App Snap: A Versatile Tool for Engaging Children and Young People in Dialogue About Smartphone App Privacy

Sophia Walsh
University of Bristol

Kopo M. Ramokapane
University of Bristol

Abstract

While children are active smartphone users, studies suggest they often lack the ability to make informed privacy choices about smartphone applications. Consequently, there is a growing body of literature aiming to understand how children perceive and practice privacy on smartphone devices. However, methods to engage children, either for raising awareness or understanding their practices, are limited. In this paper, we present initial reflections on the engagement tool *App Snap,* which we created to engage children around smartphone app privacy. Initial feedback shows promise, and researchers are already using the game as part of their data collection efforts.

1 Introduction

A recent report on Children's Media Use and Attitudes by the UK communications watchdog Ofcom revealed that 59% of UK children aged 8-11 own a smartphone, with this figure increasing to 95% for ages 12-15 [11]. Smartphone use among these age groups revolves around the use of downloadable applications (apps). Children navigate their smartphone device platforms, installing and uninstalling apps of their choice, often without parental guidance. However, there is a common belief that children are too young to fully comprehend privacy risks or make informed decisions about what data they should protect or share online [12]. Consequently, there have been numerous efforts (e.g., [20]) to understand children's privacy and safety on smartphones.

An important step in understanding children's attitudes and understanding of smartphone and app privacy is engaging them in open and unstructured conversation. However, engaging children on these issues can be challenging. For example, some children may be reluctant to discuss their privacy practices or what they do on their phones, making it difficult for researchers to gather data on how children understand privacy concepts and risks. There is an urgent need to develop innovative methods to engage children and effectively raise privacy awareness. Involving young people in conversations about smartphone app privacy can help us understand their capabilities and knowledge around data collection and practices or if they can recognise risk, or what available privacy mechanisms they use to inform their choices. Also, by engaging children directly, we can know how to better support them and develop effective tools that can minimise risk and challenges they face.

In this paper, we present our initial reflections and experiences with a new engagement tool designed to support privacy research and raise awareness among children and young people. Our tool is based on smartphone privacy labels and is designed for all smartphone users including children and adults. We have trialed this activity informally with young people, adults, and families, and found it to be very effective in engaging different user groups in conversations about smartphone app privacy. Moreover, the majority of the people who engaged with our tool were surprised to learn about privacy labels and appreciated knowing that they can see what data apps collect and process from their devices.

2 Background

2.1 Smartphone App Use and Young People

Despite children's increased online presence, there is often an assumption that they possess the technical knowledge necessary to navigate the digital world and manage their security and privacy. However, prior research [12, 15] has shown that they lack the skills needed to navigate online interactions safely. They may inadvertently disclose information that could put them at risk of physical harm or expose them to

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

inappropriate content. Furthermore, their engagement data can be exploited for commercial gains.

There have been efforts to understand children's perception of privacy and how to empower them to be safe online. Livingstone et al. [10] reviewed literature on children's privacy and classified it into three broad categories: interpersonal, institutional, and commercial privacy. They argued that commercial privacy, how personal data is harvested and used for business and marketing purposes, is the area children are least able to comprehend and manage on their own. Moreover, Wang et al. [17] interviewed 48 UK-based children aged 7-13 to examine how they perceive commercial privacy. They found that there were key gaps in children's knowledge about how data was transmitted across platforms, who was involved in data processing, and about data ownership. Their research calls for transparent and autonomy-supportive tools to better support children. Kumar et al. [7] explored ways in which US-based children aged 5 to 11 can be helped to manage their privacy and security online. They also argued that children require better scaffolding to support their learning on privacy and security, proposing resources to prompt engagement for learning within families.

2.2 Engaging Children and Young People

In terms of engaging children in research, various methods have been employed to study how children understand and perceive privacy in different settings. Common methods include interviews (both in-person and online) [17], focus groups [16], and surveys [1]. Participatory and co-design methods [2,8] involve children directly in the research process, enabling them to share their perspectives and help design privacy tools or educational materials. While these methods offer a broad understanding of children's privacy needs and behaviors, some lack context or rely on self-reporting, which can affect results. Moreover, some educational games intended for children often have complex rules or require internet access, which can create cognitive and logistical barriers to effective engagement [19]. Kumar et al. [9] argue that most literature around children and privacy lacks children participation.

Other researchers (e.g., [3]) have utilised offline data cards to engage children. These data cards were used to facilitate discussion on the process of sharing and selling of personal data by online technology companies. They illustrate how offline resources can help visualize and contextualize online data collection practices. We aim to further bridge a gap with a method that is engaging, minimizes reliance on children recalling information and reduces the need for online access.

