Surveillance Disguised as Protection: A Comparative Analysis of Sideloaded and In-Store Parental Control Apps

Eva-Maria Maier
St. Pölten UAS
Austria
eva-maria.maier@proton.me

Leonie Maria Tanczer
University College London
United Kingdom
l.tanczer@ucl.ac.uk

Lukas Daniel Klausner
St. Pölten UAS
Austria
mail@l17r.eu

Abstract

Parental control applications, software tools designed to manage and monitor children's online activities, serve as essential safeguards for parents in the digital age. However, their usage has sparked concerns about security and privacy violations inherent in various child monitoring products. Sideloaded software (i. e. apps installed outside official app stores) poses an increased risk, as it is not bound by the regulations of trusted platforms. Despite this, the market of sideloaded parental control software has remained widely unexplored by the research community. This paper examines 20 sideloaded parental control apps and compares them to 20 apps available on the Google Play Store. We base our analysis on privacy policies, Android package kit (APK) files, application behaviour, network traffic and application functionalities. Our findings reveal that sideloaded parental control apps fall short compared to their in-store counterparts, lacking specialised parental control features and safeguards against misuse while concealing themselves on the user's device. Alarmingly, three apps transmitted sensitive data unencrypted, half lacked a privacy policy and 8 out of 20 were flagged for potential stalkerware indicators of compromise (IOC).

Keywords

application analysis, dual-use applications, mobile security, parental control, sideloading, stalkerware

1 Introduction

Parental control systems are increasingly used by parents[1] to protect their children's safety, security and privacy.[2] They can be classified into time, content and activity restricting as well as monitoring and tracking services [125]. They often provide functionalities such as logging and limiting screentime, browser history monitoring and blocking of apps [116]. According to a report by Internet Matters, around 80% of parents in the United Kingdom (UK) use at least one form of parental control, with broadband controls and mobile phone applications ("apps") being among the most widely adopted solutions [122].

The prevalence of smartphones and tablets among minors has heightened the importance of parental control apps and made these tools commonplace [79, 81]. Studies show that some parents view monitoring tools not only as helpful instruments but as a necessity for responsible parenting [60, 80]. This form of "care surveillance" has been studied extensively [20, 32, 126]. It is reinforced by research indicating that a lack of parental control over a minor's smartphone escalates the risk of children becoming victims of online harassment [102], while understanding how children interact with digital media can help reduce family conflict [66].

While there are many reasons for parents to consider using such apps, concerns have been raised about security and privacy violations in child monitoring products. Feal et al. [41] discovered that parental control apps lack transparency and do not comply with regulatory requirements. Ali et al. [3] and Largent [71] disclosed several vulnerabilities in such software, including remote code execution, authentication bypass and device malfunction. Whittaker [120] reported on a major data breach leaking thousands of user passwords in a teen phone monitoring app. In response to such findings, children's rights advocates, including the 5Rights Foundation, criticised the absence of comprehensive online protection legislation for children, condemning the existence of products and services that pay little regard to the welfare of young people and minors [45].

Deploying parental control systems unavailable on official platforms, such as the Google Play Store, calls for special consideration. Users can acquire alternative apps by downloading them from third-party websites and installing them on their device after granting the necessary permissions. These so-called *sideloaded apps* offer parents additional functionalities such as extensive uninstallation restrictions and hiding their presence through stealthiness and obfuscation [67]. Users of such sideloaded services can therefore implement parental controls in scenarios where their child opposes or circumvents monitoring measures [64, 119].

Sideloaded apps can introduce additional privacy and security risks that parents might not be aware of. The providers of sideloaded services are not required to follow app store policies, which restrict or prevent the misuse of Android Application Programming Interface (API) capabilities, remote control and similar functionalities [52]. Both Apple and Google review apps before allowing them on their stores. Apple uses a team of experts that rejected 27% of apps in 2022, while Google relies on automation and real-time scanning for security [85]. Sideloaded apps operate without the safeguards and standards set by such platforms, increasing the risks of data leakage, outdated software and the absence of robust encryption protocols.

---

[1] We use the term "parent" to refer to the adults entrusted with the responsibility of caregiving and guardianship, including parents *stricto sensu*, legal guardians and other adults playing a central role in a child's upbringing.

[2] For the purpose of our paper, "safety" refers to protection against dangers and harm, "security" involves protecting children from online threats and "privacy" encompasses children's data protection.

Another consideration relates to parents inadvertently installing dual-use apps or stalkerware/spyware[3] marketed as parental control tools on their children's devices [81]. Not all parents may fully understand the implications of using sideloaded apps, especially when encountering them through channels such as advertisements or recommendations outside official app stores. While both stalkerware and parental control apps can monitor a person's activities, the key difference lies in a product's aim for secrecy and intent: Stalkerware often conceals its presence and operates without the user's knowledge or consent [62]. Indicators of compromise (IOC) for stalkerware (see subsection 5.7) have therefore been collected and provided by different sources [61, 77].

Given the potential hazards of these technologies and the need for heightened protections for vulnerable groups like children [44], our paper seeks to shed light on the sideloaded parental control app ecosystem. Sideloaded apps occupy a unique and underexplored niche in the broader app landscape. Vendors often justify sideloading as a means to navigate challenges posed by official app stores, including strict regulatory requirements. These apps also provide parents with tools that are harder for children to outmanoeuvre and allow vendors to avoid app store fees [18, 85]. Despite their prevalence, precise data on the size and impact of this sideloaded app domain remains scarce (see subsection 4.3).

Our focus is specifically on Android-based systems, which held approximately 70% market share in the first quarter of 2024 [105] and where sideloading is a common and relatively straightforward process. By contrast, sideloading is far less prevalent on iOS devices, where app distribution is tightly controlled, and sideloading requires rooting [55]. Yet, this dynamic may shift as the European Union's (EU) Digital Markets Act (DMA)[4] is increasingly enforced [9]. This regulatory backdrop, coupled with the distinct risks associated with sideloaded apps, highlights the urgency of examining this ecosystem in depth. The driving research questions for our study, therefore, were:

Q1: How do sideloaded parental control apps compare to Google Play Store parental control apps in terms of permissions, trackers, functionalities and obfuscation techniques?

Q2: How clearly and transparently do sideloaded parental control apps communicate their privacy and data collection practices to users within their privacy policies?

Q3: How do sideloaded parental control apps handle encryption and sensitive data transmission?

Q4: How many sideloaded parental control apps match common stalkerware indicators of compromise (IOC)?

2 Background

Parental control apps serve as an element of guardianship, frequently acting as a protection mechanism for parents to ensure a safe and secure online environment for their children. Indeed, parents currently face various challenges in their duty of care. Minors who engage with internet-enabled services can be subjected to harmful behaviour and may end up being confronted with cyberbullying, online grooming, inappropriate content and various forms of scams [30, 60, 112]. Teens who have encountered such issues are also more likely to be closely supervised by their parents [49] and contextualise these privacy-invasive behaviours differently when they occur via electronic means [68].

2.1 Dataveillance

A downside of children being monitored by and engaging with digital technologies is that they have become subject to many surveillance systems, emphasising the urgency of addressing children's rights and holding industry actors responsible. Technologies spanning from mobile games and wearables to educational software generate extensive data about children, capitalising on and profiting from their personal information [76]. While children may not always fully understand practices of datafication,[5] they care about its various aspects and want to be able to stop their data from being used in ways unknown to them [117]. Children's rights instruments that address the risks and harms of data surveillance remain an area for improvement [76], with UNICEF arguing for children's data protection responsibility also falling onto tech vendors [57].

2.2 Misuse

Besides the risks associated with parental control apps processing children's data, concerns arise about their implemented monitoring capabilities that make them susceptible to misuse. Child monitoring apps often offer features like location tracking, message monitoring and call log access – functionalities that could potentially be exploited by malicious actors [65]. This dynamic raises the critical issue of parental control apps serving as a dual-use technology. Chatterjee et al. [25] define dual-use apps as software designed for a legitimate use case that can be misused by an abuser, such as a perpetrator of intimate partner violence (e. g. because their capabilities permit another person remote access to a device's data without the device user's knowledge). Past literature has established that some parental control apps, as well as Bluetooth Trackers, can and have been repurposed [25, 47, 58, 83], especially if not enough precautions are put in place [65].

2.3 Marketing Shift

Some stalkerware products have been revealed to advertise themselves or particular functionalities as parental control [25, 27, 83]. This is problematic, as these products not only mislead users but also typically invest minimal effort in securing the sensitive data they collect [50, 73, 77]. Recent data breaches and court rulings confirm this [40]. For instance, the hacking of two stalkerware firms in 2018 exposed private text messages containing conversations between children and their parents or spouses. One text read "You cheated….smh…", while others appeared to be written by children about issues at school [29]. Furthermore, the United States of America (US) Department of Justice's 2014 criminal indictment against the makers of the spyware app StealthGenie appears to

---

[3] There are different definitions for the terms "stalkerware" and "spyware", and there is currently no consensus on their key features [10]. However, spyware is generally a broader term encompassing various types of software, including adware, keyloggers and rootkits [43]. We use "stalkerware" to characterise any software falling under the mentioned categories, except when we cite articles explicitly using the term "spyware".

[4] The DMA restricts the influence of major digital platforms acting as gatekeepers by mandating that companies like Apple permit software from outside their app stores and submit annual reports on DMA compliance [36].

[5] "Datafication" here includes the recording, tracking, aggregating, analysing and exploiting of children's online actions for purposes such as monetisation [118].

have prompted some vendors to shift their marketing focus. Rather than targeting "cheating partners", they now emphasise the more "legitimate" monitoring of minors or employees [73].

3 Related Work

This section summarises the literature on in-store parental control and children's apps. Since there is limited research on the side-loaded parental control market, we also include studies that focus on stalkerware apps, as many of these are marketed as parental control tools. Additionally, we look at past publications on recommendations for parental control software developers.

3.1 Research on In-Store Parental Control Apps

In-store childcare and children's apps showcased a lack of transparency and compliance with regulatory requirements. Feal et al. [41] studied the Android parental control app ecosystem and discovered that 34% of the tested apps sent personal information without appropriate consent and 72% shared data with third parties without stating this in their privacy policies. They raise the question of whether protecting children justifies the risks regarding the collection and processing of their data. Okoyomon et al. [91] substantiated these findings by observing that 10% of over 68,000 apps on the Google Play Store's Designed for Families program share data, including personal identifiers, with third parties without declaring this in their privacy policies. By conducting a privacy policy analysis, they also found that 9.1% did not acknowledge that they targeted kids or did not even mention them in their privacy policy. Additionally, interviews have shown that many developers lack a good understanding of their own apps' data collection behaviour due to the use of third-party software development kits,[6] often leading to unintentional violations of privacy regulations [5].

Many children-focused apps use tracking libraries and require a large number of permissions, including ones classified as dangerous by the Android protection levels. For instance, Sun et al. [107] concluded that 81.25% of family apps use trackers, while Gruber et al. [56] found that 45% use more than two trackers. Concerning permissions, Gruber et al. [56] calculated a mean of 19 potentially dangerous permission per app. Sun et al. [107] discovered that 4.47% of children's apps request location permissions, despite the platforms prohibiting the collection of children's location data.

Researchers have brought to light a myriad of vulnerabilities that undermine children's online and offline safety. Ali et al. [3] exposed pervasive security and privacy issues, including improper access control, the possibility of online password brute-forcing, vulnerable backends and lack of encryption. Blancaflor et al. [14] also detected apps sending unencrypted data and further identified 18 unique vulnerabilities in three popular apps based on Open Worldwide Application Security Project (OWASP) security requirements.

3.2 Research on Dual-Use Apps and Stalkerware

Prior research has extensively documented the entrenched issue of dual-use and stalkerware apps, particularly within the realms of parental control and domestic abuse. Almansoori et al. [4] showcased the prevalence of dual-use apps exploited in intimate partner

surveillance on the Google Play Store, identifying 3,988 out of 51,868 apps as dual-use, with many categorised as parental control. They noted that many more dual-use apps may be distributed outside official platforms, calling for future research into the prevalence of sideloaded versions. Chatterjee et al. [25] explored apps used in intimate partner violence cases, including 23 sideloaded apps unavailable on official stores, many of which belonged to the child monitoring and subordinate tracking categories.

