KOALA Hero: Inform Children of Privacy Risks of Mobile Apps

Jun Zhao
jun.zhao@cs.ox.ac.uk
Department of Computer Science.
University of Oxford
Oxford, UK

Blanche Duron
blanche.duron@cs.ox.ac.uk
Department of Computer Science.
University of Oxford
Oxford, UK

Ge Wang
ge.wang@cs.ox.ac.uk
Department of Computer Science.
University of Oxford
Oxford, UK

ABSTRACT

Children's online activities are routinely tracked, aggregated, and exploited by online services, to manipulate children's online behaviour or monetise. This contributes to the so-called *datafied childhood.* Unfortunately, such datafication remains largely invisible behind the services and is practically impossible to avoid. Existing approaches largely focus on direct online harms, and provide limited support to raise children's awareness or understanding of how their data may be processed, transmitted across platforms, and used to affect their best interests. Through co-design workshops, we identified key barriers for children and families to cope with this type of data privacy risk. Our contribution is that instead of regarding children as passive users and needing protection, we draw on critical digital literacy theories and design a KOALA Hero app, which is aimed to enhance children's cognitive, situated and critical thinking of datafication and online data privacy risks. KOALA Hero represents our first step towards facilitating children's understanding of the invisible data privacy risks. We hope future empirical evaluations will further inform us regarding how our design approaches may affect the thinking process and behaviours of children and families.

CCS CONCEPTS

• **Human-centered computing → Empirical studies in HCI**; **HCI design and evaluation methods**.

KEYWORDS

Children online privacy; children online safety; parental controls; mobile apps

ACM Reference Format:
Jun Zhao, Blanche Duron, and Ge Wang. 2022. KOALA Hero: Inform Children of Privacy Risks of Mobile Apps. In *Interaction Design and Children (IDC '22), June 27–30, 2022, Braga, Portugal.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3501712.3535278

1 INTRODUCTION

Today, children are spending an unprecedented amount of time online. The latest report shows that in the UK, 96% of children aged 5-15 are online, and more than half of ten-year-olds have their own smartphones or tablets [30]. While the Internet provides great new opportunities for children to learn, have fun, and grow, there have been increased concerns regarding children's exposure to excessive screen time [29, 37, 38], cyber-bullying, or inappropriate/harmful content [23, 33, 43]. Despite that several recent legislation frameworks have been established as a direct response to the need for safeguarding children's online well-being [1–3, 5, 6], the rate of compliance is still low. Parents are still expected to take the primary responsibility to safeguard their children's online safety and privacy. As a result, we have seen the emergence of a plethora of a new genre of apps, known as *parental control apps*, designed to support parents to control over their children's online activities and protect them from online harms [41].

However, this reliance on parental control apps has raised many questions about their efficacy. Research has revealed that the monitoring or surveillance-based approach commonly found in the current parental control apps not only reduces the potential effectiveness of such an approach but also may inadvertently damage parents' and children's mutual trust, introduce new harms or take away valuable opportunities for digital environments for children [15, 39, 40]. Furthermore, these approaches largely focus on direct online harms, such as cyber-bullying or inappropriate content, and provide little support for children to comprehend risks related to online data privacy and associated datafication harms.

Data privacy harms refers to the infringement of children's personal data as well as their online actions, such as searches, communications or content consumption. As children's data and actions are being pervasively recorded, tracked, aggregated, analysed, and exploited by online services, to manipulate children's online behaviour, engagement, or content consumption [25, 27, 44], this contributes to the so-called *datafied childhood.*

At the core of this datafication is online services' ability to make *algorithmic impact/harms* on children, analysing their data, supported by algorithms, with the aim to evaluate certain personal aspects relating to a natural person [24], in particular, to predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements [4]. Such datafication is practically impossible to avoid or undo through deletion [24]. Furthermore, such activities take place mostly invisibly behind the scenes of apps and services and are less well understood or discussed as risks than other kinds of more easily characterised harms, such as the collection or disclosure of particular kinds of sensitive data. Given that most adults have little understanding of how their own data are being collected, processed, and used to shape their digital environments [13], it is not surprising that children too, lack a robust understanding or adequate mental models of how their data are processed or used [20, 43].