2.3 Privacy Notices

Complying to privacy regulations (e.g., GDPR) relies on notice and choice to inform and get consent from users. This notice can be provided through various forms, such as privacy policies, privacy labels, and cookie notices. However, this notice-and-choice paradigm presents significant challenges for children. Research indicates that children often struggle to comprehend privacy notices due to their complexity and length. Their developmental stages limit their understanding of data collection and consent implications, making them more susceptible to persuasive design techniques [14]. In response, regulations like the Children's Online Privacy Protection Act (COPPA) [1] and specific GDPR provisions provide additional safeguards for children's data, including parental consent requirements. To better protect and empower children regarding their privacy, it is crucial to develop age-appropriate, engaging, and easy-to-understand activities that help them make informed privacy decisions.

The concept of privacy nutrition labels was first introduced in 2009 by Kelley et al. [4] with the aim of improving the presentation and comprehensibility of privacy policies. Apple and Google adopted this approach for apps used on their smartphones in 2021 and 2022 respectively. In general, the aim of privacy labels is to offer app users concise information about the data practices of app owners or developers, thereby improving the visual presentation and understandability of their privacy policies. They serve as a mechanism to help reduce information asymmetry that usually exists between service providers and users. In terms of smartphone ecosystems, privacy labels are presented to users as part of the app description. Privacy label assumption is that the user will check them before deciding whether they want to install an app or not. Initial studies (e.g., [4]) reported that users found them more useful than privacy policies. However, recent studies present conflicting conclusions, e.g., [18], [6], [5]. Despite these issues, privacy labels offer an opportunity to raise awareness about data collection and use by service providers. Our game specifically aims to empower children regarding privacy labels, teaching children how to use them and make informed decisions around whether to or not install an app.

3 New Engagement Method: App Snap

3.1 Concept

To encourage and facilitate conversations about data privacy and explore the diverse experiences of smartphone users regarding app privacy in the wild, we designed a tabletop game centred around privacy labels: *App Snap*. Our objective was to create an engaging activity that not only promotes open, unstructured discussions about app data collection and usage but also raises awareness among smartphone users. Moreover, we aimed to develop a valuable tool for researchers engaging in app privacy studies.

The activity consists of a set of cards: half of the cards depict smartphone apps and the other half feature their cor-

[1] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

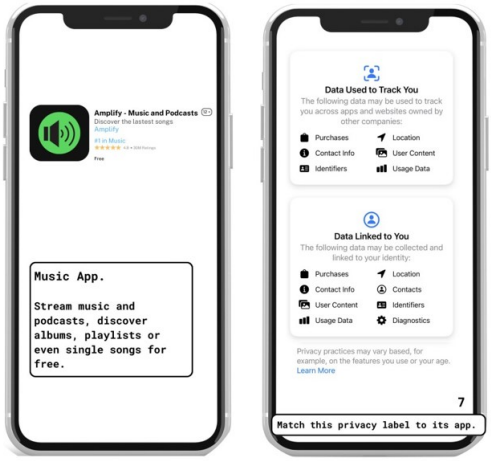

Figure 1: Examples of Apple App Card and Privacy Nutritional Label Card.

responding privacy labels. Each of the app cards represents a fictional app that resembles a popular app, with a description of the purpose of the app. The label cards, or Privacy Nutrition/Data Safety labels, contains the data types that the respective app collects. These privacy labels resemble the actual labels published for the mirrored apps. Figure 1 shows an example of a fictional app with its label. For each fictional app, there is an app description so that participants can reflect on the app's purpose and the data types they think or expect the app to collect and process to offer its service.

The main idea is for participants to match apps with their respective privacy labels. While the goal is to accurately match the app with its privacy label, the primary purpose is for participants to explain or discuss their choices. Participants can engage with the game/activity as individuals, pairs, or groups. The game requires a facilitator, this is an individual who explains the game and prompts discussions during game play. The facilitator does not need to be privacy expert but someone who is aware of smartphone app privacy labels and their role.

We created cards for Android and iOS operating systems to ensure that users of both can engage in the activity. Currently, the Apple iOS version has 9 cards representing smartphone apps; the Android version has 6 cards. The choice of apps can be modified. This modification can be done by privacy researchers depending on their research goals. Researchers can create their own context-specific cards to meet their research needs.

