Understanding and Supporting App Developers Towards Designing Privacy-Friendly Apps for Children



Anirudh Ekambaranathan
Linacre College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy

Michaelmas 2022

Acknowledgements

Oxford will forever hold a special place in my heart. It was the first place where I truly felt at home and where my aspirations were able to flourish through the countless opportunities it provided.

As part of my DPhil degree, I joined the Centre for Doctoral Training (CDT) programme in Cyber Security. In the first year of the CDT, students generally complete 'mini-projects', which are two month research projects to become acquainted with a research field and a research group, as preparation to deciding what the student will focus on in the coming years. For one of my mini-projects, I was fortunate to work the incredibly kind and compassionate Jun Zhao. Her involvement and dedication to my work sparked within me an immediate realisation that she was someone I wanted to work with throughout the journey of my DPhil. I am deeply indebted to Jun for her invaluable guidance and unwavering support during my DPhil journey. She was an invaluable mentor and supporter, and I owe my successful and wonderful experience at Oxford to her. I can confidently say that without her, my DPhil would not have been the same. For that, I am eternally grateful.

I am also incredibly fortunate to have as my second supervisor Max Van Kleek. His expertise, unwavering dedication, and friendly advice were essential to the success of my research journey. His commitment to excellence and impeccable work ethic inspired me to strive for the highest standards of quality. His insights were invaluable in shaping my understanding of the research and in developing my writing capabilities. I cannot thank him enough for his guidance and support.

I would also like to extend my gratitude to the entire HCAI group that I was a part of. I owe a debt of gratitude to Konrad Kollnig and Ge Wang for the invaluable and inspiring conversations we had over coffee during the early years of my DPhil. I am also ever grateful to Siddhartha Datta for his consistent support and friendship.

I would like to express my gratitude to Ivan Flechais and Ruba Abu-

Salma for their thorough examination of my thesis during the viva. Their valuable feedback and perspectives have been instrumental in shaping my work, and I appreciate their contributions to my research journey.

I would like to extend a special thanks to David Hobbs, who was the administrator of the CDT until its final years. Despite my initial discouragement over the application fee, he encouraged me to apply after reviewing my resume. It is safe to say that without him I may have never applied.

During my time at Linacre College, I was fortunate to be a part of a remarkable group of people whom I feel privileged to have known. I owe my deepest gratitude to these individuals: Varnika Agarwal, Dilhan Manawadu, and Vihanga Munasinghe, who were not just friends, but like family to me. Varnika on many occasions has cooked me the most incredible Indian food, and I especially enjoyed our chats over chai. I am also grateful to her for introducing me to the kind and supportive Saloni Singla, with whom I formed an immediate connection. I am also grateful to Dilhan and Vihanga for their kindness, love, and hospitality. Their unwavering support and friendship have made my time in Oxford truly unforgettable.

I would also like to extend a special thanks to Shuwen Zhou, who I had breakfast with every day during her time in Oxford. I consider Shuwen to be one of my dearest friends.

As part of my CDT, I quickly formed close friendships with a group of people. I would like to thank Freddie Barr-Smith and George Chalhoub for being dependable friends and inspiring a tireless work ethic.

I would like to extend special thanks to Sebastian Köhler and Hanna Schalling who have graciously hosted me for dinner on many occasions. Sebastian has always been an incredibly kind and reliable friend.

I would also like to thank Jack Jackson for the memorable times we shared during the second year of my DPhil, attending various social events and parties at Linacre College and other colleges.

I am deeply grateful to Martin Georgiev not only for being a close friend throughout the long and exciting journey of our DPhil but also for the many wild adventures and challenging monthly projects we embarked on together. Martin has been an invaluable support throughout this time, and I am forever grateful for his unwavering encouragement and friendship.

In my final year at Oxford, I was blessed to cross paths with the remarkable Klaudia Krawiecka. Our friendship was instantaneous and we formed a bond that was truly unbreakable. Despite the short time we were able to spend together, our connection was profound and I regret not having the

chance to get to know her sooner.

