



Kent Academic Repository

Fitzpatrick, Jamie and Franqueira, Virginia N. L. (2025) *Analysis of Permissions and Trackers in Android Apps Targeting Children Under Thirteen*. In: Praça, Isabel and Bernardi, Simona and Inácio, Pedro R.M., eds. *Cybersecurity. 9th European Interdisciplinary Cybersecurity Conference, EICC 2025, Rennes, France, June 18–19, 2025, Proceedings. Communications in Computer and Information Science* . Springer Nature E-ISBN 978-3-031-94855-8.

Downloaded from

<https://kar.kent.ac.uk/109993/> The University of Kent's Academic Repository KAR

The version of record is available from

https://doi.org/10.1007/978-3-031-94855-8_5

This document version

Author's Accepted Manuscript

DOI for this version

Licence for this version

UNSPECIFIED

Additional information

Versions of research works

Versions of Record

If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts

If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in **Title of Journal** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries

If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our [Take Down policy](https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies) (available from <https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies>).

Analysis of Permissions and Trackers in Android Apps Targeting Children Under Thirteen

Jamie Fitzpatrick and Virginia N. L. Franqueira ✉^[0000–0003–1332–9115]

Institute of Cyber Security for Society (iCSS), School of Computing
University of Kent, Canterbury, CT2 7NP, UK
jamiefitz07@outlook.com, ✉ v.franqueira@kent.ac.uk

Abstract. As mobile phone and app use among children increases, ensuring their privacy and safety has become more crucial. This study examines 27 popular Android apps for children under 13, available in the UK via Google Play Store, by analysing the permissions they request and the trackers they share data with. The aim is to determine whether these practices are justified by the apps’ functionalities, and comply with regulatory standards to adequately protect children. Using a traffic light system inspired by the ICO audits, each app is rated green, amber, or red taking into account dangerous permissions and runtime trackers in use. Only one app reached an overall green rating, while 10 apps achieved an overall red rating. The majority of tracker companies (20 out of 21) are based outside the UK or EU, including the US, Russia, China, Israel and India, and two trackers are linked to profiling and fingerprinting of users. Overall, findings suggest that apps often prioritise functionality and user experience over privacy and safety of children.

Keywords: Apps compliance · tracking behaviours · dangerous permissions · children privacy and safety · ICO Children’s code · traffic light.

1 Introduction

The Office of Communications (Ofcom) revealed that, as of 2024, 96% of children aged 3-17 went online and, by age 11, nine of ten children had their own mobile phones, with some children using digital devices as young as three [26]. The Coronavirus (COVID-19) pandemic further amplified children’s use of technology, as represented by a longitudinal study which spanned from pre-pandemic to restrictions being lifted [16]. Therefore, this current prevalence of technology is urging a focus on protecting young people and ensuring that risks associated with its use do not overshadow the potential benefits.

There has been a considerable increase in the use of digital technologies to facilitate education, particularly during and following the pandemic [4]. Such use of technology in schools has garnered both positive and negative feedback. On the positive side, educators report that integrating technology into the curriculum helps students acquire essential skills valuable to future education and careers [33]. However, the risks cannot be overlooked, as children may be exposed

to different types of harm [24]. Educational applications (apps) are a desirable tool for teachers and parents because they provide easy access to relevant materials in informal settings [17]. However, it can be challenging for parents and educators to evaluate whether an app is safe for children.

When discussing “privacy concerns”, the focus is on how apps collect, use, store, and share children’s personal information. Westin [32] defined privacy as the right of individuals, groups, or institutions to decide when, how, and to what extent information about themselves is disclosed to others. Consent, however, is often obscured and difficult to comprehend [1]. Reyes et al. [27] studied apps’ compliance against the Children’s Online Privacy Protection Act (COPPA) in the US, and found that many apps potentially violate this regulation by engaging in third-party tracking. Similarly, Livingstone et al. [24] noted that children are more vulnerable to online privacy threats than adults due to their lack of awareness of the risks. Children’s ability to navigate and mindfully avoid potential privacy risks may vary depending on their development, digital skills, or socio-economic circumstances [24]. Although there are existing measures to protect children using technology, such as parental controls to monitor and limit device usage [10], these techniques primarily focus on avoiding exposure to age-inappropriate content. Additionally, some controls require access to system resources and sensitive data on the child’s phone to function properly. So, while limiting exposure to harmful content, they may inadvertently increase privacy concerns by collecting more data than necessary [10].

The contribution of this study is threefold. Firstly, it provides a comparative evaluation of privacy risks for 27 Android most popular apps listed as for “Children” in the Google Play Store. Adapting the ICO audits traffic light rating system [18]¹, it provides an overview of unjustified dangerous permissions and runtime trackers per app and by category. The literature revealed that previous publications either focused on permissions or on trackers – but not both, and did not evaluate whether dangerous permissions were justified by the functionalities provided by the apps. Secondly, using static and dynamic analysis complemented by manual inspection, it highlights critical gaps in current app practices explicitly designed for children, particularly concerning transparency, unnecessary dangerous permissions, and non-compliance with data protection regulations. Thirdly, the study provides a map of trackers identified as in use by the apps with location of parent company and the type of tracking used, revealing that only one of 21 is based in the UK or EU, with the remaining located in US, Russia, China, Israel and India. Previous work focused on mobile apps in general, although eventually covering some apps for children.

The remainder of the paper is structured as follows. Section 2 reviews related work, while Section 3 presents the scope of this study and the methodology followed. Section 4 outlines the key findings of permissions and trackers, and provides category-based results. Section 5 applies a traffic light rating system to the apps, and discusses the implications of the findings. Finally, Section 6 concludes the paper.

¹ Called “assurance ratings” by ICO.

2 Related Work

This section reviews the literature related to the analysis of privacy in Android apps (Section 2.1), and applicable laws and regulations (Section 2.2).