IDC '22, June 27–30, 2022, Braga, Portugal

ACM ISBN 978-1-4503-9197-9/22/06.
https://doi.org/10.1145/3501712.3535278

The KOALA Hero app is specifically designed to support children and families to gain more understanding about these *implicit data privacy* risks online, particularly those associated with the use of mobile apps. KOALA Hero is built on empirical studies with families (interviews and co-design workshops) and theories related to children's knowledge development [12] and critical digital literacy development [17]. Its core objective is to present data privacy risks related to the use of mobile apps in an easy-to-understand format, with the support of stories and analogies. KOALA Hero represents the first step of our effort towards improving children's understanding and coping skill development in relation to data privacy risks and contributes to an empirically and theoretically-led exploration.

2 RELATED WORK

Livingstone et al. [26] categorised the main online risks that children are subject to under *content (child as receiver), contact (child as participant) and conduct (child as actor)* risks. Similarly, the UK Online Safety Bill [6] identified the scope of online harms as explicit harms (e.g. harassment and cyberstalking), harms with a less clear definition (e.g. cyberbullying and trolling), and underage exposure (e.g. inappropriate material). These harms become an even more critical issue when it comes to children's use of mobile devices, which enable children to have instant access to the internet [28, 36], and make it impossible for parents to keep track of children's online activities [34].

In addition to these increased harms, one often overlooked risk for children today is the omnipresence of data trackers associated with apps used by children every day [9, 18, 19]. A substantial amount of sensitive data about children [10, 22, 35] including location information can be collected through this practice and sent to data brokers for data profiling. This type of data privacy risk is widely identified in apps often used by children [9, 18] for the generation of targeted advertisements and monetisation [7, 14, 21]. However, unfortunately, avoiding these risks is practically impossible at the moment [24], despite several recent regulation movements.

In response to these growing concerns expressed relating to data privacy, researchers have looked into how we may better support them in gaining a better understanding or awareness of such practices. Kumar et al. [20] found that children between the ages of 8 and 11 started to understand that data collection on online platforms could create some risks for them, but tended to associate such risks mainly with 'stranger-danger'. Zhao et al. [43] found through focus group studies with UK children aged 6-10, that while they could identify and articulate certain privacy risks well, they had less awareness of other risks, such as online tracking or personalised promotions. These findings were compatible with findings from a study in 2017 [32], in which teenagers aged 14 to 18 were found to have more concerns over interpersonal contexts, but often less understanding of potential threats to their privacy from ways first and third parties might make use of their data, and how personal data could be used in predictive ways to shape their future experiences and behaviours.

While children would likely have difficulties in fully understanding the complexities of datafication or its means, some recent research has shown that children were well-equipped and capable of grasping essential concepts related to datafication, such as that their personal data (such as activity history) could be processed and used to sell products to users such as themselves, if they were given sufficient scaffolding and nudges from parents and educators, and their understanding grows with experience [24]. However, research with over 200 children aged 8-12 with the goal of developing critical data literacy also showed that repeated exposure to a phenomenon, in this case online data privacy practices, did not produce knowledge [31]. Instead, children needed support and guidance from adults and educators to develop critical data literacy, as such literacy did not tend to simply develop from time spent online [16].

3 DESIGN PROCESS

The design of KOALA Hero has undergone two critical stages: a scoping stage and a co-design stage. At the scoping stage, we conducted semi-structured interviews with 12 parents-and-children pairs [42] to identify barriers for parents and children to cope with online privacy risks. We then followed up with a systematic review of current parental control apps available on the Google PlayStore [39] to identify gaps in the current technological support. This review identified families' needs for better support for understanding online privacy risks, enhancing children's risk coping skills development, and facilitating parents' and children's communications about online safety and privacy.