Investigations have also scrutinised the promotion and monetisation tactics employed by spyware vendors. Molnar and Harkin [83] found that spyware is frequently marketed for both malicious and ostensibly "credible" purposes, such as parental control – though the monitoring capabilities often exceed appropriate levels. Their content analysis revealed that multiple apps advertising child monitoring also promoted spying on intimate partners. Complementing this, Gibson et al. [50] analysed over 6,400 spyware apps, showcasing not only their diverse revenue generation strategies but also the broader ecosystem of payment processors that sustains this surveillance industry. Researchers have further exposed security flaws and data protection failures within these types of apps. Technical analyses of stalkerware by Liu et al. [73] and Mannan and Youssef [78] included apps advertised as parental control, providing insights into the abuse of Android APIs, functionalities and security shortcomings.

Our present work builds on these prior studies, examining how the parental control market overlaps with stalkerware. Six of the apps reviewed by Liu et al. [73] are also part of this paper, as well as eleven of the apps analysed by Mannan and Youssef [78]. By expanding on their research and incorporating an examination of privacy policies and IOCs, our research offers additional insights and extends their findings.

3.3 Recommendations and Best Practices

In the face of the unveiled issues in children's and parental control software, regulators created recommendations for software developers handling children's and other vulnerable communities' data [19]. The eSafety Commissioner, an independent Australian regulator [34], formulated safety-by-design principles. These emphasise the responsibility of service providers to reduce their users' exposure to harm. They further demand user empowerment and autonomy to support safe online interactions and advocate for transparency and accountability in the tech sector. Other resources propose similar measures, such as the child-rights-by-design principles created by the aforementioned 5Rights Foundation [75].

Literature has also provided guidance and best practices for parental control. Gnanasekaran and De Moor [51] conducted a literature review which yielded nine recommendations, split into the categories of usability, security and privacy. The security recommendations include increasing awareness amongst children and parents and following security standards and procedures. The privacy recommendations suggest monitoring children's activity in non-intrusive ways, making it clear what parents consent to in terms of data sharing and granting parents access to the children's data to delete or restrict data collection by an app.

---

[6] A software development kit (SDK) is a set of tools and resources that enables developers to create apps for a specific platform or framework.

3.4 Research Gap

While the Background section highlighted that there are publications on in-store parental control apps and stalkerware, including dual-use parental control, little is known about the sideloaded parental control industry. Prior work on parental control apps primarily focused on software available through official app stores [41, 91], excluding sideloaded software. This lack of research implies the existence of an evidence gap in the understanding of the risks, privacy concerns and functionalities associated with the sideloaded parental control ecosystem. Considering the issues uncovered by prior literature, it can be assumed that the situation for sideloaded apps is likely similar, if not worse. Sideloading presents increased risks due to issues unique to sideloaded apps, including the dearth of independent oversight by an official app store, the lack of user ratings and reviews to inform users and the inability to provide regular, automatic updates. Besides, the absence of robust studies, which scholars like Almansoori et al. [4] called for, may hinder the development of informed policies and guidelines for the responsible design and the ethical use of such apps moving forward.

4 Methodology

We selected a comparable sample size of sideloaded and Google Play Store parental control apps. We then assessed these apps against stalkerware indicators of compromise (IOC) provided by Tiny-Check's [26] GitHub repository. A static analysis was conducted on both sideloaded and in-store apps, followed by a comparative analysis of their features. We further collected and analysed their network traffic data and privacy policies and compared the data-sharing practices outlined in the policies with the actual network traffic observed. The data collection encompassed the period from May to November 2024.

4.1 Selection Process of Sideloaded Apps

We conducted a Google web search using a list of 15 phrases (see Appendix A) that parents might use when seeking a legitimate parental control solution. To exclude results from the Google Play Store, we added the term "-site .google.com". We manually analysed the first 60 results of each search query, as Google automatically stops loading websites after this point and the results tend to be less relevant. Any tools mentioned across a cumulative total of 900 results were documented to obtain an extensive list of all currently relevant software in the parental control software market, resulting in a total of 132 tools. We further narrowed this set of software down to only include Android apps that are not available on the Google Play Store. After subtracting tools that were no longer accessible, we were left with 44 Android apps. These were further inspected to exclude apps that redirect to or were purchased by other parental control services already on the list. Excluded were Refog (part of Aura, available on Google Play Store), Circle (redirects to FlexiSpy), MobileSpy (redirects to mSpy) and Spynger[7] (acquired by mSpy, as confirmed by their support staff). Subsequently, the list was sorted according to the Tranco rankings of each app's official website [96] (see subsection 4.3), with 20 websites ranking among the top 1 million most visited and popular sites on the internet.

---

[7] On their website, Spynger advertises itself as the "best cheating app" and promotes spying on your partner if there are suspicions of infidelity.

Due to their lower visibility and relevance, apps without a Tranco score (i. e. not among the first 1 million websites) were disregarded. Eleven apps that did not offer a free version or trial period were purchased, with prices ranging from €23.28 to €59.99. Paying for the apps was necessary to ensure a representative analysis of the sideloaded market without omitting popular options. While this included transactions with companies that could be considered as offering stalkerware (see subsection 5.7), it was necessary to gain insights into the potential risks associated with such software and to advance the current knowledge on the subject. The resulting 20 apps analysed in this paper were Bark, mSpy, Spapp Monitoring, Hoverwatch, AnyControl, uMobix, TheOneSpy, Kidlogger, FlexiSpy, XNSPY, TiSpy, SPYX, WebWatcher, MoniMaster, Cocospy, iKeyMonitor, SPY24, Chyldmonitor, EvaSpy and Kidstracker (listed in order of descending Tranco ranking).

4.2 Selection Process of Google Play Store Apps

To select Google Play Store apps, we employed the same search terms used for sideloaded apps (see Appendix A). The results were manually filtered to identify apps intended for child devices, replacing parent versions with their child counterparts. During this process we encountered two cases where the parent app was available on the Google Play Store while the child app could only be downloaded from the vendor's website: AirDroid Parental Control and FlashGet Kids: Parental Control. Prior to selecting the apps with the highest download numbers, we excluded apps tailored to one specific service, such as the Nintendo Switch Parental Controls or YouTube Kids. Two more apps were excluded because they offered significantly fewer features, limited to GPS tracking and few additional functionalities, making them unsuitable for direct comparison with both sideloaded and in-store parental control apps. We picked a sample size of 20 apps, corresponding to the number of sideloaded apps: Life360, iSharing: GPS Location Tracker, Pingo, Kids Place Parental Control, Kaspersky SafeKids with GPS, Alli360, Parental Control – Kidslox, ST Kids App, Spy Phone Labs Phone Tracker, KidControl Family GPS locator, Kids App Qustodio, MMGuardian Child Phone App, Parental Control Kroha, Microsoft Family Safety, ESET Parental Control, MobileFence, Tigrow!, FamiSafe Kids, FamilyTime Jr. and Kidsy (listed in descending order of approximate download numbers from the Google Play Store).

4.3 Popularity

To estimate the popularity of sideloaded parental control, we utilise the Tranco rankings taken on 2 June 2024 because app usage numbers reported on websites are considered unreliable as they tend to exaggerate their customer base [83]. Of the 20 apps, the most popular one is Bark with a score of 10,840. To put this number into perspective, samsungmobile.com (scoring 10,856) and nintendo.de (scoring 10,835) rank similarly. Four apps are ranked among the top 100,000 websites, nine among the top 300,000 and 16 among the top 500,000. Another metric that can be used to estimate the prevalence of these tools is data breaches: security researchers found over 60,000 users registered with XNSpy [121], and another breach unveiled 130,000 accounts on Retina-X and FlexiSpy [46]. A recent incident in May 2024 exposed the databases of mSpy, leaking almost 2.4 million unique emails [7].

4.4 Setup

The setup consisted of an emulated Android device with an API level of 31 which corresponds to Android 12.0. This API level was chosen due to being widely supported by developers, increasing the likelihood of the app features working on the emulator.[8] For each sideloaded app a new emulated device was set up and the parental control app was subsequently installed using the APK file (i. e. Android package kits, used to distribute apps on the Android operating system) downloaded from the vendor's website. In-store parental control apps were tested on a physical device running Android 9.0. None of the studied apps required a rooted device. The vendors of sideloaded apps typically provided a dashboard displaying the monitored data on their website, while in-store vendors were more likely to offer a second app or mode for parents. Charles Proxy [98] was used to capture and analyse network traffic, including HTTPS traffic. To decrypt the traffic, Charles Proxy certificates were installed on the emulators. For apps using certificate pinning[9], we used Frida [48], a toolkit that injects custom scripts into running apps to bypass certificate pinning. All apps were downloaded and tested in Austria, consequently requiring the vendors to adhere to the General Data Protection Regulation (GDPR), which applies to all mobile apps that collect and process the personal data of EU citizens (regardless of whether the processing occurs in the EU) [38]. The emulator's GPS was enabled and set to a location in Austria.

The apps were installed in line with the installation guides provided by the parental control vendors. The features of each app were tested by manually interacting with the phone for approximately thirty minutes. In this period, user behaviour was mimicked by engaging with different installed apps, browsing websites, downloading content, taking pictures, receiving and making calls, receiving and writing SMS messages and so on.

4.4.1 Obtaining Google Play Store APKs. To conduct a static analysis, we first required the APK files of the Google Play Store apps. We employed an Android emulator using a Google Play image, which allowed us to install the selected apps on the emulator directly. Using the Android Debug Bridge (adb) [31], we then determined the app package and its path and extract it from the emulator. In the case of split APKs, which are multiple APK files making up one app to optimise file size and delivery for different device configurations, we merged the split files using the open-source tool APKEditor [100].

4.5 Privacy Policies

The presence of a privacy policy on the vendor's website, in the Google Play Store or in the app was evaluated to ensure that both parties involved, such as parents and children, receive clear information regarding the app's privacy practices. The policies were analysed in a word-by-word textual examination.

We extracted the following information from the policies: length, Flesch reading ease score [42], last update, scope, type of collected

data, sharing with third parties including mentioned third parties and reasons for sharing, user rights and contact info. This analysis was performed manually. We further categorised the policy scope into five groups to assess its relevance to the user. This is a slight modification of the categorisation used by Sunyaev et al. [108]:

(1) Website only: Policy covers only the website.
(2) App only: Policy covers only the app under test.
(3) Multiple apps: Policy covers multiple apps by the same vendor, including those under test.
(4) All company-based services: Policy covers all services the vendor offers.
(5) No relation: No relation was found between the policy and the app under test.

The Flesch reading ease score assesses the ease of understanding a written text based on sentence length and the number of syllables per word. It ranges from 0 to 100; the higher the score, the easier the text is to understand. The online tool Flesch Kincaid Calculator [21] was used for the calculation.

4.6 Static Analysis

To conduct a static analysis, we reviewed the APK files with Exodus [97] and MobSF [82], which provided output for deeper examination. Security researchers frequently employ MobSF to conduct security analyses on mobile apps [94] as it can identify a wide range of Android security issues [99]. Exodus has also been used by cybersecurity companies [103] and researchers [70]. We used both tools to conduct a static analysis of the parental control apps without executing them. This involves automated analysis of the manifest files, source code and assets to identify specifications and security vulnerabilities. We compared the generated lists of permissions, app libraries, trackers and general technical information wherever applicable. We further split the permissions into potentially dangerous permissions and other categories, based on the protection levels specified by Android [6].

5 Results

The next section presents our analysis of 20 sideloaded parental control apps and 20 Google Play Store parental control apps. We first outline the results of our app analysis, followed by the examination of their privacy policies and network traffic. Last, we spotlight our findings regarding stalkerware IOC.

5.1 Static Analysis

All APK files were subjected to static analysis using both Exodus and MobSF. We compared the results from these tools and resolved discrepancies. This included cases where the number of trackers identified differed between the two tools or where MobSF detected additional permissions that Exodus did not. The key findings from this analysis are presented in two separate tables. Table 1 covers the apps available on the Google Play Store and Table 2 focuses on sideloaded apps.

5.1.1 Trackers. Our analysis revealed that Google Play Store apps generally have more trackers than sideloaded apps. On average, sideloaded apps had 1.8 trackers, with a range from zero to five, whereas in-store apps averaged 4.2 trackers. iSharing: GPS Location

---

[8] The AnyControl app had to be installed on a physical device (using Android 12.0) because it was built for ARM architecture, which is incompatible with an x86_64 emulator.
[9] A security technique where the app is configured to only trust a specific certificate, thus preventing the capture of unencrypted traffic with the help of unauthorised certificates.

Tracker had the most trackers, totalling nine. We identified 15 different trackers among the sideloaded apps. The most frequently used were Google CrashLytics, present in nine apps, and Google Firebase Analytics, which appeared in eleven apps. The Google Play Store apps contained 22 unique trackers. Google CrashLytics and Google Firebase Analytics remained the most popular ones, with 18 and 16 occurrences respectively. A more detailed breakdown can be found in Table 4.