2.1 Privacy of Android Apps

A wide range of research has analysed the privacy practices of apps on the Google Play Store, with many diving into the prevalence and implications of third-party tracking and Android permissions (e.g., [3,5,8,11,21,23]). However, there was a lack of studies specifically focusing on children apps. Furthermore, although the related works tended to use much larger samples than this study, they either focused on trackers or on permissions, and did not try to understand if dangerous permissions were justified by app functionalities.

Research on third-party tracking often employs both static and dynamic analysis. Static analysis examines an app’s behaviour without executing it, therefore relying on decompiling it to view its code [21]. Dynamic analysis, however, involves running an app and observing its behaviours, such as looking at its network traffic [23]. Binns et al. [3] studied 959,000 apps from the UK and US Google Play Stores, using the APKTool to decompile their APK files and map trackers to known tracking companies found during previous studies. They found that most apps contained third-party tracking, especially in the “News”, “Games & Entertainment” and “Family” super genres, raising concerns about compliance with the GDPR (see Section 2.2). It was also recognised that the parent companies connected to various trackers were seen to operate outside of the EU. However, the authors only used static analysis of trackers while this research involved static and dynamic analysis of trackers, and reported on the latter in the traffic light comparison of apps. Also, their results date to six years ago, justifying the need for the study reported in this paper.

Concerning regulations, Kollnig et al. [21] investigated the absence of consent in apps using third-party tracking in a random sample of 1,201 apps. Each app was run for 15 seconds and then immediately uninstalled to find which companies were contacted before the opportunity to consent. The tool NetGuard was used to analyse the network traffic, and it was found that most apps engaged in tracking but very few required explicit consent, violating privacy laws.

Ekambaranathan et al. [8] conducted surveys and structured interviews to identify developers’ understanding of their responsibilities, the practices they adopted in development, the barriers they faced in adopting data protection frameworks, and how they overcame these. It was found that, although developers recognised that children’s apps should be designed to ensure they are age-appropriate and meet developmental needs, they faced challenges in finding guidelines to do so. It was also found that developers made compromises to add third-party tracking libraries to the code to allow for monetisation, especially with perceived “harmless” libraries such as Google Analytics.

Regarding Android permissions, Calciati et al. [5] analysed almost 3 million app releases, including different versions of the same apps. They found that

17% of the apps added new dangerous permissions, or moved existing ones to granted permission groups between releases, without user knowledge or consent. Felt et al. [11] developed Stowaway, a tool that determines a set of API calls and maps them to a specific permission to determine if an app is requesting more permissions than necessary. About one-third of their sample (940 apps) were over-privileged, although it was acknowledged that this may be unintentional due to API poor documentation.

2.2 Laws and Regulations

The abundance of mobile apps in recent decades has changed how children access information and interact, offering education and entertainment opportunities. However, they also raise concerns about children’s data privacy and online safety [24]. To address these issues, regulations have evolved to include more specific requirements for children’s apps.

The General Data Protection Regulation (GDPR) sets a high standard for data protection, promoting fair and lawful data collection and users’ right to access, erase, or modify their data [9, Article 8]. For children, the GDPR requires transparency about data collection and clear consent by parents. It also strictly restricts profiling and automated decision-making, ensuring that children are not inappropriately targeted or influenced by digital marketing without appropriate safeguards. Overall, it shifts focus towards protecting user data and ensuring transparency in data collection practices within apps used by children.

In the UK, the Data Protection Act (2018) [28] incorporates the GDPR principles, ensuring data protection for all users. The Privacy and Electronic Communications Regulations (PECR) [29] legislation further safeguards children by controlling how communications tools are used within apps, protecting them from harmful content and unsolicited marketing [20]. Additionally, the Online Safety Act [30] calls for robust age verification mechanisms for access to adult content, e.g., check of official documents, and reliable age estimation to meet the minimum requirement of 13 years old for social media.

The Information Commissioner’s Office (ICO) enforces the Children’s code, which includes 15 standards for developers of children’s apps [19]. This code applies to any “information society services” likely accessed by children, including apps and social media platforms. The key principle is that children’s best interests should guide all aspects of design and development. The code mandates Data Protection Impact Assessments (DPIAs) to identify risks and actively implement mitigation measures. The standards also focus on limiting data collection, particularly sensitive data such as location, and emphasise transparency. Additionally, the ICO states that profiling should not cause harm or compromise safety and should be avoided (or limited) if an app can function without it.

3 Methodology

The regulations, reviewed in Section 2.2, aim to create a safer digital environment for children, although questions remain about the extent of compliance – the

focus of this study. This section describes the research methodology employed to investigate permissions and tracking behaviours of Android apps for children.

3.1 Research Scope

This study examines the data privacy practices of children’s apps on the Google Play Store. It focuses on free apps in the “Children” category, for ages 0-12. Free apps were chosen to ensure accessibility across socio-economic backgrounds. Thirty most popular apps were selected for analysis to exemplify widely used apps and provide a valuable snapshot. The study examines apps available in the UK, which could offer insights applicable to other regions with similar regulations.

3.2 Research Design

A mixed-methods approach was used, combining quantitative data analysis with qualitative assessment of apps’ main functionalities. This enabled a thorough examination of both permissions and trackers, and their practical implications.

Data collection and tools used. Data was collected using the google-play-scraper tool² (on July 15, 2024), to identify the top 30 free apps in the Children category. This tool enables customisation of responses via JavaScript input, allowing for specified outputs depending on characteristics such as country (“UK”) and category (“Children”). Apart from the 30 apps initially selected and, due to its popularity and existing concerns at the time of the study [15], the Roblox app was also included. The information available on the Google Play Store (as of July 18, 2024) regarding each app’s version was also collected using the Play Store interface to ensure consistency in the permission and trackers analysis throughout the study.

Each app’s APK file was downloaded using APKPure³, and analysed using APKTool⁴ to extract the Android Manifest file, enabling investigation of the permissions contained within the apps’ metadata.

