Poster: An Analysis of Privacy Features in ‘Expert-Approved’ Kids’ Apps

Anirudh Ekambaranathan
University of Oxford
Oxford, United Kingdom
anirudh.ekam@cs.ox.ac.uk

Jun Zhao
University of Oxford
Oxford, United Kingdom
jun.zhao@cs.ox.ac.uk

Max Van Kleek
University of Oxford
Oxford, United Kingdom
max.van.kleek@cs.ox.ac.uk

ABSTRACT

During the course of the past decade, children have become avid consumers of digital media through mobile devices. The industry for children’s mobile applications is booming and marketplaces offer categories of apps aimed specifically at children. In this study, we perform a mixed-methods privacy analysis of 137 ‘expert-approved’ children’s apps from the Google Play Store. Our findings show that these apps do not sufficiently support children to exercise their privacy rights, whilst simultaneously making use of libraries and data trackers which may collect and share sensitive user data.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**.

KEYWORDS

privacy, children’s apps, data tracking, dark patterns

ACM Reference Format:
Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2022. Poster: An Analysis of Privacy Features in ‘Expert-Approved’ Kids’ Apps. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS ’22), November 7–11, 2022, Los Angeles, CA, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3548606.3563549

1 INTRODUCTION

Many of children’s activities have shifted from the physical domain to the digital domain, with young children having become a major consumers of information through mobile devices, such as smartphones and tablets. The accelerated pace at which children are shifting their time and attention to digital devices, has facilitated the creation of a market for mobile apps specifically aimed at children, which today has become a thriving industry [4, 12, 13]. Marketplaces, such as Google Play and Apple’s App Store, have categories of apps specifically aimed at young children, covering genres such as education, action, simulation, and health.

While the use of digital devices and mobile apps are known to be associated with a range of mental and physical health risks [6, 7, 9], more recently they have been under scrutiny due to their large scale and systematic practice of collecting and sharing sensitive personal data [3, 10]. Loss of privacy through engaging in the mobile ecosystem is unavoidable nowadays, primarily due the the presence of data trackers through third-party libraries and advertising modules embedded in apps [3]. Privacy concerns in technological systems have become more widespread and apparent within communities engaging in discussions of technology ethics, such as HCI and Law, as well as regulatory bodies which intend to enforce practices aimed to protect consumers’ data. For example, the EU saw the introduction of the General Data Protection Regulation (GDPR) in 2018, and the Information Commissioner’s Office (ICO) in the UK enforced the Age Appropriate Design Code [1] forcing products and services aimed at children to treat data protection as a core element of their design.

However, despite these regulatory interventions, the current mobile ecosystem for children remains unchallenged and finds itself in a dire state of privacy [3]. While research has been done investigating matters related to privacy risks in mobile apps [2, 11], we have identified two major gaps in the literature. Firstly, most past research focuses on evaluating technical and quantitative features of apps, such as the number of permissions [2] and methods of inter-app privacy leakage. Secondly, almost all studies are aimed at apps intended to be used by adults, particularly mobile health apps and contact tracing apps due to the COVID-19 pandemic. There is a critical gap in the existing research literature addressing how children’s privacy rights are *supported* in children’s apps, focusing on qualitative features taking a human-centric approach. To address this gap, we aim to answer the following research questions:

1. What design features are present in mobile apps for children for them to support their privacy?
2. What are the data tracking and data sharing practices of apps specifically aimed at children?

To answer these questions, we make use of a bipartite mixed-methods approach performing a holistic evaluation of privacy features in children’s apps. We analysed a total of 137 ‘expert-approved’ apps for children from the Google Play Store, as they allegedly enjoy higher levels of protections [14]. Our findings show that apps rarely communicate privacy information to children in an understandable way, while profusely making use of data trackers and analytics libraries. Our work demonstrates an increased need for tighter rules, regulations, and review processes around publishing children’s apps, with a greater focus on privacy rather than content.