Table 1: Static Analysis of Google Play Store Apps

App Name	Downloads	Permissions	Dangerous Permissions	Tracker	Obfuscation	IOC Match
Alli360	1M+	34	10	4	N	
ESET Parental Control	1M+	31	10	1	N	
FamilyTime Jr	100k+	37	13	3	N	
FamiSafe Kids	500k+	38	15	8	N	
iSharing	10M+	35	16	9	N	
Kaspersky SafeKids	1M+	48	8	6	N	
KidControl	1M+	25	6	4	N	
Kids Place	5M+	37	10	4	N	
Kidslox	1M+	42	16	7	N	
Kidsy	100K+	33	12	3	N	
Kroha	1M+	39	12	3	N	
Life360	100M+	42	18	5	N	●
Microsoft Family Safety	1M+	22	9	3	N	
MMGuardian	1M+	45	17	7	N	
MobileFence	1M+	58	19	2	N	
Pingo	10M+	35	12	3	N	●
Qustodio	1M+	27	5	3	N	
Spy Phone Labs Phone tracker	1M+	15	5	0	N	●
ST Kids App	1M+	27	11	7	N	
Tigrow	500k+	27	12	1	N	

Abbreviations: N = No, IN = Icon and Name, NO = Name Only

5.1.2 Permissions. Compared to parental control apps available on the Google Play Store, sideloaded parental control apps request significantly more permissions. On average, sideloaded apps requested 44.4 permissions, whereas in-store apps averaged 34.9 permissions. The range of requested permissions for sideloaded apps varied from 22 to 70, with mSpy requiring the most. For Google Play Store apps, the range was from 15 to 58 permissions, with Mobile Fence requesting the most.

Regarding permissions classified as dangerous by Android, sideloaded apps similarly request more, averaging 21 dangerous permissions compared to 11.8 for in-store apps. Among Google Play Store apps, MobileFence – Parental Control requested the most dangerous permissions with 19, while the sideloaded app mSpy requested the most with 31.

We took a closer look at the permissions required by some of the apps. We identified several permissions that appear unnecessary for parental control or do not align with the app's features, including Bluetooth access, user credentials access, superuser permissions, flashlight access and dictionary modifications.

We further analysed three special permissions – Accessibility, Device Administrator and Draw Over Other Apps – that protect access to particularly powerful actions.

Table 2: Static Analysis of Sideloaded Apps

App Name	Tranco Score	Permissions	Dangerous Permissions	Tracker	Obfuscation	IOC Match
AnyControl	135,169	53	24	2	IN	
Bark Premium	10,840	44	14	4	N	
Chyldmonitor	728,971	38	21	1	IN	
Cocospy	461,897	38	21	1	IN	●
EvaSpy	775,227	44	17	0	IN	
FlexiSpy	264,503	47	24	1	IN	●
Hoverwatch	84,407	41	25	0	IN	●
iKeyMonitor	498,000	57	25	3	IN	●
Kidlogger	264,485	22	12	0	N	
Kidstracker	832,453	30	15	1	IN	
MoniMaster	446,047	34	19	2	IN	
mSpy	54,619	70	31	4	NO	●
Spapp Monitoring	80,573	45	24	0	IN	●
SPY24	501,038	53	26	1	IN	
SPYX	419,471	52	23	0	IN	
TheOneSpy	260,677	40	18	2	IN	
TiSpy	404,848	44	17	2	IN	●
uMobix	256,352	56	28	4	IN	
WebWatcher	424,303	38	16	2	IN	
XNSPY	365,926	41	18	5	NO	●

Abbreviations: N = No, IN = Icon and Name, NO = Name Only

Every single sideloaded app leveraged the Accessibility permission, intended to help users with disabilities, for example by creating screen readers or improving text readability. In parental control apps, this feature was used to view content displayed on the phone screen and control device interactions. Among the in-store apps, 14 used the Accessibility permission, while 6 did not.

The Device Administrator permission was used by 16 sideloaded apps and 15 in-store apps. This permission grants the ability to change passwords and lock the device but was mainly used to hinder the parental control app's uninstallation in the apps analysed by us. Device Administrator apps cannot be uninstalled like normal apps; the permission must be revoked before the app can be uninstalled.

The last special permission, Draw Over Other Apps, was used by 13 sideloaded apps and 14 in-store apps. This permission can be used to display content on top of other apps. We observed this permission being mainly used to further hinder the parental control app's uninstallation, for example, by automatically closing the settings app when an uninstallation attempt is made.

5.2 Functionalities

We documented the functionalities of each app during testing, including features not available in our current subscription model based on the information given on the websites or on the Google Play Store. The functionalities provided by the analysed parental control apps can be divided into the following categories:

(1) **Monitoring capabilities:** This encompasses basic monitoring functionalities provided by most parental control apps, including reading SMS messages, call history and browser history or location tracking.

(2) **Social media and messengers:** The majority of analysed apps offered the monitoring of popular social media apps and messengers. The most common were Facebook, Instagram, Snapchat and WhatsApp.

(3) **Remote control and access:** Remote control could be exerted via the monitoring dashboard of the parental control service or with SMS codes. Capabilities include making the device ring, activating the cameras or microphone and taking screenshots.

(4) **Specialised parental control:** This category contains functionalities that are typically only useful for parental control and have limited use for, for example, intimate partner surveillance, such as time limits and content filtering.

Expanding on the last category, we defined a list of functionalities that fall under specialised parental control: app time limits, setting schedules, content filtering, SOS/panic buttons, geofencing, keyword detection,[10] homework/task management, blocking apps and spyware detection. Given past research showing that stalkerware has presented itself as sideloaded parental control [25, 27, 83], we determine whether the analysed apps include specialised parental control functionalities and use this to indicate whether parental control was an objective for the app developers.

Five sideloaded apps did not include any specialised parental control functionalities: Cocospy, FlexiSpy, Hoverwatch, Kidstracker and Webwatcher. In comparison, none of the Google Play Store apps lacked specialised parental control features.

We also observed that Google Play Store apps offered fewer functionalities than sideloaded apps. Monitoring of other installed social media apps, which is heavily advertised by all sideloaded apps, is only mentioned by four in-store apps. Other features, such as keylogging, remote camera access and screen recordings were only offered by sideloaded apps.

Another concerning finding is that 12 of the sideloaded parental control apps promoted the monitoring of dating apps such as Tinder and Hinge, which could be used to monitor adults, as both apps have an age requirement of 18 years.
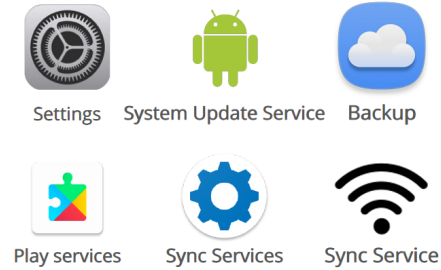
5.3 Obfuscation

A frequently quoted differentiator between parental control apps and stalkerware is whether the app hides its activity from the device owner [62]. Therefore, we examine which apps obfuscate their names and icons to appear inconspicuous or to masquerade as a different service.

None of the analysed in-store parental control apps used obfuscation – which is unsurprising considering it is prohibited by the Google Play Store policies [109]. Contrarily, 17 out of 20 sideloaded apps obfuscated their name; the only exceptions were Bark, Kidlogger and WebWatcher. Common obfuscated names include generic or system-related terms like "Settings", "System Service", "WiFi Service" and "Sync Services". These names are designed to blend in with legitimate system functions, giving the impression that they are a standard component of the device's software. Regarding the sideloaded app icons, 17 apps used an innocuous image, such as

the ones shown in Figure 1, i. e. all except for Bark, Kidlogger and mSpy[11]. Oftentimes icons resembling the settings icon, the Android logo or a WiFi symbol were used.

Figure 1: Obfuscation of sideloaded apps (upper left to lower right): AnyControl, MoniMaster, Spapp Monitoring, uMobix, FlexiSpy and Hoverwatch

5.4 Google Play Protect Services

Google Play Protect is a security feature on Android devices that scans and safeguards against potentially harmful apps and malware from the Google Play Store and other sources. Disabling Google Play Protect leaves the device vulnerable to malware and viruses, which is not ideal, especially for children's phones. However, 17 out of 20 sideloaded apps instruct the user to disable the feature, as otherwise the parental control app might be flagged as malicious and disabled by Google Play Protect. We tested how many of the sideloaded apps would be detected by Google Play Protect. In total, 13 apps were detected by Google Play Protect version 42.1.27-31, whereas seven were not considered to be harmful: Bark, EvaSpy, FlexiSpy, Spapp Monitoring, SPYX, TheOneSpy and TiSpy.

5.5 Privacy Policies

Our findings reveal significant differences between in-store and sideloaded apps regarding the availability, applicability and completeness of their privacy policies, raising concerns about transparency and user privacy. Table 3 offers an overview of key results.

5.5.1 Availability and Applicability. While all 20 sideloaded app vendors included a privacy policy on their website, just eight linked to or displayed a privacy policy within the app and a further eight apps did not seek consent for their privacy policies at all. Another issue we identified was that even if consent was sought, several sideloaded apps did not include the app in the scope of their privacy policy. Ten privacy policies applied only to the vendor's websites, leaving the app without a relevant privacy policy. Since the content of these policies was not applicable to our analysis, they were excluded. Only policies for AnyControl, Bark, Hoverwatch, Kidstracker, MoniMaster, Spapp Monitoring, SPY24, uMobix, WebWatcher and XNSPY remained.

Concerning in-store apps, 19 out of 20 provided an applicable privacy policy on the Google Play Store, and 16 of these included a

---

[10] Apps such as Bark monitor keywords and send a report if a term appears in conversational texts or other activity. This can be used to detect cyberbullying, access to inappropriate content etc.

[11] mSpy provided users with the option to obfuscate the app, but it was not enabled by default.

direct link to the policy within the app itself. Only KidControl failed to provide a privacy policy. Although the app remained available in the store, it was non-functional, with user reviews indicating that it had been broken since around a month prior.

5.5.2 Readability. The readability of the policies ranged from fairly difficult to very difficult, with an average score of 32.8 on the Flesch–Kincaid readability test for sideloaded apps, corresponding to the reading level of college students or college graduates. The policy of uMobix stands out as an outlier, being the only one to achieve a score above 50. The average length of the policies for sideloaded apps was around 17,330 characters. mSpy and SPYX were significantly longer, with around 44,700 and 43,800 characters. Comparatively short are the policies for AnyControl and Kidlogger, with both being less than 5,000 characters in length.

In-store app policies had comparable readability, with an average Flesch-Kincaid score of 31.1, but were longer, averaging 23,460 characters. The length of in-store policies also exhibited variation, ranging from 3,720 characters for MobileFence – Parental Control to 57,580 characters for Life360.

5.5.3 Contact Information. In-store apps were more likely to specify data protection officer (DPO) contact information, with 11 doing so compared to just one sideloaded app. Excluding those without privacy policies, one app from each group lacked any contact details, while the rest provided only general information. The GDPR requires companies that process sensitive data on a large scale or involve large-scale, regular and systematic monitoring of individuals to appoint a DPO [35]. This applies to the analysed parental control vendors, raising questions of compliance with the GDPR.

5.5.4 User Rights. User rights were mentioned by 15 in-store apps but only by 6 sideloaded apps. This disparity implies that sideloaded apps are more likely to lack full adherence to regulatory requirements. According to the GDPR, the types of data collected, the legal basis for processing, the sharing of information and user rights must be communicated [37].

5.5.5 Data Sharing with Third Parties. All ten sideloaded apps and 17 in-store apps stated in their policies that they share data with third parties, though it was often unclear whether personal data was included. Only one sideloaded app specified a third-party recipient, compared to 12 in-store apps that identified the services to which they provided data. Both groups cited similar reasons for data sharing, most commonly compliance with legal and regulatory requirements, service provision and marketing. However, in-store apps demonstrated significantly greater transparency on this topic, while the explanations given by sideloaded apps often lacked specific details, making it difficult to assess the extent of data-sharing practices.

5.6 Network Traffic

The network traffic captured during the testing was analysed to determine the usage of certificate pinning, encryption and URLs. Nine sideloaded apps employed some form of certificate pinning, compared to seventeen in-store parental control apps. The higher adoption of certificate pinning in in-store apps is expected, given

that sideloaded apps have been found to neglect security standards [8, 11]. Moreover, two sideloaded apps, EvaSpy and TiSpy, obfuscated their source code. Connections to trackers like Google Crashlytics and Firebase Analytics frequently failed due to server-side certificate pinning, which could not be bypassed. As a result, we are unable to provide information about the transmission of personally identifiable information to third parties.