TrackerControl (TC), an app developed by Kollnig et al. [22], was used to observe the tracking behaviours of the sample apps installed on an Android device (a Samsung Galaxy A20e running Android 11). TC helped to identify tracking libraries found in the apps’ code (static analysis) and to detect the tracker domains at work during runtime (dynamic analysis). The APKTool can only be used for static analysis of trackers while TC can do both types of analysis, therefore, we opted for APKTool to study permissions and TC to study trackers.

Four apps were excluded due to inconsistencies among app versions available for data collection (i.e., *Nat West Rooster Money*, *CBeebies Playtime Island*, and *CBeebies Little Learners*), and because an APK could not be reliably accessed

² <https://pypi.org/project/google-play-scraper/>

³ <https://apkpure.com/>

⁴ <https://apktool.org/>

(for *LEGO DUPLO Peppa Pig*). Thus, to maintain consistency of data collection and analysis, these apps were not included in the final sample of 27 apps.

Data Analysis. As aforementioned, each of the 27 apps was downloaded and opened on the testing Galaxy Android device. Doing so meant that the functionalities of each app could be examined, allowing the apps to be categorised based on these observations.

The quantitative analysis involved descriptive statistics of the permissions and tracking data collected. The qualitative analysis included determining if dangerous permissions could be justified by the main app functionalities. It also involved using the apps’ tracker domains, recovered from TC, to investigate (using Exodus⁵) the type of tracking, their parent company, and their country of origin.

Dangerous permissions, also known as runtime permissions, grant app access to restricted data and actions. Android defines [13] “restricted data” as sensitive information stored on or about the device, such as contact details or system state, and “restricted actions” as those typically performed by the user, like recording audio or video. Due to their potential to access sensitive personal data and impact device functionality or other apps, these permissions must be explicitly requested during app runtime.

In this study, the traffic light ratings from ICO audits [18] were adapted as follows. Only dangerous permissions and runtime tracking, uncovered via dynamic analysis of trackers, were considered for this purpose.

- Permissions
 - **Red:** Dangerous permissions cannot be justified by app’s functionalities.
 - **Amber:** Dangerous permissions can be justified by app’s functionalities.
 - **Green:** No dangerous permissions used by app.
- Trackers
 - **Red:** 4 or more runtime tracking companies associated with app.
 - **Amber:** 1-3 runtime tracking companies associated with app.
 - **Green:** No runtime tracking companies associated with app.
- Overall
 - **Red:** A combination of a red and an amber rating, or two red ratings.
 - **Amber:** A combination of a green and an amber rating, or two amber.
 - **Green:** A combination of two green ratings for permissions and trackers.

4 Findings

First, the primary functionalities of each of the 27 apps were observed, leading to the categories shown in Table 1. Please note that these categories were not based on existing Google Play Store categories, but were assigned through testing each app and observing their functionalities first-hand.

⁵ <https://etip.exodus-privacy.eu.org>

Table 1. The apps in our sample categorised based on their primary functionalities.

Category	Description	Apps in the sample
Educational	Apps enhancing learning through interactive lessons	<i>ClassDojo</i> , <i>Kahoot</i> , <i>ScratchJr</i> , <i>Minecraft Education</i> , <i>PAW Patrol Academy</i> , <i>Times Tables Rock Stars</i> , <i>Sago Mini School</i>
Role-Playing & Simulation	Apps providing an immersive environment for character-driven narratives or real-life simulations	<i>Toca Boca World</i> , <i>Avatar World</i> , <i>Toca Boca Jr</i> , <i>Disney Frozen Royal Castle</i> , <i>Bluey: Let's Play</i> , <i>Baby Panda's School Bus</i> , <i>Aha World: School Day</i>
Creative	Apps promoting creativity	<i>Toca Boca Hair Salon 4</i> , <i>Coloring Games: Color & Paint</i> , <i>LEGO Builder</i> , <i>Little Panda's Ice Cream Games</i> , <i>Cake maker: Kids Cooking Games</i> , <i>Disney Coloring World</i>
Casual & Action	Apps that are focused on entertainment	<i>Fluvsies - A Fluff to Luv</i> , <i>Fluvsies Merge Party</i> , <i>slither.io</i> , <i>Tag with Ryan</i>
Video & Content	Apps delivering or facilitating video content	<i>YouTube Kids</i> , <i>VLC for Android</i>
	App uncategorised due to its distinctive nature as a gaming platform and interactive world	<i>Roblox</i>

4.1 Findings Related to Permissions

This section details the findings related to Android permissions for the 27 apps, highlighting trends to understand the types of permissions requested.

Overview of Permissions. Figure 1 presents the total number of permissions found in each app, organised by category. Across all apps, 66 distinct permissions were identified, with an average of 11.96 permissions requested per app (standard deviation: 6.38). Four apps had 20 or more permissions, with *ClassDojo* having the highest at 29. *Coloring Games: Color & Paint* had the fewest at 3.

Notably, the apps with the most permissions are spread across different categories, challenging the hypothesis that certain categories request more permissions. However, apps in the “Video & Content” category show a significantly higher average number of permissions (18), likely due to the additional functionalities needed for video platforms (e.g., media storage access), compared to simpler apps like colouring apps. The *Aha World: School Day* app is an outlier in the “Role-Play & Simulation” category with 26 permissions, much higher than the category’s average of 9.5, and the *ClassDojo* app similarly exceeds the “Educational” category average of 10, with 29 permissions.

