android Open Source Project Android 13 Features and Changes List. 2023. Available online: https://developer.android.com/about/versions/13/summary (accessed on 13 June 2023).
41. Rescorla, E. WebRTC Security Architecture. RFC 8827, RFC Editor, 2021. Available online: https://datatracker.ietf.org/doc/rfc8827/ (accessed on 13 June 2023).
42. Mahi, R.; Matthews, P.; Rosenberg, J. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). RFC 5766, RFC Editor, 2010. Available online: https://datatracker.ietf.org/doc/rfc5766/ (accessed on 13 June 2023).
43. MITRE Corporation Common Weakness Enumeration. 2023. Available online: https://cwe.mitre.org/ (accessed on 20 April 2023).
44. Alomar, N.; Egelman, S. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proc. Priv. Enhancing Technol.* **2022**, *4*, 24. [CrossRef]

45. Li, T.; Louie, E.; Dabbish, L.; Hong, J.I. How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit. *Proc. ACM Hum.-Comput. Interact.* **2021**, *4*, 1–28. [CrossRef]
46. Ekambaranathan, A.; Zhao, J.; Van Kleek, M. "Money makes the world go around": Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan, 8–13 May 2021; pp. 1–15.
47. Parsons, J.; Schrider, M.; Ogunlela, O.; Ghanavati, S. Understanding Developers Privacy Concerns Through Reddit Thread Analysis. *arXiv* **2023**, arXiv:2304.07650.
48. Zimmeck, S.; Goldstein, R.; Baraka, D. PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps. In Proceedings of the NDSS, Online, 21–25 February 2021.
49. Pan, S.; Zhang, D.; Staples, M.; Xing, Z.; Chen, J.; Xu, X.; Hoang, J. A Large-scale Empirical Study of Online Automated Privacy Policy Generators for Mobile Apps. *arXiv* **2023**, arXiv:2305.03271.
50. OWASP® Foundation Secure Product Design Cheat Sheet 2023. Available online: https://cheatsheetseries.owasp.org/cheatsheets/Secure_Product_Design_Cheat_Sheet.html (accessed on 13 June 2023).
51. Pradeep, A.; Paracha, M.T.; Bhowmick, P.; Davanian, A.; Razaghpanah, A.; Chung, T.; Lindorfer, M.; Vallina-Rodriguez, N.; Levin, D.; Choffnes, D. A Comparative Analysis of Certificate Pinning in Android & IOS. In Proceedings of the 22nd ACM Internet Measurement Conference, IMC'22, Nice, France, 25–27 October 2022; Association for Computing Machinery: New York, NY, USA, 2022; pp. 605–618. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.