We were unable to capture unencrypted traffic for some apps due to factors such as their use of VPNs, custom encryption methods and server-side security checks. However, we successfully obtained unencrypted network traffic for 16 sideloaded apps and 16 in-store apps. For an additional 3 in-store apps, we were only able to collect limited data due to application instability caused by resource mismatches.

Our analysis revealed that three sideloaded apps – FlexiSpy, Kidlogger and TheOneSpy – did not implement Transport Layer Security (TLS)[12] encryption. Kidlogger and TheOneSpy transmitted sensitive data in plaintext, whereas FlexiSpy used a custom encryption protocol. Despite employing AES encryption, FlexiSpy's implementation has been shown to be vulnerable to decryption [69], allowing potential attackers to intercept and access sensitive user data. In contrast, none of the analysed in-store applications exhibited these issues.

The network traffic also showed that mSpy transmits sensitive GPS location data on top of device data to Amplitude, a product analytics platform that assists businesses in tracking and analysing user behaviour. We also discovered links between different sideloaded parental control apps. EvaSpy retrieves information hosted on "172.232.207.34/TiSPY", while MoniMaster downloads a certificate from "clevguard.net". This suggests these apps may share infrastructure or resources, pointing to possible links in their development or distribution.

5.7 Stalkerware Indicators of Compromise (IOC)

Due to the overlap and misuse of parental control apps and stalkerware (see subsection 3.2), we decided to match the identified apps to common stalkerware IOC, as described in Q4. Our primary source was TinyCheck, a tool designed to detect spyware and stalkerware on mobile devices by analysing network traffic without requiring direct access to the device. TinyCheck's IOCs are sourced from Kaspersky's Global Research and Analysis Team, along with contributions from various researchers and experts, including specialised stalkerware repositories. Their information is free, open-source, regularly updated and used by women's shelters. We cross-referenced the domains and corresponding IP addresses identified for each app with these IOCs.

Among the 44 identified apps not available on the Google Play Store, 25% were classified as stalkerware by TinyCheck, with one additional app flagged as suspected stalkerware.

Of the 20 sideloaded apps analysed in this study, eight (or 40%) were classified as stalkerware: Cocospy, FlexiSpy, Hoverwatch, iKey-Monitor, mSpy, Spapp Monitoring, TiSpy and XNSPY. Three of them were not detected by Google Play Protect as potentially malicious apps (FlexiSpy, Spapp Monitoring and TiSpy), aligning with past research on the limitations of Google Play Protect [59].

---

[12] TLS, used in the HTTPS protocol, encrypts data to ensure secure communication.

We further discovered 4 apps currently available on the Google Play Store that are considered stalkerware by the IOC used for this study: Find My Kids: GPS-Tracker, KidsGuard Pro-Phone Monitoring, Life360 and mLite – GPS Location Tracker.

6 Discussion

Our analysis of 20 parental control apps from sideloaded sources and 20 from the Google Play Store highlights concerning patterns in the sideloaded parental control market, as evidenced by our discoveries related to the driving research questions.

Regarding Q1, we found that sideloaded parental control apps appear to offer even more extensive surveillance capabilities, while simultaneously offering fewer specialised parental control features. These apps request a significantly higher number of permissions, including potentially dangerous ones. Particularly alarming is the fact that over half of the analysed parental control apps included features to monitor popular dating apps, which raises serious privacy and safety concerns for children. While underage users may find ways to access these platforms, these services have an age requirement of at least 18 years old. The availability of monitoring tools that enable surveillance of these age-restricted apps can hint at the fact that this feature is designed for monitoring the activities of adults. While it can only be speculated, the software providers may endorse surveillance within intimate partner relationships while posing as parental control software. When it comes to trackers, we found that Google Play Store apps use significantly more trackers than sideloaded apps. Most of the encountered trackers aim to improve app performance, enhance user experience, or assess marketing effectiveness. While obfuscation was not present in Google Play Store apps, most sideloaded apps attempt to hide their activity by pretending to be inconspicuous system-related services.

Concerning Q2, we found that parents and children were, in most cases, not sufficiently informed about the sideloaded apps' privacy practices because the policies were often unclear, hard to access, or lacked crucial information. In connection with this, we identified multiple suspected violations of the GDPR regarding privacy policies, indicating potential legal and regulatory problems. The absence of privacy policies calls into question the credibility of the analysed app vendors' claims that their apps are intended to provide a safe and secure digital environment for children.

On the topic of Q3, we found that three sideloaded parental control apps failed to protect confidential user data during transmission by not implementing encryption. We uncovered potential relationships between different parental control vendors and discovered one app sharing sensitive location data with third-party trackers.

Regarding Q4, we found that 25% of all sideloaded Android parental control apps identified were flagged as stalkerware by TinyCheck. This number increases to 40% for the 20 most popular apps analysed in this study. It is important to note that TinyCheck does not offer a comprehensive list of IOCs and does not distinguish between dual-use apps and stalkerware. When we compared our app sample with the IOCs database from Echap [33], a hacker collective that combats sexual violence and provides resources to help organisations and individuals prevent cyber violence, a higher number of apps were flagged as stalkerware. According to their IOCs, 50% of the 44 identified sideloaded parental control apps and 80% of the 20 apps analysed in this study are listed as potential stalkerware. By comparing these results, we noted that TinyCheck appeared to apply stricter criteria for identifying stalkerware, while Echap flagged dual-use apps as well, without distinguishing them from stalkerware. However, since neither source provided a detailed explanation of their IOC selection process or criteria, these differences in classification remain somewhat unclear.

Below, we discuss the implications of our findings in more detail, assess their adherence to safety-by-design principles and consider the ramifications this has on the legitimacy of the sideloaded parental control software market and legislation.

6.1 Risks of Sideloaded Parental Control Apps

We identified several risk factors associated with the usage of the examined sideloaded parental control apps, which we outline below.

6.1.1 Lack of Meaningful Safeguards Against Misuse. We observed that sideloaded parental control apps lacked adequate safeguards, such as regular notifications informing the user of monitoring, which are a necessity to prevent the misuse of parental control apps for malicious purposes [65]. When safeguards are present in sideloaded apps, they depend on the correctness of user-entered data without independently verifying it, meaning the measure is ineffective in preventing misuse. In practice, there are user-friendly and privacy-conscious options to ensure apps are not used without someone's consent or awareness, such as periodic reminders that monitoring is active, a permanent icon in the notification bar and accessible activity dashboards. Such safeguards were implemented by 17 in-store parental control apps but were largely absent in sideloaded apps. This issue is exacerbated by the fact that the majority of sideloaded apps obfuscate their name and icon, making them better targets for malicious use.

6.1.2 Abuse of Special Permissions. The second finding concerns the use of the following privileges: display above other apps, device administrator and accessibility. Kidlogger best exemplifies the exploitation of special privileges. The window is immediately minimised when the user navigates to the settings and attempts to open Kidlogger's app information. This repeats when trying to maximise it again, meaning the user can not view essential details, such as granted permissions, or click the "uninstall" or "force stop" buttons. Combined with the device administrator privilege, which disables the uninstall button on the home screen when a user long-presses the app, the deletion of Kidlogger is challenging. In principle, the device administrator privilege can be revoked in newer Android versions, and the app can be uninstalled afterwards. However, many users, especially minors, are likely unaware of this [104]. This mechanism has been well-documented in relation to stalkerware [124], yet it was equally used by both sideloaded and in-store apps. Google has made efforts to restrict sideloaded apps from using the accessibility API starting with Android 13, but users can still manually grant this permission to parental control apps if desired [113].

6.1.3 Excessive Monitoring. We observed that sideloaded apps, which often offer extensive monitoring features not present in in-store apps, request significantly more permissions than those available on the Google Play Store, including potentially dangerous

ones. We found evidence that some of these permissions appear unnecessary for the app's parental control functionalities. The acquisition of excessive permissions enables broad data collection, which is particularly concerning for apps managing children's data. This overprivilege in permissions is a common issue across apps in general [123]. Developers use API methods to implement different app capabilities, which require permissions to work. Due to poor documentation, it is not always clear which permissions are essential, and since missing permissions might lead to app crashes, developers tend to add permissions [110] carelessly. Unwarranted permissions can, however, cause problems and make apps insecure and unreliable [118].

Excessive monitoring was also noted during the app analysis. Sideloaded apps offered concerning capabilities, such as keyloggers or remote camera access, surpassing what is typically provided by in-store parental control apps. Hoverwatch, for example, took pictures with the front camera every time the device was unlocked. Other apps let the person monitoring remotely trigger a screen recording, the camera and the microphone. It is up to debate whether parental control apps need such features. It should also be highlighted that these functionalities are common in stalkerware [95]. Additionally, more than half of the parental control apps promoted the monitoring of dating apps such as Tinder and Hinge on their websites. As these dating platforms have minimum age requirements of 18 years, the availability of monitoring tools that enable surveillance of such age-restricted apps suggests that these services could be used to track adults' activities rather than children's (i. e. in the context of intimate partner violence) while also risking outing minors who are, for example, "closeted" LGBTQ+ users [17].

6.1.4   Lack of Encryption. Three apps were found without TLS encryption, exposing network traffic to interception and unauthorised access. This negligence, especially involving children's data, poses a serious risk of sensitive information being compromised by malicious actors.

6.1.5   Circumvention of Google Play Protect Security Safeguards. Lastly, our analysis also examined how sideloaded parental control apps circumvent the Google Play Protect security feature. 13 parental control apps were identified as potentially malicious by Google Play Protect. As a result, most apps instruct the user to disable the feature during installation. Furthermore, some apps go a step further, asking users to not only disable the service but also turn off any notifications from it. As a result, users remain unaware that the protective service has been deactivated, exposing their devices to potential risks from other malicious software. This is unacceptable from a parental control perspective, as it subjects children's devices to unnecessary risks. Legitimate sideloaded parental control apps should aim to operate without triggering device protection mechanisms.

Google is currently launching an initiative to enhance Google Play Protect in selected countries to address malicious apps. According to a statement on their blog, this innovation will significantly improve the detection and blocking of harmful software, having already identified 515,000 new malicious apps [53]. Whether these improvements will affect the sideloaded parental control market is subject to future research. Google has announced an upgrade to

Google Play Protect, incorporating a new fraud protection feature designed to block sideloaded apps that request sensitive runtime permissions [53].

6.2   Privacy Policy Shortcomings
The privacy policy analysis unveiled several gaps in data protection compliance related to the deployment of sideloaded parental control apps.

6.2.1   Missing of App-Specific Privacy Policies. Our findings show a lack of comprehensive privacy policies, leaving parents uninformed about data practices, compromising their ability to make informed decisions and raising questions about the vendors' ethical standards and commitment to data privacy, transparency and accountability. Half of the analysed services did not include the app in the scope of their privacy policy or offer a separate policy for their app, meaning there was no legal information about the privacy practices of parental control apps in half of the cases.

6.2.2   Absence of Essential Information. The remaining ten policies lacked essential details, such as user rights, the types of data collected and which third parties it might be shared with. Therefore, parents using these services cannot inform themselves about the extent of data collection, encompassing their own personal information and, more significantly, that of their child. Besides, both parents and children are in the dark about whether the app is safe to use, as privacy implications and security measures implemented by the services are mostly unclear. These findings echo research by Sun et al. [106], who found a similar lack of child safety and privacy information in privacy policies of smart home products explicitly advertised for children. Information about what data a specific product might collect about children and for what purposes was rarely mentioned upfront. Moremen et al. [84] showed that while people across all generations struggle to understand technical terms, misunderstandings and lack of knowledge are particularly acute problems for children. Indeed, without explicit privacy guidelines, children using these apps may become unwitting subjects of data collection and monitoring [76]. Minors are left particularly vulnerable if their sensitive information is exposed, such as GPS locations, private messages, browser history, photos and videos. Data breaches involving sideloaded parental control apps are not rare, as shown by several breaches in recent years affecting millions of users [7, 28, 87].