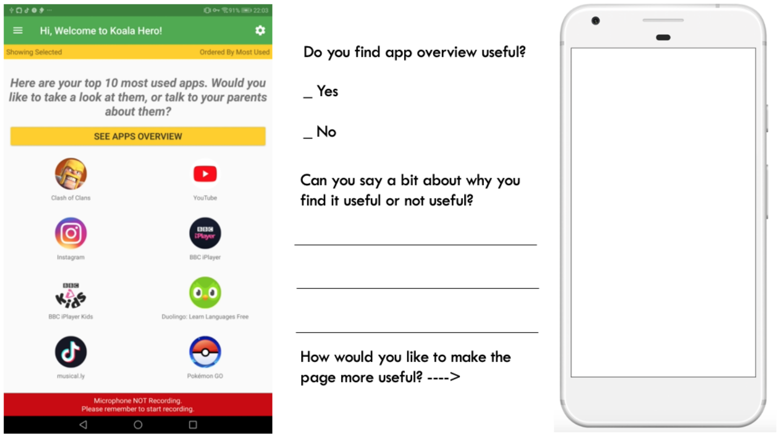
The findings from our scoping research were used to create our first prototype and as inputs to the co-design phase, to explore what kind of information children would find useful for informing them of online data privacy risks, and what kind of design features would provide better support for scaffolding children's understanding.

3.1 The Co-Design Workshop Process

The workshop contained four parts: 1) a short introduction to our existing research findings, followed by a quick discussion about what families thought about their current practice of safeguarding their children's online activities; 2) completing tasks using our app prototype; 3) designing new features for key interactions; and 4) closing discussions. The workshop was designed to last for approximately 1 hour. Both parents and children were involved, so we could observe how children may develop their understanding of risks with or without the support of their parents.

During the task completion phase, each parent-and-child pair was asked to work together to choose five apps that their children were already using on their mobile devices, and then review these apps using the KOALA Hero app prototype. Each family was given a sheet to record the apps they chose and markdown whether they thought the app was good for the children or not. Once this was completed, each family was asked to pick two apps that *surprised* them the most and shared these with the other families by explaining why they were surprised and why they thought it was bad/good for their child.

During the design phase, each family was given three design cards, each of which shows a key user interface of the KOALA Hero app prototype. An example of such a design card is shown in Figure 1. The families were asked to comment whether parts of the app design were/weren't helpful for them and then propose how they might want to make them better.



Hi, Welcome to Koala Hero!

Showing Selected — Ordered By Most Used

Here are your top 10 most used apps. Would you like to take a look at them, or talk to your parents about them?

SEE APPS OVERVIEW

Microphone NOT Recording.
Please remember to start recording.

Do you find app overview useful?

_ Yes

_ No

Can you say a bit about why you find it useful or not useful?

How would you like to make the page more useful? ---->

Figure 1: Make a better koala hero: An example design card.

In the last part of the workshop, we invited families to share with everyone whether they ever had to remove any apps from their children’s devices and why, so that we could learn more about any barriers that we may have missed using the design techniques. We also invited the families to share what they enjoyed the most and the least in the workshop on the day.

3.2 Design artefact

Figure 2 shows the three key user interaction activities that can be supported by the KOALA Hero app prototype that was used in the co-design workshop:

- An overview of the 10 most used apps over the last week: each of which can be then selected and inspected more closely. The pane also has a search box for the users to look up apps that were not yet installed on their devices.
- Expert reviews about an app: highlighting important direct harms possibly associated with the app, such as age-appropriateness, in-app advertisement, exposure to drugs or violence etc.
- Data privacy information about an app: showing where a user’s data may have been sent to and by which tracker companies.

3.3 Results and Findings

In total, we had five families who joined the study in three co-design workshops. The participants are summarised in Table 1. All children were between 6 and 10 years old, and they were accompanied by at least one parent. The study received research ethics approval from the ethics committee of our university.

Audio recordings were collected, transcribed and then qualitatively analysed using a grounded, thematic approach [11]. Overall, the participants appreciated the expert reviews and data privacy information about the apps. They also expressed that they need more support to establish trust in the information or to make use of this information. Because the sample size was small, we were unable to identify any age-specific differences amongst the participant children or parents.

