

“Money makes the world go around”: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives

Anirudh Ekambaranathan, Jun Zhao, Max Van Kleek



Introduction

Children are spending an increasing amount of time online through mobile devices. Apps used by children often contain data trackers from major vendors, such as Google and Facebook, collecting sensitive data for purposes of advertising, influencing, and analytics.

Why do developers create apps which violate children’s privacy?

Methodology

We conducted 20 semi-structured interviews and 134 surveys with children’s app developers to understand their perceptions and practices of data driven children’s apps. We asked questions such as:

- (1) What do you think privacy risks are for children online and who is responsible for this?
- (2) What are your views on current data collection practices in apps and by third-party companies?
- (3) How do you use third-party libraries and how do you ensure its safety and privacy?

Findings

Below are some of our findings. More details can be found in our the paper.

Data minimisation is not always possible

Developers wish to minimise data collection and sharing. However, they also argue that data collection and analytics are necessary for understanding their users and improving the app. Developers trust prominent vendors (e.g. Google and Unity), due to accessibility and reputation of the brand, while admitting that there may be privacy risks.

“We are typically using libraries from Apple or Google. Rarely do we use something we found on a developer network forum where you could potentially get in trouble. So, the libraries we use are primarily from major parties that have created their own stuff.” (Interview 3)

Developers are not sufficiently supported

Developers feel they bear a moral responsibility to design for children’s best interests. However, they struggle to find children-specific design guidelines and do not feel supported by major data controllers, such as Google, as they do not necessarily prioritise privacy.

Conflicts between monetisation and ethics

Developers need to generate enough revenue to sustain their business, but wish to do this in an age-appropriate way. However, due to market competition, developers are forced to rely data-driven monetisation methods.

“I can find and show you dozens of apps that are clones of our games. Someone took our app, re-skinned it a little, and then left it as it is with all the game design, offered it on Google Play and showed all kinds of ads: safe, unsafe, whatever. So if this continues, essentially it means that users who are looking for free stuff will be able to find whatever they want. It’s not even David vs Goliath, it’s a Flea vs Goliath.” (Interview 8)

Conclusion

Reliance on third-party libraries from known providers, and their lack of transparency in data practices, makes it difficult for developers to understand how to create privacy-friendly apps. They feel that commercial success comes at the cost of children’s best interests. Ethical monetisation might require a redesign of the way app stores currently function and major industry backing.

Ekambaranathan, Anirudh, Jun Zhao, and Max Van Kleek. ““Money makes the world go around”: Identifying Barriers to Better Privacy in Children’s Apps From Developers’ Perspectives.” *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 2021.