Dangerous Permissions. The dangerous permissions found in the app sample were analysed using two approaches. First, a quantitative analysis examined the

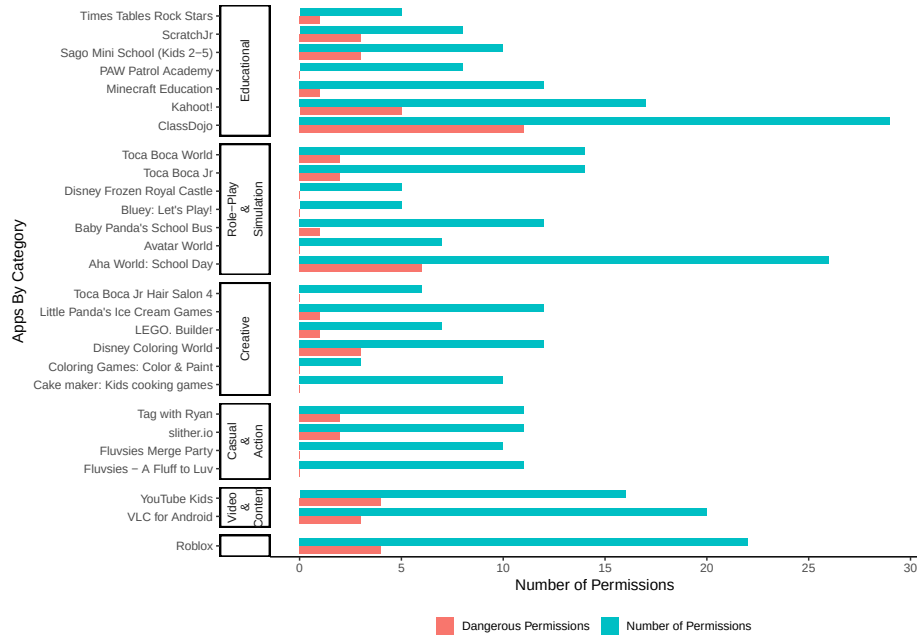


Fig. 1. Number of permissions and of dangerous permissions per app by category.

number of dangerous permissions requested across apps and categories. Second, a qualitative analysis assessed whether each dangerous permission can be justified based on the functionalities of the app requesting it.

Quantitative Observations. Figure 1 highlights the number of dangerous permissions requested by the 27 apps, revealing some notable discrepancies elaborated next. *ClassDojo*, an “Educational” app, stands out with 11 dangerous permissions. On the other hand, *PAW Patrol Academy*, in the same category, requests no dangerous permissions. This contrast is noticeable in 3 other categories with 9 apps in total requesting no dangerous permissions, i.e., “Role-Play & Simulation”, “Creative” and “Casual & Action”.

Qualitative Observations. This section assesses whether dangerous permissions requested by apps, per category, are justified by functionalities.

Educational Apps

Four out of 7 “Educational” apps request the *POST_NOTIFICATIONS* permission, which is justified by notification features such as class updates (*ClassDojo*) or to maintain engagement through content updates (*Kahoot*, *Minecraft Education*, and *PAW Patrol Academy*).

ClassDojo and *Kahoot* request microphone-related permissions (*RECORD_AUDIO* and *AUDIO_CAPTURE*). These are justified by functions like record-

ing voice messages such as a teacher giving instructions (*ClassDojo*) and incorporating audio in quizzes (*Kahoot*). Similarly, permissions for accessing media files (*READ_MEDIA_AUDIO*, *READ_MEDIA_VIDEO*, *READ_MEDIA_IMAGES*) in these apps are required to upload and use multimedia files. The app *ScratchJr* also requests access to the microphone through *AUDIO_CAPTURE*, which can be explained by the app’s recording function allowing users to add audio to their coding projects.

ScratchJr, *ClassDojo* and *Kahoot* also request camera access for capturing images or videos for use in projects or quizzes, which is consistent with their functionalities. Storage permissions (*READ_EXTERNAL_STORAGE* and *WRITE_EXTERNAL_STORAGE*) are important to justify due to the sensitivity of accessing and changing device data. *ClassDojo* and *Kahoot* both have upload and download functionalities, and *Sago Mini School* requires each activity to be downloaded locally before use.

Times Tables Rock Stars allows teachers to download data about each child in their class, displaying statistics on progress and completion of homework. This app also allows users to play without an internet connection, which means that data on progress and app settings would be required to facilitate offline play, meaning access to the device’s storage could be justified. *Minecraft Education* needs access to write to the device storage to save game data and to allow the user to continue on “missions” upon return to the app. Finally, *ScratchJr* allows users to upload files from their device to display in the app and incorporate into their coding learning.

ClassDojo’s “approximate location access” potentially raises concerns; it is used to help users locate nearby schools during registration. However, no explicit request for location access was noted when first running the app during testing.

Role-Play & Simulation Apps

There are fewer dangerous permissions in this category. Three apps (*Toca Boca World*, *Toca Boca Jr*, *Avatar World*) request storage access which may be to save game progress and images, justifying this permission. *Aha World: School Day* requests microphone access for voice-over features, which is clearly justified. However, its request for media access lacks clear functionality, as there are no ways to upload images, audio, or video, and this could raise privacy concerns.

A potentially unjustified permission is *Baby Panda’s School Bus*’s ability to download without notifying the user. While it could be used for updates, silent downloads pose risks if exploited by malicious actors.

Creative Apps

Few dangerous permissions were found in the ‘Creative’ category. *LEGO Builder*’s camera access allows users to scan QR codes on LEGO sets to find their building instructions, which is clearly justified. Also, *Disney Coloring World* allows notifications and requests storage data to save the user’s artwork.

However, *Little Panda’s Ice Cream Games* has the ability to download without notification, which, as mentioned, can represent high risk if the files being downloaded are not safe or relevant to the app itself.

Casual & Action Apps

Only two apps in this category request any dangerous permissions. *Tag With Ryan* accesses device storage which can be used to save game progress, thus justified. *Slither.io*, however, requests access to the phone state. This poses a risk since it allows access to the status of any ongoing calls, cellular network information and the Telecom account registered on the device. It is unknown if this could reveal account details and geolocation, which could be indirectly correlated to a child using the phone [14].