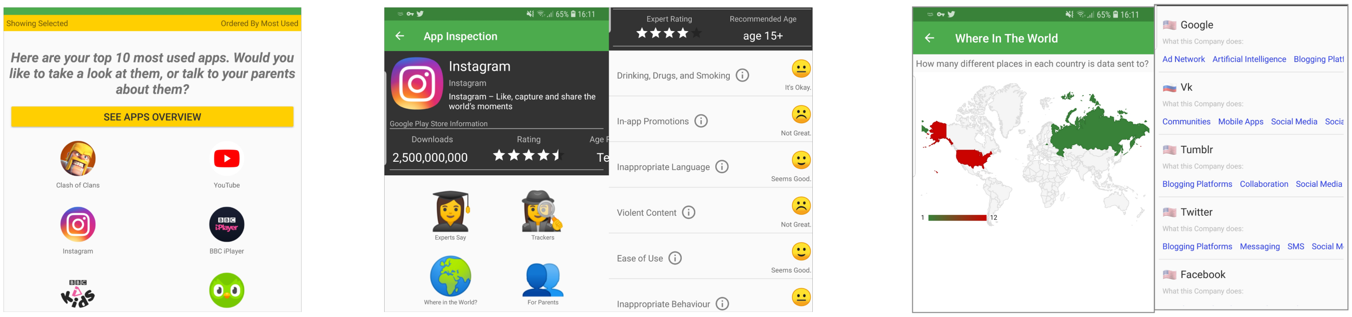
Parents	Children
P1 (Mum)	10-yo boy and 7-yo girl
P2 (Dad)	7-yo boy
P3 (Dad)	10-yo girl
P4 (Mum)	6-yo boy
P5 (Mum)	8-yo girl

Table 1: Summary of participants to the co-design workshops.

3.3.1 *Need for more justification of the risk reviews.*

Parents in the study did not seem to have any specific resources they felt they could draw on for guiding their choice of mobile apps for their children. They normally would search around for ‘good’ apps or follow their children’s requests. As such, all parents found the ‘expert review’ information (Figure 2 (b)) that we aggregated from CommonSenseMedia could potentially be useful. For example, one parent commented that she found the information was comprehensive and was being presented in a way that was easy to read and gain a quick overview of the apps. However, the key issue raised by all participants was regarding the trustworthiness of the information.

Both children and parents found that they could not always agree with the reviews given by the CommonSenseMedia. For example, one parent mentioned that she could not understand why ‘Pokemon Go’ was rated for children aged 13+. She thought this was just a fun game with lots of cartoon characters having some battling together. The feeling was strengthened by her child’s own experience with the game and her shared disagreement with the rating. Furthermore, families found it hard to make sense of the expert ratings when they were not provided with justification about how the ratings were generated. Participants also questioned the validity of these reviews being possibly supplied by families from a different country.



Here are your top 10 most used apps. Would you like to take a look at them, or talk to your parents about them?

How many different places in each country is data sent to?

(a) The overview pane

(b) The expert app reviews

(c) The data privacy risks

Figure 2: The first prototype of KOALA Hero app.

3.3.2 *Need for more actionable information.*

Families had varied opinions regarding the importance of the data privacy risk information (see Figure 2 (c)) for helping them to choose mobile apps for their children. Two families found it very useful to know about the data privacy information behind the apps. The other three families felt that such information was good to know; however, one parent believed that it should be down to institutions to regulate these behaviours. Another parent felt that although it was not ideal for the apps to send information to third parties, this information largely wouldn't reveal their children's exact online identity. Therefore, they would value the educational benefit of these apps over the risks of losing their children's data.

Families expressed that this information might only be truly useful if they could see corresponding options to manage the tracking behaviour of the apps, for example, stopping the tracking of particular companies or stopping sending data to particular countries.

3.3.3 *Child-led risk mediation v.s Parental mediation.*

Four out of the five parents did not regard child-led risk management as the preferred approach. Only one parent emphasised that a child must learn by themselves and expressed a preference for any risk alerts to be sent directly to the child. This indicated that a parent-led risk mediation approach could still dominate parents of children of this age group.

We also observed that parents did not find it entirely comfortable to make use of the information given in the app prototype to talk and discuss risks with their children. Although participants had been given a 3-minute short video, introducing them to how the app works, parents struggled to make sense of some of the information in the app or keep children engaged in the discussions. When parents were not able to find the information they needed, they found no mechanisms to gain help.