6.2.3   Failure to Obtain Meaningful Consent. Our findings also raise critical questions about consent. The GDPR mandates that parental consent be obtained for children under the age of 16 [39]. However, Parsons et al. [95] argue that obtaining consent from just one parent is inadequate in joint parenting situations. Each parent with custodial rights must provide informed and verifiable consent to the surveillance of the child. None of the analysed apps implemented measures to ensure this. Parsons et al. underscore the importance of mutual consent by addressing situations of intimate partner violence where single-parent consent can lead to harm to the non-consenting partner, who is indirectly subject to the monitoring abilities of the parental control app. Some software vendors stated that only the device owner's consent is required for monitoring. However, device ownership extends beyond legal guardianship.

This prompts consideration of whether consent given by other relatives (e. g. step-parents or foster care workers) is sufficient to facilitate child monitoring and how mutual consent provisions could be technically implemented in shared device scenarios.

6.2.4 Imbalance in User Rights and Data Autonomy. Sideloaded parental control apps present a significant control imbalance regarding user rights. Children lack autonomy over their data, even when the monitoring concludes or they reach adulthood. In addition to the frequent omission of user rights in policies, it is crucial to emphasise that, across all cases, only the account creator (typically the assumed parent) possesses the capability to exercise these rights. As a result, the monitored individual is devoid of authority over their own data unless they attain account ownership or initiate direct contact with the software vendor. Even when the use of the parental control app ceases, such as when the child reaches the age of 18, the individual still cannot access or request the deletion of their data. None of the policies addressed this issue or explicitly provided ways for the person whose data is being collected to exercise any authority over their data. As court cases have begun of children suing their parents for breaches of privacy due to parental "oversharenting" (i. e. parents sharing too much or inappropriate information) [12, 92], it is plausible that such developments are on the horizon.

6.2.5 Readability. Our results also showed that the readability of all policies ranged from fairly difficult to very difficult. Poor readability is a problem among privacy policies in general. A previous study found that the average Flesch–Kincaid readability score for privacy policies of the top one million websites was 39.8 [72], which is not significantly better than the average of the analysed parental control policies. Some of the contributing factors to these suboptimal implementations may include communication gaps and adversarial relationships between software developers and privacy experts [126].

Lastly, it is important to note that even when privacy policies are accessible, research has found that a significant portion of users (74%) simply do not read them [89]. Furthermore, even when users do read and understand the policy, they often struggle to translate that information into a clear understanding of the privacy risks they face [114]. This is caused by factors such as the length of policies, the difficulty of comprehending them, vague language and the limitations of real choice [16]. Some scholars thus argue that digital consent is intrinsically flawed [24], which further means that parents may not fully grasp what they are agreeing to. These challenges are exacerbated by the incomprehensible and inchoate policies analysed in this work, which often did not adequately address their respective apps.

Regardless of these issues, studying the privacy policies of sideloaded apps remains relevant. Even though users might not read or fully make sense of them, privacy policies serve as a legal framework that outlines the company's commitments and practices. They provide a baseline for accountability and are usually the only formal source of information about how user data is handled. Moreover, a comprehensive policy allows users to inform themselves, whereas the absence or incompleteness of a policy takes this option away entirely, increasing the risk of uninformed consent.

6.3 Safety-by-Design Non-Compliance

The studied sideloaded parental control apps severely lack adherence to safety-by-design principles, which give platforms and services guidance to incorporate, evaluate and enhance user safety. We used the eSafety Commissioner's recommendations [34] to assess whether the vendors should be trusted with children's data. However, there is an abundance of other efforts underway to centre children's technology design needs, including the UK's Age Appropriate Design Code [115] and California's Age Appropriate Design Code Act [22].

6.3.1 Service Provider Responsibility. The first safety-by-design principle places responsibility on service providers to understand potential online harms and to address them in the design of their systems. Arguably, all analysed app vendors failed this measure, as none implemented effective safeguards, like ongoing or regular status bar notifications showing monitoring is active. We encountered disclaimers on both the vendor's websites as well as in the apps, shifting the responsibility to the app users.

6.3.2 User Empowerment and Autonomy. The second principle focuses on user empowerment and autonomy, stating that the service should align with the best interests of users, particularly the children being monitored. While parental control offers benefits to minors, such as protecting them from inappropriate content or enabling parents to intervene in critical situations such as cyberbullying, common in-store apps can also provide these positive outcomes. Conversely, the obfuscation inherent in many sideloaded parental control apps, which often monitor children without their knowledge or consent, undermines their sense of agency and significantly diminishes their autonomy. The notion that excessive monitoring may not serve the best interests of children is also suggested by app reviews: More than half of the Google Play Store reviews for parental control apps are negative [1], with ratings from children being notably lower than those from parents [49]. Recent research even found evidence that overcontrol is linked to brain connectivity patterns tied to threat sensitivity, supporting its classification as childhood trauma [23]. Inadequate security measures also negate this principle's tenets, as well as the lack of comprehensive and complete privacy policies. The second principle recommends the implementation of built-in support functions and feedback loops. Although some parental control apps offered support services for the parent through their website, no such services were available for children or implemented into the apps themselves.

6.3.3 Transparency and Accountability. The third and final principle addresses transparency and accountability. Companies should ensure that user safety policies, terms and conditions, community guidelines and processes about user safety are accessible, easy to find, regularly updated and easily understood. Yet, half of the sideloaded parental control apps did not provide privacy policies applicable to the apps, and most policies were not even displayed within the apps.

In conclusion, most of the analysed sideloaded parental control apps fail to adhere to any of the proposed safety-by-design principles. While past research has shown that these principles may be challenging to implement [54], they provide a solid foundation for vendors which they must be expected to comply with.

6.4 Ethical Implications

Our research raises several important questions regarding the use of sideloaded parental control apps that warrant careful consideration. The implications of our work, therefore, extend beyond the technical domain, encompassing broader societal concerns.

6.4.1 Legitimisation of the Sideloaded Parental Control Software Market. Considering that more than half of the identified sideloaded parental control apps were matched to stalkerware IOC, it is imperative to understand the danger stalkerware poses. Stalkerware often targets individuals such as partners, ex-partners and family members, granting access to personal and sensitive information. Such an invasion of privacy can have severe emotional, psychological and physical consequences for the affected parties [25, 47, 95]. Kaspersky's 2023 report identified 31,031 stalkerware victims, an increase from 2022, though the actual number is likely higher as only Kaspersky users were analysed. They emphasise that stalkerware remains a global issue [63].

Liu et al. [73] suggested that fines, such as the one imposed against the spyware product StealthGenie in 2014 [90], compelled stalkerware developers trying to avoid similar penalties to market their product for ostensibly lawful purposes, mainly child and employee monitoring. Consequently, the market of sideloaded parental control apps appears to be subverted by stalkerware, making it harder to find credible software.

Despite arguments challenging the legitimacy of the sideloaded parental control market, some vendors have provided reasons why this market is still important. Bark used to offer its software on the Google Play Store but has since decided to move to sideloading, citing stricter regulations by the Google Play Store when it comes to monitoring children's communication. They addressed this topic on their website, as seen in Figure 2. Other vendors point
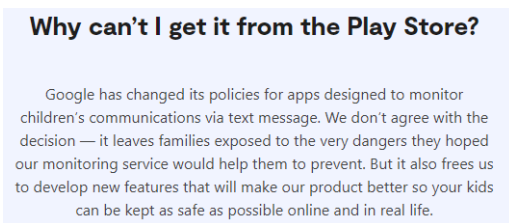
Figure 2: Bark's reasoning behind shifting their app to the sideloaded app market

out that sideloaded apps can address situations where children have learned to circumvent or uninstall in-store apps. Sideloaded apps often remain hidden and are more difficult to uninstall, providing parents with a tool to maintain monitoring when they believe it is still necessary. Another possible reason for sideloading is to avoid paying service fees and commissions on sales [18, 85]. While this is typically not lucrative, as sideloaded apps are less visible and get fewer customers, the strategy could be more effective if only the children's app is sideloaded while the parent's app remains on the official store. This way, vendors can maintain visibility while sidestepping fees by charging solely for the children's app.

Aside from the specifics of sideloaded apps, researchers have also argued that parental control apps are not optimal for good parenting. Such top-down monitoring approaches should be replaced with family online safety apps, which focus more on aspects such as children's autonomy, learning and appropriate use of technology [49] or constructive parent-child interactions such as conversations to shape minors' privacy and security literacy [2, 15, 88, 111].

6.4.2 Legal and Regulatory Responses. Policy and legislation response are necessary to protect children's data from being endangered by stalkerware posing as parental control apps. Researchers like Sonia Livingstone, who specialises in children's digital rights, have highlighted the challenges policymakers face in realising children's rights online [74]. She suggests measures such as prioritising digital literacy education for both children and parents and building expertise on digital matters within the child workforce.[13]

Recent developments such as the UK's Online Safety Act (2023) and the proposed USA's Kids Online Safety Act (KOSA) push for such reforms. Still, they primarily focus on obligations for social media platforms and their provisions related to parental control apps and children's data privacy remain heavily contested [13, 86]. While existing frameworks, such as the GDPR, set benchmarks to safeguard individuals' data, including children's data, our research uncovered numerous potential GDPR violations with no apparent legal consequences to date. Data protection authorities should, therefore, take a more active role in overseeing the sideloaded app market, particularly those apps claiming to be parental control tools and enforcing compliance with data privacy laws.

6.4.3 Advice for App Developers and Parents. Our research also shows the need for explicit recommendations for app developers and parents. The sideloaded software market must adhere to established safety-by-design principles, ensuring their apps have robust privacy protections, clear consent processes and transparent privacy policies from the outset [51]. Developers should also incorporate mechanisms that allow children to exercise their rights over their data once they reach adulthood. Parents should be provided with accessible resources and tools to help them make informed decisions about which parental control apps to install, particularly in light of the DMA, which will open up the availability of third-party apps independent of app stores. Educating parents about the risks of sideloaded apps and promoting the use of safe and child-friendly apps that have undergone rigorous security and privacy checks can help mitigate the risks associated with poorly vetted third-party apps.

6.4.4 Misuse of Findings. We acknowledge the risk of individuals misusing our work in their search for apps with specific properties or capabilities. However, the intent behind this paper was not to advocate or facilitate malicious use. Instead, we aimed to raise awareness in this field and incentivise changes in the practices of the sideloaded parental control market.

6.4.5 Coordinated Disclosure. In light of the concerns around the potential misuse of these apps and the detected potential security

---

[13] Occupations that involve working with or caring for children, such as teaching or childcare.

and GDPR breaches, we adhered to the OWASP guide for coordinated disclosure [93]. We shared our findings with all 20 sideloaded app vendors in advance, following CERT/CC's disclosure policy, to give them the opportunity to respond and implement any necessary measures before our results are made public. Due to the absence of critical findings for in-store apps, there was no need for notification in their case. As of publication, only two vendors have responded to our disclosure and we are unaware of any changes being implemented. Lastly, the Android Security Team was notified about the seven sideloaded apps with stalkerware traits that were not flagged by Google Play Protect.

7 Limitations

Several limitations affect our study. First, the Google Play Store's lack of download number filtering may have led to the exclusion of some popular parental control apps from our selection. Second, issues outlined in subsection 5.6 prevented us from analysing all sideloaded apps, limiting our sample. Third, static analysis using MobSF and Exodus does not account for dynamic execution, such as runtime permissions or unexecuted code paths involving third-party endpoints. Since these tools rely on pre-compiled tracker databases, any trackers absent from these databases may go undetected, leading to potential false negatives. Additionally, the tools may struggle with obfuscation, possibly preventing a complete assessment when heavily obfuscated code is present. Finally, the Flesch-Kincaid readability test, while useful, has limitations, as it only measures quantifiable aspects of readability and assumes uniform reader characteristics, such as cognitive ability and maturity [101]. Despite these limitations, our findings remain robust, replicable and reproducible, with the potential for addressing these gaps in future research.

8 Conclusion

This study found several privacy, safety and security concerns regarding sideloaded parental control apps. We examined the apps of 20 sideloaded and 20 Google Play Store apps as well as their privacy policies. We recognised that many issues identified in previous research on in-store parental control apps also apply to the sideloaded versions examined in this study [41, 91]. Some problems are exacerbated in sideloaded apps, including excessive monitoring, inappropriate functionalities and overlap with stalkerware, further compounded by a lack of safeguards. Unlike in-store parental control apps, the sideloaded versions provided far more extensive monitoring capabilities, thus requiring more permissions. However, fewer of these sideloaded apps offered specialised parental control functionalities. Obfuscation was also more prevalent among the sideloaded apps, while trackers were more common among in-store apps, suggesting a greater focus on user analytics.