Video & Content Apps

The *YouTube Kids* app requests *GET_ACCOUNTS*, likely to connect to a Google account for parental control or expanded content access. Microphone access is justified in association with the search functionality offered by “Hello Google”. *YouTube Kids* may also offer notification updates like its partner app *YouTube* (not part of this study). However, the need to access storage is not clear, as it does not seem that users can download content from the app. *VLC for Android*’s storage access is justified by the app’s functionality of playing downloaded media, but the ability to access the microphone is questionable. This is because the app appears to only be a media player, not recorder, so microphone access is likely not essential.

Roblox App

Roblox requests four dangerous permissions. *WRITE_EXTERNAL_STORAGE* and *READ_EXTERNAL_STORAGE* are justified by the app’s ability to save gameplay screenshots or videos. *READ_CONTACTS*, though potentially high-risk, has a clear use within the platform to connect players via contact information using phone numbers or emails linked to Roblox accounts. The app offers *POST_NOTIFICATIONS* to inform users on game updates and app-wide events.

4.2 Findings Related to Trackers

Figure 2 summarises the number of tracking companies observed in each app during both static and dynamic analysis, by category. Two of the apps had the highest number of tracking libraries: *Fluvsies Merge Party* and its variant *Fluvsies – A Fluff to Luv*, each containing 9 in total observed during dynamic analysis, which corresponded to 7 distinct tracking companies. In contrast, 2 of the apps used no tracker libraries at all (*VLC for Android* and *Coloring Games: Color & Paint*). On average, each app contained approximately 3.67 tracker libraries, with a standard deviation of 2.22, indicating that there was only moderate variability across the sample.

ScratchJr revealed trackers during static analysis only, while 2 apps only revealed trackers during dynamic analysis (i.e., *Times Tables Rock Stars* and *Avatar World*). This mismatch is further discussed in Section 5.4.

Overall, there is an observable difference in the average number of tracking companies associated with each category. “Casual & Action” apps show a greater number of tracking companies compared to the rest of the categories, likely due to the higher numbers found in the two *Fluvsies* apps. “Video & Content” apps

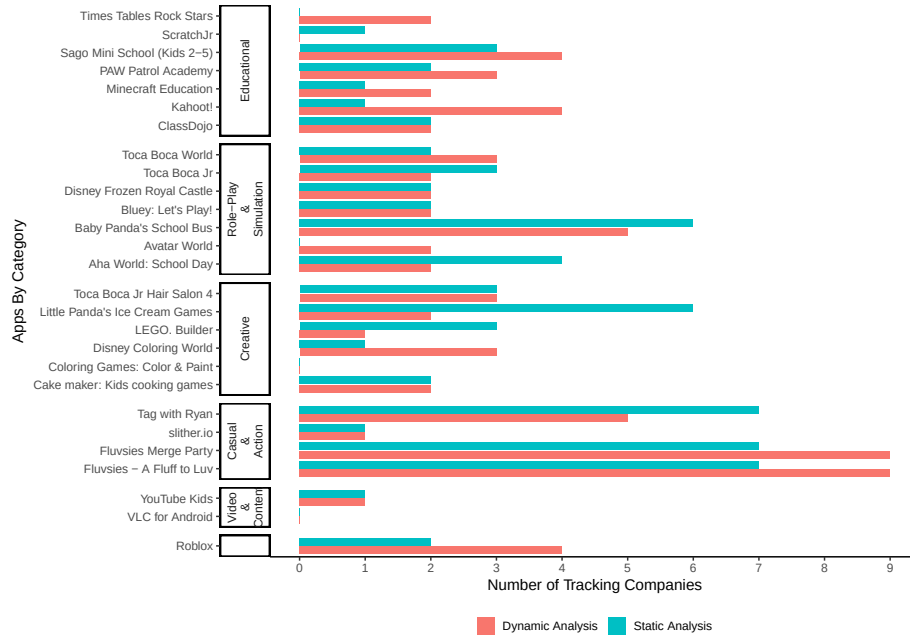


Fig. 2. Number of tracker companies from static/dynamic analysis per app by category.

have fewer associated tracking companies than the rest of the categories, with an average of only 0.5.

Static Analysis of Trackers. Across the 27 apps, 15 distinct tracking companies were found during static analysis. Google was the most common owner of the tracking libraries found within the apps, present in 23 out of 27 apps. This starkly contrasted with the next most common tracker company, AppsFlyer, which was only found in 8 apps. On the other hand, AppMetrica and Moat were the least common, each appearing in just one app.

Dynamic Analysis of Trackers. During runtime, there were considerably more tracking companies observed in each of the apps, and the total number of distinct companies rose to 22 from 15 in static analysis.

When investigating the tracking companies and the type of tracking they partake in, the most common forms were “Analytics” and “Advertisement”. In the sample, 35 analytics tracking domains and 25 advertisement tracking domains across the apps were observed in total. An interesting finding was the presence of “Fingerprinting”, identified exclusively within Google’s DoubleClick domain. Potentially more concerning, however, was the detection of “Profiling” activities conducted by Amplitude, a company active across three apps: *Bluey: Let’s Play*, *Kahoot*, and *Disney Frozen Royal Castle*. Profiling involves the creation of de-

Table 2. Tracking companies mapped to other details including number of apps from static and dynamic analysis. (The table is in order of total tracking.)