4 CRITICAL DIGITAL LITERACY AND THE NEW KOALA HERO

The results from the co-design workshops identified some key design directions to make the information in KOALA Hero more actionable and comprehensible. They also indicated children's knowledge gaps in data privacy, which could hinder the effectiveness of any support for informing children and families of data privacy risks.

We took these design feedback on board and drew on the theories of critical digital literacy in our next design cycle. Kafai et al [17] proposed that computational thinking should include three key frames: *cognitive thinking*, which focuses on the understanding of key computational concepts, practices, and perspectives and the associated skill building and competencies; *situated thinking* encourages learning to take place in contexts that the learner cares about so that they include their personal expression and social engagement in their pathway of learning; and finally *critical computational thinking* emphasises the importance of supporting the questioning of larger structures and processes behind the computational phenomenon.

Existing online safety supports largely focus on supporting children's cognitive understandings but provide little support for situating their understandings in contents that are personal to them, or encouraging their critical questioning of the observable phenomenons. Thus, the KOALA Hero app aims to incorporate critical digital literacy theories to provide more effective support for families and children's privacy risk coping. This is reflected by the following design principles:

- Increase support for *cognitive* understanding of risks: by adding introductory information about data tracking risks using stories and analogies. Data tracking associated with their apps is now represented as different types of 'cookie monsters' (e.g. social, advertising, or essential), making risks more tangible and visual. The educational videos can be accessed at the launch of the app or at any time through the 'learning tap' (see Figure 3 (a)), explaining how cookie monsters could help online services to manipulate children's online experiences, share evil messages amongst each other and exacerbate the harms. This also provides further justification that is needed about why data tracking risks can affect children's online data privacy and how these risks were detected by researchers.
- Encourage *situated* thinking: by designing KOALA Hero as an app that children can install on their own Android devices and explore the data privacy risks they are currently

experiencing during their use of devices. Furthermore, drawing some existing privacy label designs [8], on the overview page, KOALA Hero highlights the risk factors (on the top right corner of each app) associated with each of the user's favourite and most used apps (see Fig 3 (b)), creating a situation that is more likely to be relevant for the users, and encourages users to explore apps associated with higher risk factors.

- Finally, we support *critical* thinking by allowing users to practice exercising their self-autonomy. After having been provided with more information about privacy risks, children are now provided with the 'block' buttons (see Fig 3(c)) to block the implicit data collection by certain companies. This is a function that children can explore together with their parents, by discussing the data collection by a particular company or the necessity of certain data collection and the possibly associated harms. Furthermore, we are setting up associated data analytic coding projects using Jupyter Python Notebook (https://jupyter.org), enabling older children to quantify the implications of data risks at a large scale and enhancing their ability to question the structure and process involved in the violation of their data rights and make more informed decisions.

KOALA Hero is built on top of Tracker Control (TC) [18, 19], to provide the tracker detection and block functions. KOALA Hero is designed for children aged from 7 years above. It can be used by children themselves or together with parents or guardians[1].

5 CONCLUSIONS AND FUTURE WORK

In this paper, we introduce KOALA Hero – an Android App that is guided by multiple empirical studies and critical digital literacy theories. The key contribution of this app is to take a first step toward supporting children's understanding of data privacy risks through a multitude of design features, to facilitate children's cognitive, situated and critical thinking about data privacy.

There are still many features to be added or completed before this app can be made available for public users. We are currently planning an assessment study to understand how the different design features of the app may affect users' perceptions and behaviours towards data tracking risks. We are particularly interested to find out whether the app may stimulate more conversations at home about data privacy risks and additional risk-based considerations when making choices of app usage for children and parents.

REFERENCES

[1] 2020. Age appropriate design code. 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] 2020. General comment No. 25 (2021) on children's rights in relation to the digital environment. https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

[3] 2020. Guidance for Regulation of Artificial Intelligence Applications. https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf

[4] 2020. What is automated individual decision-making and profiling? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/

[5] 2021. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206

[6] 2022. Online Safety Bill. https://bills.parliament.uk/bills/3137

[7] Alessandro Acquisti, Curtis Taylor, and Liad Wagman. 2016. The economics of privacy. *Journal of Economic Literature* 54, 2 (2016), 442–92.