The privacy policies for sideloaded apps raised many issues, especially completeness, transparency and availability. Most sideloaded vendors failed to provide children or monitored individuals any means to exercise authority over their personal data and user rights, such as deletion of information. This disregard for children's digital autonomy and privacy is deeply troubling. A significant number of sideloaded parental control apps have triggered alerts from stalkerware detection tools, suggesting that certain features of these apps

bear a concerning resemblance to those typically associated with surveillance software.

Moreover, most analysed apps fail to meet basic safety-by-design principles despite handling sensitive and personally identifiable children's data. As such, the studied apps cannot be considered "ethical" parental control, as the level of surveillance significantly surpasses that of conventional, in-store options. The erosion of children's independence, agency and trust facilitated by sideloaded apps is a grave concern. Sideloaded parental control apps that operate in the shadows without transparency or user consent undermine the foundations of a healthy parent-child relationship built on mutual understanding and respect.

Based on our findings, we call for greater oversight and regulation of the sideloaded software market to mitigate these products' dangers for children and other vulnerable groups, such as stalking and intimate partner violence victims. Data protection authorities must step in to ensure sideloaded apps adhere to the highest privacy and security standards. Only then can we create a digital landscape that empowers children, preserves their rights and fosters the trust essential for their well-being, protection and development.

We also want to address upcoming changes in the evolving landscape of sideloaded software, particularly with the DMA requiring Apple to open its smartphone ecosystem to sideloaded software. Given these impending shifts, future analyses of sideloaded parental control software and the broader sideloaded software market will be crucial.

Other valuable research opportunities include interviewing app developers and company executives to gather insights into their views on privacy practices and abuse vectors. Additionally, questioning parents who use sideloaded parental control apps on their motives and awareness of dangers could provide further relevant context. Finally, future research could focus on developing and proposing concrete recommendations for policymakers, app developers and parents based on the identified security and privacy issues in parental control apps.

References

[1] Omer Akgul, Sai Teja Peddinti, Nina Taft, Michelle L. Mazurek, Hamza Harkous, Animesh Srivastava, and Benoit Seguin. 2024. A Decade of Privacy-Relevant Android App Reviews: Large Scale Trends. In *Proceedings of the 33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Berkeley, CA, 5089–5106. https://www.usenix.org/conference/usenixsecurity24/presentation/akgul

[2] Kenan Kamel A Alghythee, Adel Hrncic, Karthik Singh, Sumanth Kunisetty, Yaxing Yao, and Nikita Soni. 2024. Towards Understanding Family Privacy and Security Literacy Conversations at Home: Design Implications for Privacy Literacy Interfaces. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*. ACM, New York, NY, Article 983, 12 pages. https://doi.org/10.1145/3613904.3641962

[3] Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, and Amr Youssef. 2020. Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions. In *Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC '20)*. ACM, New York, NY, 69–83. https://doi.org/10.1145/3427228.3427287

[4] Majed Almansoori, Andrea Gallardo, Julio Poveda, Adil Ahmed, and Rahul Chatterjee. 2022. A Global Survey of Android Dual-Use Applications Used in Intimate Partner Surveillance. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022), 120–139. https://doi.org/10.56553/popets-2022-0102

[5] Noura Alomar and Serge Egelman. 2022. Developers Say the Darnedest Things: Privacy Compliance Processes Followed by Developers of Child-Directed Apps. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022), 250––273. https://doi.org/10.56553/popets-2022-0108

[6] Android for Developers. 2023. <permission>. Retrieved 2023-08-28 from https://developer.android.com/guide/topics/manifest/permission-element

[7] Lore Apostol. 2024-07-12. Millions of mSpy Spyware App Customers Exposed via Third-Party Zendesk Chat Support. Retrieved 2023-05-01 from https://www.technadu.com/millions-of-mspy-spyware-customers-exposed-via-zendesk/539017/

[8] Apple. 2021. *Building a Trusted Ecosystem for Millions of Apps: A Threat Analysis of Sideloading*. Technical Report. Apple. https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf

[9] Apple. 2024. Apple Announces Changes to iOS, Safari, and the App Store in the European Union. Retrieved 2024-02-10 from https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

[10] Tomás Bermudez, Maddalena Esposito, and Jay Neuner. 2020. *Mapping the State of Knowledge on the Use of Stalkerware*. Master's thesis. University College London, London.

[11] Juan Francisco Bertona. 2024-06-19. Beyond the App Store: The Hidden Risks of Sideloading Apps. Retrieved 2024-08-18 from https://www.zimperium.com/blog/the-hidden-risks-of-sideloading-apps/

[12] Claire Bessant. 2017. Could a Child Sue Their Parents for Sharenting? Retrieved 2024-08-31 from https://blogs.lse.ac.uk/parenting4digitalfuture/2017/10/11/could-a-child-sue-their-parents-for-sharenting/

[13] Aliya Bhatia. 2024-05-23. *CDT, ACLU, EFF, Fight for the Future, and OTI Call on House Subcommittee to Improve Kids Online Safety Act to Ensure Kids' Access to Critical Information*. Technical Report. Center for Democracy and Technology. Retrieved 2024-08-27 from https://cdt.org/insights/cdt-aclu-eff-fight-for-the-future-and-oti-call-on-house-subcommittee-to-improve-kids-online-safety-act-to-ensure-kids-access-to-critical-information/

[14] Eric B. Blancaflor, Gerardine Anne J. Anson, Angela Mae V. Encinas, Kiel Cedrick T. Huplo, Mark Anthony V. Marin, and Stephany Lhaime G. Zamora. 2021. A Vulnerability Assessment on the Parental Control Mobile Applications' Security: Status Based on the OWASP Security Requirements. In *Proceedings of the 11th Annual International Conference on Industrial Engineering and Operations Management*. IEOM Society, Singapore, 6463––6472.

[15] Elana B. Blinder, Marshini Chetty, Jessica Vitak, Zoe Torok, Salina Fessehazion, Jason Yip, Jerry Alan Fails, Elizabeth Bonsignore, and Tamara Clegg. 2024. Evaluating the Use of Hypothetical 'Would You Rather' Scenarios to Discuss Privacy and Security Concepts with Children. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1, Article 165 (2024), 32 pages. https://doi.org/10.1145/3641004

[16] Frederik Z. Borgesius. 2015. Informed Consent: We Can Do Better to Defend Privacy. *IEEE Security & Privacy* 13, 2 (2015), 103–107. https://doi.org/10.1109/MSP.2015.34

[17] Elijah Bouma-Sims, Sanjnah Ananda Kumar, and Lorrie Faith Cranor. 2024. Exploring the Privacy Experiences of Closeted Users of Online Dating Services in the US. *Proceedings on Privacy Enhancing Technologies* 2024, 2 (2024), 160–181. https://doi.org/10.56553/popets-2024-0046

[18] Robert Brady. 2018. App Sideloading and Cyber Risk. *British Computer Society* (2018). Retrieved 2024-08-29 from https://www.bcs.org/articles-opinion-and-research/app-sideloading-and-cyber-risk/

[19] Andi Brown, Diarmaid Harkin, and Leonie M. Tanczer. 2024. Safeguarding the "Internet of Things" for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence Against Women* (2024), 24 pages. https://doi.org/10.1177/10778012231222486

[20] Zuzana Sekeráková Búriková and Veronika Valkovičová. 2024. Introduction to the Thematic Issue. Beyond the Ideal: Surveillance, Control, and the Complexities of Care. *Sociológia - Slovak Sociological Review* 56, 4 (2024), 285–301. https://doi.org/10.31577/sociologia.2024.56.4.10

[21] Character Calculator. 2024. Flesch Reading Ease Calculator. Retrieved 2024-07-27 from https://charactercalculator.com/flesch-reading-ease

[22] California State Legislature. 2022. Ca. Civ. Code § 1798.99.28 The California Age-Appropriate Design Code Act (CAADCA). Retrieved 2024-08-31 from https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

[23] Giuseppe A. Carbone, Claudio Imperatori, Mauro Adenzato, Aurelia Lo Presti, Benedetto Farina, and Rita B. Ardito. 2024. Is Parental Overcontrol a Specific Form of Child Maltreatment? Insights from a Resting State EEG Connectivity Study. *Child Abuse & Neglect* 155 (2024). https://doi.org/10.1016/j.chiabu.2024.106962

[24] Elinor Carmi. 2021. A Feminist Critique to Digital Consent. *Seminar.net* 17, 2 (2021), 21 pages. https://doi.org/10.7577/seminar.4291

[25] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *Proceedings of the 2018 IEEE Symposium on Security and Privacy (S&P 2018)*. IEEE, New York, NY, 441–458. https://doi.org/10.1109/SP.2018.00061

[26] Tiny Check. 2024. Tiny Check. Retrieved 2024-06-11 from https://tiny-check.com

[27] Danielle Keats Citron. 2023. Spying Inc. *Washington and Lee Law Review* 72, 3 (2023), 1243–1282. https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/7

[28] Graham Cluley. 2024-05-31. *Stalkerware App PCTattletale Announces It Is Out of Business After Suffering Data Breach and Website Defacement*. Bitdefender. Retrieved 2024-08-29 from https://www.bitdefender.com/blog/hotforsecurity/stalkerware-app-pctattletale-announces-it-is-out-of-business-after-suffering-data-breach-and-website-defacement/

[29] Joseph Cox. 2018-02-22. *Hacker Strikes 'Stalkerware' Companies, Stealing Alleged Texts and GPS Locations of Customers*. VICE. Retrieved 2023-08-09 from https://www.vice.com/en/article/7x77ex/hacker-strikes-stalkerware-companies-stealing-alleged-texts-and-gps-locations-of-customers

[30] danah boyd and Eszter Hargittai. 2013. Connected and Concerned: Variation in Parents' Online Safety Concerns. *Policy & Internet* 5 (2013), 245–269. Issue 3. https://doi.org/10.1002/1944-2866.POI332

[31] Android Developers. 2024. Android Debug Bridge (ADB). https://developer.android.com/tools/adb 2024-08-13.

[32] Catherine Dungey. 2024. A Bird's Eye View: Care, Control, and the Use of Surveillance Apps Among Family Members in Germany. *Sociológia - Slovak Sociological Review* 56, 4 (2024), 325–345. https://doi.org/10.31577/sociologia.2024.56.4.12

[33] Echap. 2024. Echap. https://echap.eu.org Accessed: 2024-08-18.

[34] eSafety Commissioner. 2019. Principles and Background | eSafety Commissioner. https://www.esafety.gov.au/industry/safety-by-design/principles-and-background

[35] European Commission. 2017. Guidelines on Data Protection Officers ('DPOs'). Retrieved 2023-09-14 from https://ec.europa.eu/newsroom/article29/items/612048

[36] European Commission. 2024. Digital Markets Act. Retrieved 2024-08-29 from https://digital-markets-act.ec.europa.eu/

[37] European Parliament and Council of the European Union. 2018. General Data Protection Regulation: Art. 13 GDPR – Information to Be Provided Where Personal Data Are Collected from the Data Subject. Retrieved 2023-08-12 from https://gdpr-info.eu/art-13-gdpr/

[38] European Parliament and Council of the European Union. 2018. General Data Protection Regulation: Art. 3 GDPR – Territorial Scope. Retrieved 2023-08-12 from https://gdpr-info.eu/art-3-gdpr/

[39] European Parliament and Council of the European Union. 2018. General Data Protection Regulation: Art. 8 GDPR – Conditions Applicable to Child's Consent in Relation to Information Society Services. Retrieved 2023-08-12 from https://gdpr-info.eu/art-8-gdpr/

[40] Sead Fadilpašić. 2024-05-02. *Two Notorious Stalkerware Apps Appear to Finally Have Been Taken Offline Following Court Ruling*. TechRadar. Retrieved 2024-08-18 from https://www.techradar.com/pro/security/two-notorious-stalkerware-apps-appear-to-finally-have-been-taken-offline-following-court-ruling

[41] Álvaro Feal, Paolo Calciati, Narseo Vallina-Rodriguez, Carmela Troncoso, and Alessandra Gorla. 2020. Angel or Devil? A Privacy Study of Mobile Parental Control Apps. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (2020), 314–335. https://doi.org/10.2478/popets-2020-0029

[42] Rudolph Flesch. 1948. A New Readability Yardstick. *Journal of Applied Psychology* 32, 3 (1948), 221–233. https://doi.org/10.1037/h0057532

[43] Fortinet. 2023. What Is Spyware? Definition, Types And Protection. Retrieved 2023-09-10 from https://www.fortinet.com/resources/cyberglossary/spyware

[44] 5Rights Foundation. 2022. *Approaches to Children's Data Protection: A Comparative International Mapping.* Technical Report. 5Rights Foundation. https://5rightsfoundation.com/in-action/approaches-to-childrens-data-protection-a-comparative-international-mapping.html

[45] 5Rights Foundation. 2023. Child Online Protection. Retrieved 2024-01-31 from https://5rightsfoundation.com/our-work/child-online-protection/

[46] Lorenzo Franceschi-Bicchierai and Joseph Cox. 2017. Inside the 'Stalkerware' Surveillance Market, Where Ordinary People Tap Each Other's Phones. Retrieved 2023-05-01 from https://www.vice.com/en/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x

[47] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18).* ACM, New York, NY, Article 667, 13 pages. https://doi.org/10.1145/3173574.3174241

[48] Frida. 2024. Frida. https://frida.re Version 16.4.7.