Company	Parent Company	Country	Apps Static	Apps Dynamic	Tracking Use
Google	Alphabet	US	23	20	Analytics, Advertisement, Crash Reporting, Fingerprinting
Unity Technologies	Unity Technologies	US	5	9	Advertisement
AppsFlyer	AppsFlyer	US	8	4	Advertisement
MixPanel	MixPanel	US	3	4	Analytics
Amazon	Amazon	US		6	Analytics
Singular	Singular	US	3	3	Analytics
KIDOZ	Shaol Games	Israel	3	3	Analytics, Advertisement
SuperAwesome	SuperAwesome	UK	3	3	Advertisement
IAB Open Measurement	IAB Tech Lab	US	5		Advertisement
Amplitude	Amplitude	US	2	3	Analytics, Profiling
ironSource	Unity Technologies	Israel	4		Analytics
Sentry	Functional Software Inc	US	3	1	Crash Reporting
Blackstone	Blackstone	US		3	Advertisement
Tencent	Tencent	China		3	Analytics
Bugly	Tencent	China	3		Crash reporting, Analytics
InMobi	InMobi	India	2	1	Advertisement
Microsoft	Microsoft	US		2	Analytics, Crash Reporting
Yandex	Yandex	Russia		1	Advertisement
SuperSonic Ads	ironSource	US		1	Advertisement
AppMetrica	Yandex	Russia	1		Analytics
Moat	Oracle	US	1		Advertisement, Analytics

tailed user profiles, which raises significant privacy concerns, particularly in the context of children’s apps.

By mapping known tracking domains to their parent companies and corresponding countries, it was revealed that just one company, SuperAwesome, was based in the UK. As shown in Table 2, the majority of the trackers were linked to companies operating in the US, with 11 of the 16 companies based there. Additionally, trackers from companies operating in Israel, Russia, India, and China were detected, clearly highlighting the global distribution of tracking activities and raising questions about their operation outside of the jurisdiction of the UK, and therefore their compliance with the regulations covered in Section 2.2.

5 Discussion

This section discusses the key takeaways and lessons learned from this study.

5.1 Traffic Light Analysis

Table 3 illustrates the resulting ratings of each app regarding the dangerous permissions and their ability to be justified by apps’ functionalities (Section 4.1) and the number of tracking companies associated with the apps during runtime (Section 4.2). This table provides an overlook of the app ratings, following the criteria for red, amber and green, outlined in Section 3.2.

Using the traffic light analysis, only one app (*Coloring Games: Color & Paint*) had an overall green rating. Out of 27 total apps in the sample for this study, 10 of them had an overall red rating. Although this is not statistically significant, in the context of child safety using those apps, this is significant. The fact that red ratings were not just confined to one or a few categories raises concerns regarding the safety of children’s apps as a whole. Whilst it is acknowledged that it would be impossible to demand apps not to engage in any of these behaviours, the extent to which these apps reflect potentially unsafe circumstances for children under 13 asks for intervention.

As apparent in Table 3, apps are much more likely to acquire a green rating in permissions (9) than in trackers (3). This is because, although dangerous permissions are present in the majority of the apps, their functionalities allow the requests to be justified. In terms of trackers, however, justifying the number is much more difficult in that tracking behaviours, such as collecting and further sharing data, carry much more privacy implications than if an app legitimately uses a permission for its sole purpose within the app.

5.2 Permissions in Children’s Apps

The fact that some apps do not require any dangerous permissions may raise questions about the necessity of such permissions in other apps, e.g., if within the same category. It suggests that, for some functionalities, dangerous permissions may not always be essential to the core operations of an app. This could highlight potential areas where apps may be over-privileged, and developers might need to reconsider the scope of the permissions they are requesting. However, it is acknowledged that for certain functionalities, such as apps related to media like *VLC Player*, apps would need specific dangerous permissions to work as intended. On the other hand, some apps could potentially do without certain functionalities, such as child input through the device camera or microphone. Such apps would function just the same with the removal of these dangerous permissions and would decrease the overall risks for children’s using them. This queries the extent to which developers follow the Google Play Store-recommended development strategy of minimal permission requests [13] or whether such developers create over-privileged apps only with the user experience in mind.

Table 3. The traffic light rating of each app by category, considering dangerous permissions and runtime tracking. (Note: “Perm.” is an abbreviation for “Permissions”.)

App	Category	Perm. Rating	Trackers Rating	Overall Rating
ClassDojo	Educational	Red	Amber	Red
Kahoot!	Educational	Amber	Red	Red
Minecraft Education	Educational	Amber	Amber	Amber
PAW Patrol Academy	Educational	Green	Amber	Amber
Sago Mini School	Educational	Amber	Red	Red
ScratchJr	Educational	Amber	Green	Amber
Times Tables Rock Stars	Educational	Amber	Amber	Amber
Aha World: School Day	Role-Play & Simulation	Red	Amber	Red
Avatar World	Role-Play & Simulation	Green	Amber	Amber
Baby Panda’s School Bus	Role-Play & Simulation	Red	Red	Red
Bluey: Let’s Play!	Role-Play & Simulation	Green	Amber	Amber
Disney Frozen Royal Castle	Role-Play & Simulation	Green	Amber	Amber
Toca Boca Jr	Role-Play & Simulation	Amber	Amber	Amber
Toca Boca World	Role-Play & Simulation	Amber	Amber	Amber
Cake maker: Kids cooking games	Creative	Green	Amber	Amber
Coloring Games: Color & Paint	Creative	Green	Green	Green
Disney Coloring World	Creative	Amber	Amber	Amber
LEGO® Builder	Creative	Amber	Amber	Amber
Little Panda’s Ice Cream Games	Creative	Red	Amber	Red
Toca Boca Jr Hair Salon 4	Creative	Green	Amber	Amber
Fluvsies - A Fluff to Luv	Casual & Action	Green	Red	Amber
Fluvsies Merge Party	Casual & Action	Green	Red	Amber
slither.io	Casual & Action	Red	Amber	Red
Tag with Ryan	Casual & Action	Amber	Red	Red
VLC for Android	Video & Content	Red	Green	Amber
YouTube Kids	Video & Content	Red	Amber	Red
Roblox	N/A	Amber	Red	Red

Considering *Roblox* was of particular concern initially, it was unfortunate to see that the app received an overall red rating, and it was on par with many of the other apps in the sample. It indicates that the extent of privacy issues related to popular online platforms used by children are not unique, although findings are not generalisable.