[8] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. 2015. Your location has been shared 5,398 times! A field study on mobile app privacy nudging. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*. 787–796.

[9] 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.

[10] Theodore Book, Adam Pridgen, and Dan S Wallach. 2013. Longitudinal analysis of android ad library permissions. *arXiv preprint arXiv:1303.0857* (2013).

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[12] Jerome Bruner. 1984. Vygotsky's zone of proximal development: The hidden agenda. *New directions for child development* (1984).

[13] Moritz Büchi, Eduard Fosch-Villaronga, Christoph Lutz, Aurelia Tamò-Larrieux, and Shruthi Velidi. 2021. Making sense of algorithmic profiling: user perceptions on Facebook. *Information, Communication & Society* (2021), 1–17.

[14] Interactive Advertising Bureau. 2015. IAB Internet Advertising Revenue Report: 2015 Full Year Results.

[15] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J LaViola Jr, and Pamela J Wisniewski. 2018. Safety vs. surveillance: what children have to say about mobile apps for parental control. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–14.

[16] Engin Isin and Evelyn Ruppert. 2020. *Being digital citizens.* Rowman & Littlefield Publishers.

[17] Yasmin Kafai, Chris Proctor, and Debora Lui. 2020. From theory bias to theory dialogue: embracing cognitive, situated, and critical framings of computational thinking in K-12 CS education. *ACM Inroads* 11, 1 (2020), 44–53.

[18] Konrad Kollnig, Reuben Binns, Max Van Kleek, Ulrik Lyngs, Jun Zhao, Claudine Tinsman, and Nigel Shadbolt. 2021. Before and after GDPR: Tracking in Mobile Apps. 10, 4 (2021). https://doi.org/10.14763/2021.4.1611

[19] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2022. Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps. *Proceedings on Privacy Enhancing Technologies* (2022).

[20] Priya Kumar, Shalmali Milind naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2018. No Telling Passcodes Out Because They're Private?: Understanding Children's Mental Models of Privacy and Security Online. In *Proceedings of ACM Human-Computer Interaction (CSCW '18 Online First)*. ACM.

[21] Ilias Leontiadis, Christos Efstratiou, Marco Picone, and Cecilia Mascolo. 2012. Don't kill my ads!: balancing privacy in an ad-supported mobile application market. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications*. ACM, 2.

[22] Jialiu Lin. 2013. *Understanding and capturing people's mobile app privacy preferences.* Technical Report. CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE.

[23] Sonia Livingstone, Julia Davidson, Dr Joanne Bryce, Ciaran Haughton, and Anulekha Nandi. 2017. Children's online activities, risks and safety.

[24] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. 2019. Children's data and privacy online. *Technology* 58, 2 (2019), 157–65.

[25] Giovanna Mascheroni. 2020. Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology* 68, 6 (2020), 798–813.

[26] Giovanna Mascheroni, Sonia Livingstone, and Elisabeth Staksrud. 2015. Developing a framework for researching children's online risks and opportunities in Europe. (12 2015).

[27] Ulises A Mejias and Nick Couldry. 2019. Datafication. *Internet Policy Review* 8, 4 (2019).

[28] Stefanie Mollborn and Paula Fomby. 2020. Making Sense of Kids' Technology Use. (2020).