2 METHODS

2.1 Scope and app selection

For this study, we focused specifically on ‘expert-approved’ apps from the Google Play Store [14]. As explained by Google, these apps

---

CCS ’22, November 7–11, 2022, Los Angeles, CA, USA

ACM ISBN 978-1-4503-9450-5/22/11.
https://doi.org/10.1145/3548606.3563549

have been approved by teachers and children's education and media specialists to ensure they are 'age appropriate' and 'thoughtfully designed'. We selected these apps as they are promoted to enjoy improved protection and may therefore seem more safe for children to use. There are no exact indications on the website as to how these apps are assessed.

We used a custom web scraper to create an initial dataset of 1038 expert-approved apps. We sorted the apps by popularity according to the number of reviews they have. To ensure a diversity of apps, we made sure that there were no duplicate developers and studios, and that we had at least one app from each genre. We also limited ourselves to free apps and apps which clearly had an age indication. We were left with a total of 470 apps, of which we selected the top 150 apps for analysis. During our analysis we encountered issues with 13 of the apps, because they were not in English, were premium, or presented other technical issues (installation, crashing, etc.).

2.2 Feature analysis

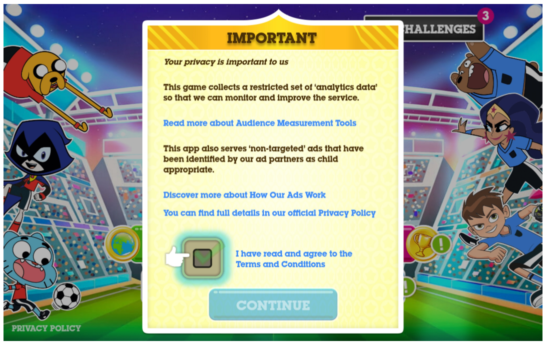
For the first part, we used a grounded approach to perform a qualitative feature analysis [5, 15]. After installing each app on our device, we opened it an explored all available features within it. We recorded all the features in spreadsheet by tracking the apps column-wise and the features row-wise. We created a new row for each feature which we had not encountered before. After an initial round of feature extraction and coding, we performed an iterative round of coding to provide more details about how the features were presented. For example, we distinguished where in the app privacy policies were presented and whether they were protected by an age gate. While the focus of the paper is towards privacy and data protection features, we also collected features which technically may inform privacy aspects, including features related to advertising and in-app purchases.

Through the coding process we inductively created a list of all features related to privacy and data protection present in children's app. We identified a total of 81 features within 137 apps, including 737 instances where these features were available within the app.

2.3 Technical set up

For our analysis we used the Huawei Mediapad M5, with 4GB RAM, 32GB storage, and running the Android 9.0 operating system. We initialsed the device using a child account, creating a female persona of 10 years old. We needed to verify the child account through a parent account using a credit card. Using a child account we were faced with several limitations. For instance, we did not have access to the developer settings, and needed approval from the parent account before installing certain apps.

We also installed the TC Slim app [1], which can dynamically identify trackers [8]. We then individually installed each app and performed our analysis. Upon opening the app, we first explored and collected all design features, and then used the app for another 5 - 10 minutes to ensure all the trackers were registered.



Your privacy is important to us

This game collects a restricted set of 'analytics data' so that we can monitor and improve the service.

Read more about Audience Measurement Tools

This app also serves 'non-targeted' ads that have been identified by our ad partners as child appropriate.

Discover more about How Our Ads Work

You can find full details in our official Privacy Policy

☐ I have read and agree to the Terms and Conditions

Figure 1: Children being nudged into accepting the terms and conditions, and privacy policy.