Fortunately, as prescribed in the ICO Children’s code [19], which states that transparency and age-appropriate application are essential for the privacy and safety of children, the dangerous permissions in the sample of apps typically provided explicit occasions for user consent. However, since it is not easy to

understand the implications of accepting a dangerous permission for parents [31] and children [1], it may not be natural to assume that this is an acceptable form of consent.

5.3 Tracking Behaviours in Children’s Apps

It is acknowledged that some apps, especially those from independent developers or startups, need income to remain free of charge. Thus, it is understandable from this perspective why an app would contain some form of tracker to provide a way of monetisation. Still, it is unclear why an app for children aimed at 12 years old and under would need such a variety of advertising trackers embedded, with many ads not relevant to children of this age range (e.g., stair lift and holiday booking). Also, if their sole purpose is monetisation, it is unclear why developers would purposefully implement trackers into their apps that feature eye-catching redirect buttons (e.g., colourful and flashing). This is because this can hold implications for children’s safety in that they may end up accessing something that is not age appropriate, conflicting with the ICO Children’s code [19].

Analytics tracking was the most common type of tracking found in the apps analysed (Section 4.2). This form of tracking involves collecting data on user behaviour, such as how often they use the app, which features they use, and how long they spend doing certain activities. This aims to provide developers objective feedback to improve app functionality and user experience [25]. However, analytics also raise significant privacy concerns when it comes to children’s apps. Although this data is often anonymous, it can be used to create detailed profiles without the children’s or their parents’ explicit knowledge or consent.

The ICO Children’s code states that “profiling” should only be in place to protect a child from any harmful effects, which, in the apps in our sample, seems very unlikely to be the case. As seen in Section 5.3, the tracker Amplitude, identified as in use by the majority of the apps in our sample, conducts such a type of tracking behaviour. Similarly, the Google tracker that engages in “fingerprinting” (DoubleClick) was identified in 5 of the apps: *slither.io*, *Fluvsies – A Fluff to Luv*, *Cake maker: Kids cooking games*, *Fluvsies Merge Party*, and *Baby Panda’s School Bus*. Fingerprinting is comparable to profiling in that it involves the collection of user-specific data, but instead includes device information which, when combined, can identify a particular device and its user [2]. This is of particular interest as it can be a much more invasive type of tracking which can persist across different apps and websites and is much more difficult to block or control.

5.4 Limitations and Future Work

A limitation of the methodology followed for this study is scalability. Despite the use of tools for recovering permissions and trackers for the selected apps, the goal of determining whether the dangerous permissions used were justified, as reflected in the traffic light comparison of apps, required manual analysis. Further automation would allow for the investigation of a larger number of apps for children.

There was a degree of subjectivity involved in the categorisation of the apps provided in Table 1. Their main functionalities were used to determine the most appropriate category. However, this process does not completely eliminate the possibility that an app could belong to multiple categories, which would affect the presented cross-category comparisons in the paper.

As shown in Table 2, not all trackers engage in advertisement; some do not engage in it at all (e.g., MixPanel) while others engage in multiple types of tracking including advertisement (e.g., Google). This raises questions about the business model adopted by free apps without advertisement trackers as a way of monetisation. Further research to map the business model of apps [7] for children would be an interesting possibility for future work. Also, this study revealed the use of advertisements inappropriate for children’s apps, such as colourful and attention grabbing ads. This is non-compliant with the ICO Children’s code [19] and, therefore, calls for a deeper analysis.

Figure 2 and Table 2 show mismatches between number of trackers uncovered by static and dynamic analysis. This lack of consistency may happen, e.g., because some tracking libraries are not present in the apps codebase or would reveal themselves only under certain circumstances or due to code obfuscation techniques [12]. We intend to study this aspect further by analysing trackers using tools claiming to be resilient to code obfuscation, such as AGRIGENTO [6].

While this study has focused primarily on dangerous permissions, future research could investigate the role and impact of other permission types, such as signature and custom permissions. Signature permissions are granted during app installation and require both the requesting app and the accessed entity to be signed with the same digital certificate. Custom permissions, on the other hand, may pose greater risks due to their variable nature. Since developers define custom permissions individually, their exact purposes are often unclear, which could make them more susceptible to misuse.

6 Conclusion

This study has examined the privacy and safety implications of 27 popular and free Android apps designed for children up to 12. Overall, this study has revealed that concerns about the privacy and safety of children using technology are not completely unwarranted. It has also delved beyond identifying the permissions and trackers associated with those apps to determine if they are essential and justified. The traffic light system used to assess these apps comparatively has highlighted that only a single app achieved a green rating overall, raising serious questions about the industry’s approach to child safety.

References

1. 5Rights Foundation: Disrupted Childhood: The Cost of Persuasive Design. https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights_DisruptedChildhood_G.pdf (2023), accessed: 28/08/2024