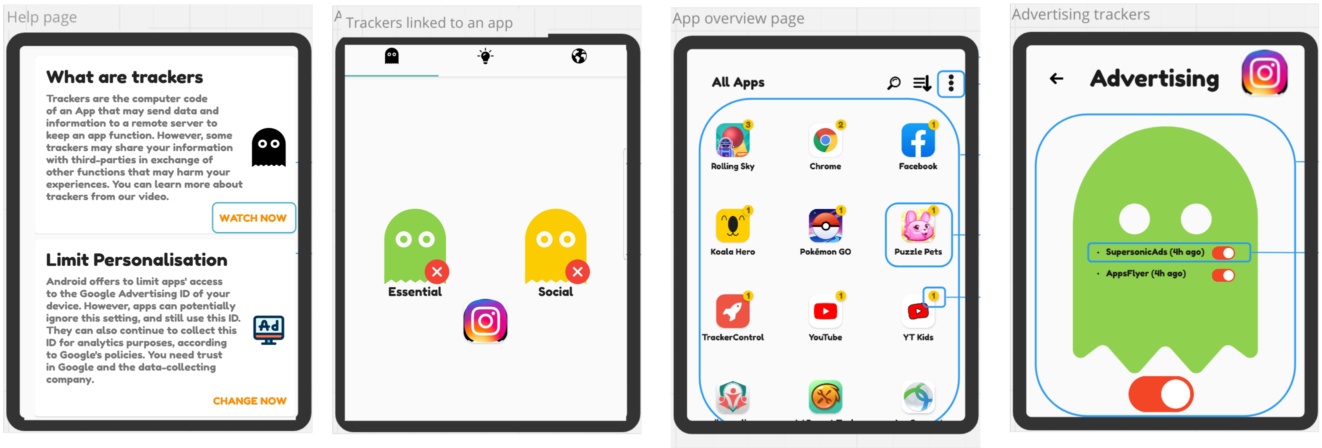
[29] Ofcom. 2019. Why children spend time online. https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2019/why-children-spend-time-online

[30] Ofcom.org. [n.d.]. Ofcom Children's Media Lives: Life in Lockdown. https://www.ofcom.org.uk/__data/assets/pdf_file/0024/200976/cml-life-in-lockdown-report.pdf

[31] Luci Pangrazio and Lourdes Cardozo-Gaibisso. 2021. "Your Data Can Go to Anyone": The Challenges of Developing Critical Data Literacies in Children. In *Critical digital literacies: Boundary-crossing practices*. Brill, 35–51.

[32] Luci Pangrazio and Neil Selwyn. 2017. 'My Data, My Bad...' Young People's Personal Data Understandings and (Counter) Practices. In *Proceedings of the 8th International Conference on Social Media & Society*. 1–5.

[1] KOALA Hero is not yet available in any public play store until we completed the next evaluation phase.



What are trackers

Trackers are the computer code of an App that may send data and information to a remote server to keep an app function. However, some trackers may share your information with third-parties in exchange of other functions that may harm your experiences. You can learn more about trackers from our video.

WATCH NOW

Limit Personalisation

Android offers to limit apps' access to the Google Advertising ID of your device. However, apps can potentially ignore this setting, and still use this ID. They can also continue to collect this ID for analytics purposes, according to Google's policies. You need trust in Google and the data-collecting company.

CHANGE NOW

(a) Learn more about trackers

(c) An overview of risks

(d) Exercise autonomy by the block button

Figure 3: The updated KOALA Hero app with enhanced support for risk understanding and control.

[33] Anthony T Pinter, Pamela J Wisniewski, Heng Xu, Mary Beth Rosson, and Jack M Caroll. 2017. Adolescent online safety: Moving beyond formative evaluations to designing solutions for the future. In *Proceedings of the 2017 Conference on Interaction Design and Children*. 352–357.

[34] Pew Research. 2020. Parenting Children in the Age of Screens. https://www.pewresearch.org/internet/2020/07/28/parenting-children-in-the-age-of-screens/

[35] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83.

[36] David Smahel, Hana MacHackova, Giovanna Mascheroni, Lenka Dedkova, Elisabeth Staksrud, Kjartan Olafsson, Sonia Livingstone, and Uwe Hasebrink. 2020. EU Kids Online 2020: Survey results from 19 countries. (2020).

[37] Unicef. 2020. Rethinking screen-time in the time of COVID-19. https://www.unicef.org/globalinsight/stories/rethinking-screen-time-time-covid-19

[38] Ge Wang, Jun Zhao, and Nigel Shadbolt. 2019. What concerns do Chinese parents have about their children's digital adoption and how to better support them? *arXiv preprint arXiv:1906.11123* (2019).

[39] 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, CSCW (2021), 1–26.

[40] 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*. 51–69.

[41] Bieke Zaman and Marije Nouwen. 2016. Parental controls: advice for parents, researchers and industry. *EU Kids Online* (2016).

[42] Jun Zhao. 2018. *Are Children Well-Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?* Technical Report. https://arxiv.org/abs/1809.10944

[43] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[44] Shoshana Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.