As part of the game package, we have created a facilitator guide, definition booklets, and step-by-step guidelines on how to find the labels on iOS and Android platforms. The facilitator guide provides information on the game format and components (i.e., cards), how to play the game, and the solutions or correct app and label pairing. The definition booklets provides data types definitions that Apple and Android use to explain their data types. The step-by-step guidelines show participants how to find the privacy labels on their respective smartphones.

3.2 Game Play

At the beginning of the game, participants/players are first introduced to the concept of privacy labels and asked about their knowledge of them. They can then choose to engage with either the Apple iOS or Android version of the game.

The app cards are laid face up on a table, while the corresponding label cards are shuffled and placed next to them in random order. Players are asked to consider the app cards and labels, matching them based on their expectations of the types of data the apps collect. They are given a few moments to think about what the apps represent and what the labels indicate; this may prompt them to refer to the definition booklets to clarify data types or uses.

It often takes multiple attempts to get the correct pairings, as it can be challenging to match them accurately on the first try. Once players believe they have correctly matched all the apps and labels, the facilitator removes the correct pairs and offers the opportunity for additional attempts. There is no limit to the number of attempts. The activity does not need to be fully completed to facilitate discussion or increase awareness.

Step-by-step guidelines on how to find privacy labels can be provided for players to identify the labels on their own phones in the future. This information can be shared at the start or end of the game, depending on the players' interest.

4 Reflections and Observations on *App Snap*

This section will discuss insights and feedback related to our game. App Snap was developed as part of a toolbox (i.e., sets of tools) for engaging marginalised and vulnerable populations. The use of the game to raise awareness is covered under our IRB application number: 2023-14496-15911. As a result, the tool can be used to raise awareness, but not to collect research data. After finalising the design of the game, we will apply to use the game to collect data.

As part of designing and refining the game, we engaged various groups of children and young people in different informal settings, including public awareness-raising events. In general, they found the game interesting and eye-opening. They often expressed different feelings about the actual apps and the privacy labels. A common comment was about why certain apps collected specific types of data. We observe that often people associate long data labels with social media apps and focus on types of data that they would expect to be collected, for example, health and fitness data by fitness apps. Moreover, while we designed this for engaging children and young people, adults engaged and loved it. We also

received positive feedback from researchers, some of whom have requested to use the game in their studies.

4.1 Benefits

Facilitation of Discussions: Without requiring a device or internet access, offline versions of online privacy features help facilitate discussions. This allows users to consider privacy features outside their typical environments, avoiding the habituation that might occur with online versions. In the context of Apple's Privacy Nutrition Label and Google's Data Safety Labels, these offline versions enable broader consideration of the labels' existence and purpose without the cognitive load of additional online information and features.
Simplicity and Accessibility: The tool benefits from these additional features:

- Simple and Easy to Understand: Few rules and a simple design lower cognitive barriers to engagement.
- Relevant: Most people use smartphone apps, making the game highly relevant.
- Portable and Offline: The game can be used in various environments, including schools, social clubs, and prisons, engaging marginalized populations.
- Accessible and Relatable: Suitable for all populations that use smartphone apps.
- Adaptable: The game can be customized for specific contexts, using cards that represent context-specific apps and labels, such as fem-tech apps' privacy labels.
- Ecologically Valid: Based on existing privacy awareness mechanisms, the game facilitates the comparison of different labels for various apps, helping users choose between them.
- Versatile: Can be used in a broad range of settings, from formal research to informal discussions about privacy.

Experimental Utility: Evaluating labels offline helps separate the label from other online distractions and purposes. This can be useful in experimental contexts to explore theoretical models. For example, dual process theories, such as the elaboration likelihood model (ELM) [13], which propose two routes involved in decision-making: central and peripheral.

4.2 Potential Uses

From our initial observations, the game can be used both as a stand-alone tool to assess awareness and understanding of privacy labels, and as part of a mixed-methods approach. We envisage several potential future uses. First, App Snap could be used as a tool to evaluate the usability of privacy labels: understanding what they mean to users, whether users find them useful when deciding which apps to use, what aspects users understand or find confusing, and what they would like to have explained better. Second, it could aid the development of new app-specific labels: by identifying which aspects of current labels are clear and which require further clarification. Co-design approaches could use the game cards as a starting point for new design recommendations. Third, it could be employed as a tool to investigate other privacy topics. It can be adapted to fit different contexts. For example, researchers can select fem-tech apps and their privacy labels when conducting studies on the privacy of female tech applications. This adaptability allows the game to address specific privacy concerns in various fields. Fourth, App Snap could be utilised as part of longitudinal studies: to determine if repeated exposure to privacy labels influences privacy attitudes and behaviors over time, measured through changes in self-report surveys. Fifth, it could be used alongside other research methods: to set the context for anticipatory focus groups, helping to explain how data collection is communicated in current technologies and exploring how users would prefer data processes to be communicated in the future. Finally, App Snap could serve as an icebreaker in workshops: to initiate discussions related to data collection and privacy and the broader data ecosystem.