2. Almond, S.: Our response to Google’s policy change on fingerprinting. <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/12/our-response-to-google-s-policy-change-on-fingerprinting/> (2024), accessed: 23/01/2025
3. Binns, R., Lyngs, U., Van Kleek, M., et al.: Third Party Tracking in the Mobile Ecosystem. In: Proc. of the 10th ACM Conference on Web Science. pp. 23–31 (2018). <https://doi.org/10.1145/3201064.3201089>
4. Blackwell, C., Lauricella, A., Wartella, E.: Factors influencing digital technology use in early childhood education. *Computers & Education* **77**, 82–90 (2014). <https://doi.org/10.1016/j.compedu.2014.04.013>
5. Calciati, P., Gorla, A., Kuznetsov, K., et al.: Automatically Granted Permissions in Android Apps: An Empirical Study on their Prevalence and on the Potential Threats for Privacy. In: Proc. of the 17th International Conference on Mining Software Repositories. pp. 114–124 (2020). <https://doi.org/10.1145/3379597.3387469>
6. Continella, A., Fratantonio, Y., Lindorfer, M., et al.: Obfuscation-resilient privacy leak detection for mobile apps through differential analysis. In: Proc. of the NDSS Symposium 2017. pp. 1–15 (2017). <https://doi.org/10.14722/ndss.2017.23465>
7. Cristofaro, M.: E-business Evolution: An Analysis of Mobile Applications’ Business Models. *Technology Analysis & Strategic Management* **32**(1), 88–103 (2020). <https://doi.org/10.1080/09537325.2019.1634804>
8. Ekambaranathan, A., Zhao, J., Van Kleek, M.: “Money makes the world go around”: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives. In: Proc. of the 2021 CHI Conference on Human Factors in Computing Systems. pp. 1–15 (2021). <https://doi.org/10.1145/3411764.3445599>
9. European Union: General Data Protection Regulation (GDPR). <https://gdpr-info.eu/art-8-gdpr/> (2016), accessed: 16/08/2024
10. Feal, A., Calciati, P., Vallina-Rodriguez, N., et al.: Angel or Devil? A Privacy Study of Mobile Parental Control Apps. In: Proc. on Privacy Enhancing Technologies Symposium. pp. 314–335 (2020). <https://doi.org/10.2478/popets-2020-0029>
11. Felt, A.P., Chin, E., Hanna, S., et al.: Android Permissions Demystified. In: Proc. of the 18th ACM conference on Compute and communications security. pp. 627–638 (2011). <https://doi.org/10.1145/2046707.2046779>
12. Glanz, L., Müller, P., Baumgärtner, L., et al.: Hidden in Plain Sight: Obfuscated Strings Threatening Your Privacy. In: Proc. of the 15th ACM Asia Conference on Computer and Communications Security. pp. 694–707 (2020). <https://doi.org/10.1145/3320269.3384745>
13. Google, A.D.: Permissions on Android. <https://developer.android.com/guide/topics/permissions/overview> (no date), accessed: 28/06/2024
14. Google, Android Developers: Manifest.permissions. <https://developer.android.com/reference/android/Manifest.permission> (no date), accessed: 30/06/2024
15. Hallett, E.: I was asked for naked photos after making ‘friends’ on roblox. <https://www.bbc.co.uk/news/uk-england-gloucestershire-68616730> (2024), accessed: 20/06/2024
16. Hedderson, M., Bekelman, T., Li, M., et al.: Trends in Screen Time Use Among Children During the COVID-19 Pandemic. *JAMA Network Open* **6**(2), 1–12 (2023). <https://doi.org/10.1001/jamanetworkopen.2022.56157>
17. Hirsh-Pasek, K., Zosh, J.M., Golinkoff, R.M., et al.: Putting Education in “Educational” Apps: Lessons from the Science of Learning. *Psychological Science in the Public Interest* **16**(1), 3–34 (2015). <https://doi.org/10.1177/1529100615569721>
18. Information Commissioner’s Office: Audits. <https://ico.org.uk/for-organisations/advice-and-services/audits/> (no date), accessed: 26/03/2025

19. Information Commissioner's Office: Introduction to the Children's code. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/> (no date), accessed: 22/06/2024
20. Information Commissioner's Office: What are PECR? <https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/what-are-pecr/> (no date), accessed: 24/06/2024
21. Kollnig, K., Binns, R., Dewitte, P., et al.: A *Fait Accompli*? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. In: Proc. of the 17th Symposium on Usable Privacy and Security. pp. 181–195. USENIX Association (2021), <https://www.usenix.org/system/files/soups2021-kollnig.pdf>
22. Kollnig, K., Shadbolt, N.: TrackerControl: Transparency and Choice around App Tracking. *The Journal of Open Source Software* **7**(75), 1–4 (2022). <https://doi.org/10.21105/joss.04270>
23. Le, A., Varmarken, J., Langhoff, S., et al.: AntMonitor: A System for Monitoring from Mobile Devices. In: Proc. of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsharing of Big (Internet) Data. pp. 15–20 (2015). <https://doi.org/10.1145/2787394.2787396>
24. Livingstone, S., Stoilova, M., Nandagiri, R.: Children's data and privacy online: Growing up in a digital age. An evidence review. (2019), https://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf
25. Mor-Samuels, E.: Everything you need to know about mobile app analytics. <https://www.appsflyer.com/blog/measurement-analytics/everything-you-need-to-know-about-mobile-app-analytics/> (2024), accessed: 20/01/2025
26. OFCOM: Children and Parents: Media Use and Attitudes Reports. <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/children-media-use-and-attitudes-2024/childrens-media-literacy-report-2024.pdf> (2024), accessed: 19/08/2024
27. Reyes, I., Wijesekera, P., Reardon, J., et al.: "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. In: Proc. on Privacy Enhancing Technologies Symposium. pp. 63–83 (2018). <https://doi.org/10.1515/popets-2018-0021>
28. UK Government: Data Protection Act (DPA). <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (2018), accessed: 20/08/2024
29. UK Parliament: The Privacy and Electronic Communications (EC Directive) Regulations. <https://www.legislation.gov.uk/uksi/2003/2426/contents> (2003), accessed: 20/08/2024
30. UK Parliament: Online Safety Act. <https://www.legislation.gov.uk/ukpga/2023/50> (2023), accessed: 16/08/2024
31. Utz, C., Degeling, M., Fahl, S., et al.: (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: Proc. of the 2019 ACM SIGSAC Conference on Computer and Communications Security. pp. 973–990 (2019). <https://doi.org/10.1145/3319535.3354212>
32. Westin, A.F.: Privacy and Freedom. Atheneum, NY (1967)
33. Winter, E., Costello, A., O'Brien, M., Hickey, G.: Teachers' Use of Technology and the Impact of Covid-19. *Irish Educational Studies* **40**(2), 235–246 (2021). <https://doi.org/10.1080/03323315.2021.1916559>