[49] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M. Carroll, and Pamela J. Wisniewski. 2018. A Matter of Control or Safety? Examining Parental Use of Technical Monitoring Apps on Teens' Mobile Devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18).* ACM, New York, NY, Article 194, 14 pages. https://doi.org/10.1145/3173574.3173768

[50] Cassidy Gibson, Vanessa Frost, Katie Platt, Washington Garcia, Luis Vargas, Sara Rampazzi, Vincent Bindschaedler, Patrick Traynor, and Kevin Butler. 2022. Analyzing the Monetization Ecosystem of Stalkerware. *Proceedings on Privacy Enhancing Technologies* 2022, 4 (2022), 105–119. https://doi.org/10.56553/popets-2022-0101

[51] Vahiny Gnanasekaran and Katrien De Moor. 2023. Usability, Security, and Privacy Recommendations for Mobile Parental Control. In *Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference (EICC '23).* ACM, New York, NY, 138–143. https://doi.org/10.1145/3590777.3590800

[52] Google Play Protect. 2023. Malware Categories | Play Protect. Retrieved 2023-02-26 from https://developers.google.com/android/play-protect/phacategories

[53] Google Security Blog. 2024-02-06. Piloting New Ways of Protecting Android Users from Financial Fraud. Retrieved 2024-02-12 from https://security.googleblog.com/2024/02/piloting-new-ways-to-protect-Android-users-from%20financial-fraud.html

[54] Thomas D. Grace, Christie Abel, and Katie Salen. 2023. Child-Centered Design in the Digital World: Investigating the Implications of the Age-Appropriate Design Code for Interactive Digital Media. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference (IDC '23).* ACM, New York, NY, 289–‐297. https://doi.org/10.1145/3585088.3589370

[55] Daniel Greene and Katie Shilton. 2018. Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development. *New Media & Society* 20, 4 (2018), 1640–1657. https://doi.org/10.1177/1461444481770239

[56] Moritz Gruber, Christian Höfig, Maximilian Golla, Tobias Urban, and Matteo Große-Kampmann. 2022. "We May Share the Number of Diaper Changes": A Privacy and Security Analysis of Mobile Child Care Applications. *Proceedings on Privacy Enhancing Technologies* 2022, 3 (2022), 394–414. https://doi.org/10.56553/popets-2022-0078

[57] Pedro Hartung. 2020. The Children's Rights-by-Design Standard for Data Use by Tech Companies. Retrieved 2023-07-04 from https://www.unicef.org/globalinsight/media/1286/file/%20UNICEF-Global-Insight-DataGov-data-use-brief-2020.pdf

[58] Alexander Heinrich, Leon Würsching, and Matthias Hollick. 2024. Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection. *Proceedings on Privacy Enhancing Technologies* 2024, 3 (2024), 353–371. https://doi.org/10.56553/popets-2024-0082

[59] Shinelle Hutchinson, Bing Zhou, and Umit Karabiyik. 2019. Are We Really Protected? An Investigation into the Play Protect Service. In *2019 IEEE International Conference on Big Data (BigData 2019).* Los Angeles, CA, 4997–‐5004. https://doi.org/10.1109/BigData47090.2019.9006100

[60] Catherine Page Jeffery. 2021. "It's Really Difficult. We've Only Got Each Other to Talk To." Monitoring, Mediation, and Good Parenting in Australia in the Digital Age. *Journal of Children and Media* 15, 2 (2021), 202–217. https://doi.org/10.1080/17482798.2020.1744458

[61] Kaspersky. 2021. *Raising the smartphone generation: New research into how parents and children manage their digital habits.* Technical Report. Kaspersky Lab. https://www.kaspersky.com/blog/digital-habits-report-2021/

[62] Kaspersky. 2023. What Is Stalkerware/Spouseware? Retrieved 2023-04-30 from https://encyclopedia.kaspersky.com/glossary/stalkerware-spouseware/

[63] Kaspersky. 2024. *The State of Stalkerware in 2023–2024.* Technical Report. Kaspersky Lab. Retrieved 2024-05-10 from https://securelist.com/state-of-stalkerware-2023/112135/

[64] Mareile Kaufmann. 2021. This Is a Secret: Learning from Children's Engagement with Surveillance and Secrecy. *Cultural Studies ↔ Critical Methodologies* 21, 5 (2021), 424–437. https://doi.org/10.1177/15327086211029350

[65] Cynthia Khoo, Kate Robertson, and Ron Deibert. 2019. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.* Technical Report Citizen Lab Research Report No. 121. University of Toronto. https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/

[66] Ada S. Kim and Katie Davis. 2017. Tweens' Perspectives on Their Parents' Media-Related Attitudes and Rules: An Exploratory Study in the US. *Journal of Children and Media* 11, 3 (2017), 358–366. https://doi.org/10.1080/17482798.2017.1308399

[67] Platon Kotzias, Juan Caballero, and Leyla Bilge. 2021. How Did That Get In My Phone? Unwanted App Distribution on Android Devices. In *Proceedings of the 2021 IEEE Symposium on Security and Privacy (S&P 2021).* IEEE, New York, NY, 53–69. https://doi.org/10.1109/SP40001.2021.00041

[68] Robert D. Laird and Skyler T. Hawk. 2024. Adolescents' Perceptions of Privacy Violations by Parents, Siblings, and Friends. *Journal of Research on Adolescence* 34, 4 (2024), 1378–1390. https://doi.org/10.1111/jora.13000

[69] Asher Langton. 2019. Stalking Stalkerware: A Deep Dive Into FlexiSPY. Retrieved 2024-05-25 from https://blogs.juniper.net/en-us/threat-research/stalking-stalkerware-a-deep-dive-into-flexispy-2

[70] Pierre Laperdrix, Naif Mehanna, Antonin Durey, and Walter Rudametkin. 2022. The Price to Play: A Privacy Analysis of Free and Paid Games in the Android Ecosystem. In *Proceedings of the ACM Web Conference 2022 (WWW '22).* ACM, New York, NY, 3440–3449. https://doi.org/10.1145/3485447.3512279

[71] William Largent. 2017. Vulnerability Spotlight: The Circle of a Bug's Life. Retrieved 2023-03-13 from https://blog.talosintelligence.com/vulnerability-spotlight-circle

[72] Timothy Libert. 2018. An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. In *Proceedings of the 2018 World Wide Web Conference (WWW '18).* International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 207–216. https://doi.org/10.1145/3178876.3186087

[73] Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey Voelker, and Damon McCoy. 2023. No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps. *Proceedings on Privacy Enhancing Technologies* 2023, 1 (2023), 207–224. https://doi.org/10.56553/popets-2023-0013

[74] Sonia Livingstone. 2020-01-28. Can We Realise Children's Rights in a Digital World? *Medium* (2020-01-28). Retrieved 2024-02-11 from https://medium.com/reframing-childhood-past-and-present/can-we-realise-childrens-rights-in-a-digital-world-d4f5f19f298f

[75] Sonia Livingstone and Kruakae Pothong. 2023. *Child Rights by Design: Guidance for Innovators of Digital Products and Services Used by Children.* Digital Futures Commission, 5Rights Foundation. http://eprints.lse.ac.uk/id/eprint/119724

[76] Deborah Lupton and Ben Williamson. 2017. The Datafied Child: The Dataveillance of Children and Implications for Their Rights. *New Media & Society* 19, 5 (2017), 780–794. https://doi.org/10.1177/1461444816686328

[77] Philippe Mangeard, Bhaskar Tejaswi, Mohammad Mannan, and Amr Youssef. 2024. WARNE: A Stalkerware Evidence Collection Tool. *Forensic Science International: Digital Investigation* 28 (2024), 1–11. https://doi.org/10.1016/j.fsidi.2023.301677

[78] Mohammad Mannan and Amr Youssef. 2023. *Privacy Analysis of Technologies Used in Intimate Partner Abuse.* Technical Report. Concordia University, Montreal, CA. Retrieved 2024-02-13 from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2022-2023/p_202223_11/

[79] Avi Marciano. 2022. Parental Surveillance and Parenting Styles: Toward a Model of Familial Surveillance Climates. *Mobile Media & Communication* 10, 1 (2022), 38–56. https://doi.org/10.1177/20501579211012436

[80] Gary Marx and Valerie Steeves. 2010. From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society* 7, 3–4 (2010), 192–230. https://doi.org/10.24908/ss.v7i3/4.4152

[81] Jane Mavoa, Simon Coghlan, and Bjørn Nansen. 2023. "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data. *Surveillance & Society* 21, 1 (March 2023), 45–60. https://doi.org/10.24908/ss.v21i1.15719

[82] MobSF2024. 2024. Mobile Security Framework (MobSF). https://github.com/MobSF/Mobile-Security-Framework-MobSF version 4.0.6.

[83] Adam Molnar and Diarmaid Harkin. 2019. *The Consumer Spyware Industry: An Australian-Based Analysis of the Threats of Consumer Spyware.* Technical Report. Australian Communications Consumer Action Network, Sydney. https://accan.org.au/grants/completed-grants/1435-risks-impacts-and-accountability-in-the-consumer-spyware-industry

[84] Charlotte Moremen, Jordan Hoogsteden, and Eleanor Birrell. 2024. Generational Differences in Understandings of Privacy Terminology. *Proceedings on Privacy Enhancing Technologies* 2024, 3 (2024), 589–605. https://doi.org/10.56553/popets-2024-0094

[85] Fiona Scott Morton. 2024. *Entry and Competition in Mobile App Stores.* Technical Report Bruegel Working Paper No. 03/2024. Bruegel, Brussels.

[86] Victoria Nash and Lisa Felton. 2024. Treating the Symptoms or the Disease? Analysing the UK Online Safety Act's Approach to Digital Regulation. *Policy & Internet* (2024), 15 pages. https://doi.org/10.1002/POI3.404

[87] Sophos News. 2020-02-24. *KidsGuard Stalkerware Leaks Data on Secretly Surveilled Victims.* Sophos Ltd. Retrieved 2024-08-29 from https://news.sophos.com/en-us/2020/02/24/kidsguard-stalkerware-leaks-data-on-secretly-surveilled-victims/

[88] NSPCC. 2024. Talking to Your Child About Online Safety. Advice on How to Start the Conversation. Retrieved 2024-08-29 from https://www.nspcc.org.uk/keeping-children-safe/online-safety/talking-child-online-safety/

[89] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society* 23, 1 (2020), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

[90] Office of Public Affairs. 2014. Office of Public Affairs | Man Pleads Guilty for Selling "StealthGenie" Spyware App and Ordered to Pay $500,000 Fine | United States Department of Justice. Retrieved 2023-08-07 from https://www.justice.gov/opa/pr/man-pleads-guilty-selling-stealthgenie-spyware-app-and-ordered-pay-500000-fine

[91] Ehimare Okoyomon, Nikita Samarin, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, Irwin Reyes, Álvaro Feal, and Serge Egelman. 2019. On the Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies. In *Proceedings of the 3rd Workshop on Technology and Consumer Protection (ConPro '19).* IEEE, New York, NY, 7 pages.

[92] L. Lin Ong, Alexa K. Fox, Laurel Aynne Cook, Claire Bessant, Ping-ping Gan, Mariea Grubbs Hoy, Emma Nottingham, Beatriz Pereira, and Stacey Barell Steinberg. 2022. Sharenting in an Evolving Digital World: Increasing Online Connection and Consumer Vulnerability. *Journal of Consumer Affairs* 56, 3 (2022), 1106–1126. https://doi.org/10.1111/joca.12462 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/joca.12462

[93] OWASP Foundation. 2024. Vulnerability Disclosure Cheat Sheet. Retrieved 2024-08-31 from https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

[94] Achilleas Papageorgiou, Michael Strigkos, Eugenia Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. 2018. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. *IEEE Access* 6 (2018), 9390–9403. https://doi.org/10.1109/ACCESS.2018.2799522

[95] Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Robert Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry.* Research Report 119. University of Toronto. 165 pages. https://tspace.library.utoronto.ca/handle/1807/96320

[96] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS 2019).* ISOC, Reston, VA, 15 pages. https://doi.org/10.14722/ndss.2019.23386

[97] Exodus Privacy. 2024. Exodus Privacy. https://exodus-privacy.eu.org version 1.4.0.