3 PRELIMINARY RESULTS

3.1 Privacy features

Through our feature analysis and coding process, we uncovered 7 high level themes: *permissions*, *social*, *privacy policies*, *privacy settings*, *parental controls*, *age assurance*, and *ads, cross promotions, and in-app purchases.*

Permissions. 24 apps requested for various permissions during or at startup. 10 out of those had a custom dialog box explaining why a specific permission is needed, out of which 2 linked to a clickable external privacy policy, and 1 linked to a non-clickable privacy policy. Permissions and their associated dialog boxes were not age protected and did not require parental supervision.

Social. 13 apps contained links to social media accounts, such as Facebook or Instagram, with 5 of these apps being age protected. 15 apps allowed for data to be shared through email or other communication tools, of which 4 were age protected. 5 apps tried to automatically sign the user in into their Google Play account, which was prevented because we were making use of a child account. 2 apps had a function which allowed users to optionally sign in using Google Play.

Privacy policies. 59 apps had a link to their privacy policy within the app. For 16 of these these, the privacy policy was available within the app itself. 31 privacy policies were protected by an age gate, often because it opened a link in the browser and left the app. Privacy policies were available in various parts of the app and was sometimes even hidden away in the settings page. In 12 apps, the privacy policy was available on the home screen, in 35 apps it was available in the settings page, and in 11 apps it was available in the About or Information sections. Only a total 7 apps presented their privacy policies in bite sized bits in a way that is suitable for children. 9 apps showed a privacy dialog at startup, and 11 apps required users to explicitly agree to the privacy policy or the terms and conditions, of which 3 nudged their users into accepting these terms. An example of this can be found in Figure 1.

Privacy settings. 40 apps had no settings section at all and 74 apps had a settings page without any privacy settings. 32 of these settings pages were age protected. Features related to data management were related to the app content, such as 'delete all your progress', rather than referring to any user privacy settings, such as deleting the accounts on the the servers. Only 1 app presented the

---

[1] https://play.google.com/store/apps/details?id=net.kollnig.missioncontrol.play

option to disable 'sending anonymous usage statistics to improve the service', however this option was enabled by default as well as protected by an age gate.

Parental controls. 6 apps required parental supervision during setup, two of which required verification through the Google Play parent account. 18 apps had an age protected specific parent section (similar to the settings page), which often linked to other apps, allowing users to rate the app and leave reviews.

Age assurance. Apps used a total of 13 different methods for age assurance. The most popular ones being: asking for the year of birth (12 apps), multiple choice maths question (11 apps), typing in or selecting the numbers which were written out textually (11 apps), and a (non-multiple choice) maths calculation (10 apps). Seemingly, the most difficult method to bypass, used by 1 app, required the parent to enter both the age and date of birth, where the app would calculate whether the age matched the date of birth.

Ads, cross promotions, and in-app purchases. 11 apps showed advertising popups to 'remove ads', which if clicked would trigger an in-app purchase. 46 apps provided a link to other apps by the same developers, of which only 24 were age protected. 28 apps actively cross promoted their apps, for example through nudges. 36 apps presented a link to the app store rating, of which 17 were age protected. 6 of these apps nudged the users into giving a rating. All in-app purchase attempts (47 apps) were age protected through Google and actively prevented because we made use of a child account. 36 of these apps used their own age gate to prevent the children from making in-app purchases. 2 apps warned that parents' supervision should be sought, but did not actively prevent children in any other way. 22 apps nudged users into buying their premium versions and 3 apps had an ad offering their premium version on startup.

3.2 Data tracking

Only 30 out of all apps did not contain any trackers. We identified a total of 43 unique tracker libraries used in the 137 apps we analysed. Figure 2 shows the distribution of most commonly occurring libraries which engage in tracking practices, including *advertising*, *analytics*, *fingerprinting*, and other *social* functions. We omit libraries which focus on providing content functionality, such as Google Firebase or AWS. Google SDKs, such as Google Analytics, Crashlytics, and Google Ads are the most commonly occurring tracking libraries (30.8%). Surprisingly, a large proportion of the apps (12.8%) also had Facebook integrations, while Facebook is specifically aimed at children above 13. Apart from Google SDKs, apps also made use of other attribution and analytics providers, such as Adjust (2.6%), Optimizely (2.6%), Mixpanel (5.1%), and Moat (5.1%).