4.3 Limitations

While our game shows a lot of promise, we have identified several limitations. First, the game is inherently limited as it can only be played once for maximum impact. To enable repeated engagement, additional apps and privacy labels would need to be created. Second, the game is designed for smartphone app users, so participants who do not own or use apps may struggle to participate. Third, the tool is not universally accessible; it relies on visual elements, which exclude users with visual impairments, although they can still engage in the discussions that follow. Finally, while the activity is reusable, scalability can be challenging. Accommodating more participants requires more cards, which may involve printing additional materials.

5 Conclusion

Engaging children in conversations about smartphone privacy is important. To address this, we created a game called *App Snap* to raise awareness and engage children and young people in research on the privacy of smartphone apps. Initial feedback from both children and researchers has been encouraging. We aim to continue improving the game and share it with researchers, particularly those working at the intersection of children and privacy.

6 Acknowledgments

This work was supported in part by EPSRC CDT TIPS-at-Scale EP/S022465/1, REPHRAIN EP/V011189/1 and Equitable Privacy EP/W025361/1.

References

[1] Common Sense Media. The common sense census 2021: Media use by tweens and teens, March 2022. Retrieved from https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021, page 22.

[2] John Dempsey, Gavin Sim, Brendan Cassidy, and Vinh-Thong Ta. Children designing privacy warnings: Informing a set of design guidelines. *International Journal of Child-Computer Interaction*, 31:100446, 2022.

[3] Liz Dowthwaite, Helen Creswick, Virginia Portillo, Jun Zhao, Menisha Patel, Elvira Perez Vallejos, Ansgar Koene, and Marina Jirotka. " it's your private information. it's your life." young people's views of personal data use by online technologies. In *Proceedings of the interaction design and children conference*, pages 121–134, 2020.

[4] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[5] Rishabh Khandelwal, Asmit Nayak, Paul Chung, and Kassem Fawaz. Comparing privacy labels of applications in android and ios. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*, pages 61–73, 2023.

[6] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. Goodbye tracking? impact of ios app tracking transparency and privacy labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, pages 508–520, 2022.

[7] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. 'no telling passcodes out because they're private' understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–21, 2017.

[8] Priya Kumar, Jessica Vitak, Marshini Chetty, Tamara L Clegg, Jonathan Yang, Brenna McNally, and Elizabeth Bonsignore. Co-designing online privacy-related games and stories with children. In *Proceedings of the 17th ACM conference on interaction design and children*, pages 67–79, 2018.

[9] Priya C Kumar, Fiona O'Connell, Lucy Li, Virginia L Byrne, Marshini Chetty, Tamara L Clegg, and Jessica Vitak. Understanding research related to designing for children's privacy and security: A document analysis. In *Proceedings of the 22nd Annual ACM Interaction Design and Children Conference*, pages 335–354, 2023.

[10] Sonia Livingstone, Mariya Stoilova, and Rishita Nandagiri. Children's data and privacy online: growing up in a digital age: an evidence review. 2019.

[11] Ofcom.org.uk. Children and parents media use and attitudes report 2024, 2024.

[12] Information Commissioners Office. Towards a better digital future: Informing the age appropriate design code, 2019. https://ico.org.uk/media/about-the-ico/consultations/2614763/ico-rr-report-0703.pdf.

[13] Richard E Petty and Pablo Briñol. The elaboration likelihood model. *Handbook of theories of social psychology*, 1:224–245, 2011.

[14] Jenny Radesky, Yolanda Linda Reid Chassiakos, Nusheen Ameenuddin, Dipesh Navsaria, et al. Digital advertising to children. *Pediatrics*, 146(1), 2020.

[15] Kate Raynes-Goldie and Matthew Allen. Gaming privacy: A canadian case study of a co-created privacy literacy game for children. 2014.

[16] Mariya Stoilova, Sonia Livingstone, and Rishita Nandagiri. Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, 8(4):197–207, 2020.

[17] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 'don't make assumptions about me!': Understanding children's perception of datafication online. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–24, 2022.

[18] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How usable are ios app privacy labels? *Proceedings on Privacy Enhancing Technologies*, 2022.

[19] Leah Zhang-Kennedy and Sonia Chiasson. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1):1–39, 2021.

[20] Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 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*, pages 1–13, 2019.