[98] Charles Proxy. 2024. Charles Web Debugging Proxy Application. https://www.charlesproxy.com Version 4.6.6.

[99] Venkatesh-Prasad Ranganath and Joydeep Mitra. 2020. Are Free Android App Security Analysis Tools Effective in Detecting Known Vulnerabilities? *Empirical Software Engineering* 25 (2020), 178–219. https://doi.org/10.1007/s10664-019-09749-y

[100] REAndroid. 2024. APK Editor. https://github.com/REAndroid/APKEditor version 1.3.9.

[101] Janice Redish. 2000. Readability Formulas Have Even More Limitations than Klare Discusses. *ACM Journal of Computer Documentation* 24, 3 (2000), 132–137. https://doi.org/10.1145/344599.344637

[102] Desirée Schmuck, Anja Stevic, Jörg Matthes, and Kathrin Karsay. 2023. Out of Control? How Parents' Perceived Lack of Control over Children's Smartphone Use Affects Children's Self-Esteem over Time. *New Media & Society* 25, 1 (2023), 199–219. https://doi.org/10.1177/14614448211011452

[103] Sergey Golubev. 2019. Finding Out What Data Apps Really Collect. Retrieved 2023-01-20 from https://www.kaspersky.com/blog/check-what-data-apps-collect/29120/

[104] Zhiyong Shan, Raina Samuel, and Iulian Neamtiu. 2019. Device Administrator Use and Abuse in Android: Detection and Characterization. In *Proceedings of the 25th Annual International Conference on Mobile Computing and Networking (MobiCom '19).* ACM, New York, NY, Article 51, 16 pages. https://doi.org/10.1145/3300061.3345452

[105] Ahmed Sherif. 2024. Global Market Share Held by Mobile Operating Systems from 2009 to 2023, by Quarter. Retrieved 2024-08-28 from https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[106] Kaiwen Sun, Jingjie Li, Yixin Zou, Jenny Radesky, Christopher Brooks, and Florian Schaub. 2024. Unfulfilled Promises of Child Safety and Privacy: Portrayals and Use of Children in Smart Home Marketing. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1, Article 145 (2024), 29 pages. https://doi.org/10.1145/3637422

[107] Ruoxi Sun, Minhui Xue, Gareth Tyson, Shuo Wang, Seyit Camtepe, and Surya Nepal. 2023. Not Seen, Not Heard in the Digital World! Measuring Privacy Practices in Children's Apps. In *Proceedings of the ACM Web Conference 2023 (WWW '23).* ACM, New York, NY, 2166–2177. https://doi.org/10.1145/3543507.3583327

[108] Ali Sunyaev, Tobias Dehling, Patrick L. Taylor, and Kenneth D. Mandl. 2015. Availability and Quality of Mobile Health App Privacy Policies. *Journal of the American Medical Informatics Association* 22, e1 (2015), e28–e33. https://doi.org/10.1136/amiajnl-2013-002605

[109] Google Play Support. 2024. Google Play Policy Centre Malware. Retrieved 2024-08-18 from https://support.google.com/googleplay/android-developer/answer/9888380?hl=en-GB

[110] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23).* ACM, Hamburg, DE, Article 168, 24 pages. https://doi.org/10.1145/3544548.3581060

[111] Nikki Theofanopoulou, Alissa N. Antle, and Petr Slovak. 2024. "They Don't Come With a Handbook": Exploring Design Opportunities for Supporting Parent-Child Interaction around Emotions in the Family Context. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1, Article 132 (2024), 33 pages. https://doi.org/10.1145/3637409

[112] Melina A. Throuvala, Mark D. Griffiths, Mike Rennoldson, and Daria J. Kuss. 2021. Policy Recommendations for Preventing Problematic Internet Use in Schools: A Qualitative Study of Parental Perspectives. *International Journal of Environmental Research and Public Health* 18, 9, Article 4522 (2021), 23 pages. https://doi.org/10.3390/ijerph18094522

[113] Alanna Titterington. 2023-12-05. *Restricted Settings in Android 13 and 14.* Kaspersky Lab. Retrieved 2023-08-27 from https://www.kaspersky.co.uk/blog/android-restricted-settings/27003/

[114] Aggeliki Tsohou and Eleni Kosta. 2017. Enabling Valid Informed Consent for Location Tracking Through Privacy Awareness of Users: A Process Theory. *Computer Law & Security Review* 33, 4 (2017), 434–457. https://doi.org/10.1016/j.clsr.2017.03.027

[115] UK Information Commissioner's Office. 2020. Age Appropriate Design: A Code of Practice for Online Services (UK AADC). Retrieved 2024-08-31 from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/

[116] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2021. Protection or Punishment? Relating the Design Space of Parental Control Apps and Perceptions About Them to Support Parenting for Online Safety. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–-26. https://doi.org/10.1145/3476084

[117] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2022. 'Don't Make Assumptions About Me!': Understanding Children's Perception of Datafication Online. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2, Article 419 (2022), 24 pages. https://doi.org/10.1145/3555144

[118] Haoyu Wang, Yao Guo, Zihao Tang, Guangdong Bai, and Xiangqun Chen. 2015. Reevaluating Android Permission Gaps with Static and Dynamic Analysis. In *Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM 2015).* IEEE, New York, NY, 6 pages. https://doi.org/10.1109/GLOCOM.2015.7417621

[119] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships. In *Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022).* USENIX Association, Berkeley, CA, 447–462. https://www.usenix.org/conference/soups2022/presentation/wei

[120] Zack Whittaker. 2018. *A Teen Phone Spying App Has Leaked Thousands of User Passwords.* ZDNET. Retrieved 2023-05-01 from https://www.zdnet.com/article/teen-phone-monitoring-app-leaks-thousands-of-users-data/

[121] Zack Whittaker. 2022. Xnspy stalkerware spied on thousands of iPhones and Android devices | TechCrunch. Retrieved 2023-04-29 from https://techcrunch.com/2022/12/12/xnspy-stalkerware-iphone-android/?guccounter=1

[122] Stuart Wood. 2023. *Exploring the Awareness and Usage of Parental Controls to Support Digital Safety.* Technical Report. Internet Matters. Retrieved 2024-01-17 from https://www.internetmatters.org/hub/research/research-tracker-

awareness-usage-parental-controls/

[123] Lei Wu, Michael Grace, Yajin Zhou, Chiachih Wu, and Xuxian Jiang. 2013. The Impact of Vendor Customizations on Android Security. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13)*. ACM, New York, NY, 623–634. https://doi.org/10.1145/2508859.2516728

[124] Yuxuan Yan, Zhenhua Li, Qi Alfred Chen, Christo Wilson, Tianyin Xu, Ennan Zhai, Yong Li, and Yunhao Liu. 2019. Understanding and Detecting Overlay-Based Android Malware at Market Scales. In *Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19)*. ACM, New York, NY, 168–179. https://doi.org/10.1145/3307334.3326094

[125] Bieke Zaman and Marije Nouwen. 2016. *Parental Controls: Advice for Parents, Researchers and Industry*. Technical Report. EU Kids Online. http://eprints.lse.ac.uk/id/eprint/65388

[126] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. 2024. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies* 2024, 1 (2024), 133–150. https://doi.org/10.56553/popets-2024-0009

A App Selection Search Terms

(1) app to manage kid's phone remotely android
(2) best app to track kid's phone android
(3) best child monitoring apps android
(4) best parental control apps android
(5) child monitoring app android
(6) free child monitoring apps android
(7) free parental control apps android
(8) how to control kid's phone usage android
(9) how to monitor child's online activity android
(10) how to monitor child's phone android
(11) parental control app android
(12) phone monitoring app for kids android
(13) phone monitoring for parents android
(14) remote phone monitoring for parents android
(15) safe phone monitoring for children android

B Privacy Policies and Trackers

Table 3: Parental Control App Privacy Policies

App Name	Available	Applicable	Scope	Location	Flesch-Kincaid Score	Length in Characters
Alli360	●	●	MA, W	S	25.47	12787
AnyControl	●	●	AS	W	27.50	4080
Bark	●	●	A, W	W	30.55	26104
Chyldmonitor	●		W	W		
Cocospy	●		W	A		
ESET Parental Control	●	●	AS	S	34.16	12305
EvaSpy	●		W	A		
FamilyTime Jr.	●	●	A	A	29.33	10915
FamiSafe Kids	●	●	AS	S	20.51	23213
FlexiSpy	●		W	W		
Hoverwatch	●	●	AS	W	41.73	17877
iKeyMonitor	●		W	W		
iSharing	●	●	A, W	S	22.84	20972
Kaspersky SafeKids	●	●	AS	S	18.06	34358
KidControl						
Kidlogger	●		W	W		
Kids Place	●	●	A, W	S	32.22	9954
Kidslox	●	●	AS	S	40.83	9110
Kidstracker	●	●	AS	W	27.88	9736
Kidsy	●	●	MA	S	44.61	37385
Kroha	●	●	A, W	S	28.22	22687
Life360	●	●	AS	S	27.87	57578
Microsoft Family Safety	●	●	AS	S	30.12	31399
MMGuardian	●	●	AS	A	25.45	24487
MobileFence	●	●	A, W	S	34.91	3717
MoniMaster	●	●	A, W	A	18.53	11675
mSpy	●		W	W		
Pingo	●	●	AS	S	38.85	36448
Qustodio	●	●	AS	S	28.26	41844
Spapp Monitoring	●	●	A, W	W	30.36	27996
Spy Phone Labs Phone Tracker	●	●	A, W	A	51.84	6755
SPY24	●	●	A, W	W	37.38	10019
SPYX	●		W	A		
ST Kids App	●	●	AS	S	30.67	16952
TheOneSpy	●		W	W		
Tigrow!	●	●	A, W	S	32.05	19728
TiSpy	●		W	A		
uMobix	●	●	A, W	W	54.95	19454
WebWatcher	●	U	U	W	28.15	13007
XNSPY	●	●	AS	W	30.27	12365

Abbreviations: A = App, AS = All Services, MA = Multiple Apps, S = Google Play Store, U = Unclear, W = Website

Table 4: Trackers Used by Parental Control Apps

App Name	ACRA	Adjust	Amplitude	AppsFlyer	Branch	Braze	Didomi	Facebook Analytics	Facebook Login	Facebook Share	Flurry	Google Admob	Google Analytics	Google CrashLytics	Google Firebase Analytics	Google Tag Manager	Huawei Mobile Services Core	Huq Sourcekit	Instabug	Microsoft Visual Studio App Center Analytics	Microsoft Visual Studio App Center Crashes	OneSignal	Pusher	Segment	Sensors Analytics	Sentiance	Sentry	Singular	Umeng Analytics
Alli360				●										●	●		●												
AnyControl														●	●														
Bark															●		●					●						●	
Chyldmonitor															●														
Cocospy																													●
ESET Parental Control														●															
EvaSpy																													
FamilyTime Jr.														●	●								●						
FamiSafe Kids		●		●				●	●	●				●	●										●				
FlexiSpy															●														
Hoverwatch																													
iKeyMonitor	●													●	●														
iSharing				●		●			●	●		●		●	●		●	●											
Kaspersky SafeKids				●									●	●	●	●	●												
KidControl												●		●	●		●												
Kidlogger																													
Kids Place												●	●	●	●														
Kidslox			●						●				●	●	●	●												●	
Kidstracker														●															
Kidsy				●										●	●														
Kroha				●										●	●														
Life360				●	●							●		●	●														
Microsoft Family Safety																				●	●						●		
MMGuardian								●	●			●	●	●	●	●													
MobileFence														●	●														
MoniMaster														●	●														
mSpy			●	●										●	●														
Pingo				●										●	●														
Qustodio														●	●									●					
Spapp Monitoring																													
Spy Phone Labs Phone Tracker																													
SPY24																			●										
SPYX																													
ST Kids App								●	●	●			●	●	●	●													
TheOneSpy														●	●														
Tigrow!														●															
TiSpy						●					●																		
uMobix			●									●		●	●														
WebWatcher														●	●														
XNSPY												●	●	●	●	●													