Looking more specifically at the privacy policies, we found that 15 of these libraries have specific configurations for when they are to be used for children's apps. For example, Adjust and Appsflyer state in their documentation that their SDKs need to be specially configured so that the advertising ID is not transmitted. It is currently unclear whether apps complied with this.

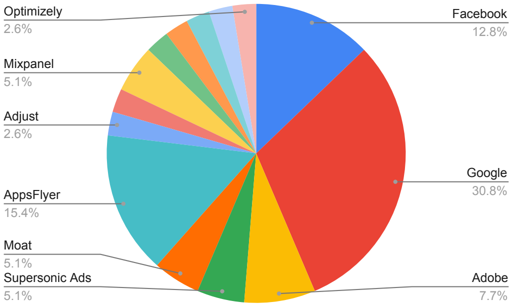


Figure 2: Distribution of most commonly occurring trackers in children's apps.

4 CONCLUSION

Through a bipartite mixed-methods approach, we analysed 137 'expert-approved' children's apps. We uncovered that these apps do not have features to support children to exercise their privacy rights, despite widespread use of tracker and analytics libraries.

REFERENCES

[1] 2020. Age appropriate design: a code of practice for online services. https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf
[2] Vincent Ang and Lwin Khin Shar. 2021. COVID-19 One Year on–Security and Privacy Review of Contact Tracing Mobile Apps. *IEEE Pervasive Computing* 20, 4 (2021), 61–70.
[3] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third party tracking in the mobile ecosystem. In *Proceedings of the 10th ACM Conference on Web Science*. ACM, 23–31.
[4] Great Britain. 2018. *Children and parents: Media use and attitudes report 2018*. Ofcom.
[5] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.
[6] Jon D Elhai, Robert D Dvorak, Jason C Levine, and Brian J Hall. 2017. Problematic smartphone use: A conceptual overview and systematic review of relations with anxiety and depression psychopathology. *Journal of affective disorders* 207 (2017), 251–259.
[7] Beeban Kidron, Alexandra Evans, Jenny Afia, Joanna R Adler, Henrietta Bowden-Jones, Liam Hackett, Anisha Juj, Andrew K Przybylski, Angharad Rudkin, and Young Scot. 2018. Disrupted childhood: the cost of persuasive design. (2018).
[8] Konrad Kollnig, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. 2021. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. 181–196. https://www.usenix.org/conference/soups2021/presentation/kollnig
[9] Hyuk Lee, Min Jae Seo, and Tae Young Choi. 2016. The effect of home-based daily journal writing in Korean adolescents with smartphone addiction. *Journal of Korean medical science* 31, 5 (2016), 764–769.
[10] Jialiu Lin. 2013. *Understanding and capturing people's mobile app privacy preferences*. Technical Report. CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE.
[11] Minxing Liu, Haoyu Wang, Yao Guo, and Jason Hong. 2016. Identifying and analyzing the privacy of apps for kids. In *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications*. 105–110.
[12] Sonia Livingstone, Julia Davidson, Joanne Bryce, Saqba Batool, Ciaran Haughton, and Anulekha Nandi. 2017. Children's online activities, risks and safety: a literature review by the UKCCIS evidence group. (2017).
[13] Ofcom. 2018. Children and Parents: Media Use and Attitudes.
[14] Google Play. 2022. Expert approved apps. https://play.google.com/intl/en-GB_ALL/console/about/programs/teacherapproved.
[15] Pamela Wisniewski, Arup Kumar Ghosh, Heng Xu, Mary Beth Rosson, and John M Carroll. 2017. Parental Control vs. Teen Self-Regulation: Is there a middle ground for mobile online safety?. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. ACM, 51–69.