I am also grateful for the opportunity to have gotten to know and befriend Janet Sadler, who took over as the administrator of the CDT after David left.

Last but not least, I would like to thank my family for their continued support. I would also like to extend my thanks to my extended family, who always supported me and took pride in me pursuing a doctorate. My parents and sister have always supported me and have always take great enthusiasm in telling their friends and family about the work I do. I am especially grateful that my parents and sister had the opportunity to visit me in Oxford and experience the beauty of the city for themselves. It was a special moment for me to be able to show them around and share my Oxford experience with them. Their presence and support during my time in Oxford made it all the more special and memorable.

Abstract

The integration of digital technology in contemporary society has led to children being exposed to and using mobile devices at younger ages. These devices have become an integral part of their daily routines and experiences, playing a crucial role in their socialisation and development. However, the use of these devices is not without drawbacks. The underlying infrastructure of many of the apps available on such devices heavily relies on a vast and intricate data-driven ecosystem. The proliferation of mobile app developers and numerous third-party and fourth-party entities heavily relies on the collection, sharing, transmission, and analysis of personal data, including that of children. The breach of privacy resulting from the extensive data tracking is prevalent and has detrimental effects on children, including the loss of autonomy and trust.

In this thesis, we investigate this problem from the perspective of app developers. We begin by conducting a critical examination of the privacy landscape of popular children's apps in the UK market. In conjunction with a systematic literature review, we develop a research-driven method for evaluating privacy practices in mobile applications. By applying this methodology to a dataset of 137 'expert-approved' children's apps, we reveal that these apps extensively tracked children's data, while providing insufficient user-facing support for children to manage and negotiate these privacy behaviours.

This finding raises the crucial question of barriers to designing privacy-friendly mobile apps for children. To explore this issue, we first conduct a mixed-method study with developers of children's apps, comprising 134 surveys and 20 interviews. Our findings show that while the developers are invested in the best interests of children, they encounter difficulties in navigating the complex data-driven ecosystem, understanding the behaviour of third-party libraries and trackers, as well as the pressure to monetise their apps through privacy-friendly alternatives.

In light of these findings, we carry out a Research through Design approach to elicit latent needs from children's app developers, using a set of 12 ideas, generated through a workshop with design expert, aimed at addressing the identified challenges. These ideas are evaluated with a sample of 20 children's app developers to uncover a set of latent requirements for support, including a demand for increased transparency regarding third-party libraries and easy-to-adopt compliance checking against regulatory guidelines.

Utilising the requirements gathered from the developers, we develop a web-based application that aims to provide transparency about the privacy behaviours of commonly used SDKs and third-party libraries for app developers. We ask a sample of 12 children's app developers to evaluate how features in our application may incentivise developers to consider privacy-friendly alternatives to commonly used SDKs, how they may plan to use it in their development practices, and how it may be improved in the future.

The research in this thesis casts a crucial new perspective upon the current state of privacy in the mobile ecosystem, through carefully-designed observations and attempts to disrupt existing practices of app developers for children. Through this journey, we contribute to the HCI research community and related designers and regulatory bodies with fresh and original insights into the design and development of privacy-friendly mobile applications for children.

List of Figures

2.1 Livingstone's three dimension's of privacy 25

3.1 Overview of our literature search strategy 67
3.2 Examples of nudging and consent in children's apps 86
3.3 Examples of advertising and consumerism in children's apps . 87
3.4 Distribution of common trackers in children's apps 90
3.5 The Tracker Knowledge Graph 92

5.1 Overview of participant reactions to our RtD study 141
5.2 Multi-stakeholder alignment for privacy-friendly app development 166

6.1 System architecture of `DataAvalanche.io` 187
6.2 Legal features in `DataAvalanche.io` 188
6.3 Meta-data features in `DataAvalanche.io` 191
6.4 SUS survey results 206

List of Tables

2.1 Summary of the AADC standards 30
2.2 Alignment of AADC with leading data protection frameworks 31
2.3 Common systemic breaches of the AADC 37

3.1 Literature review results 68
3.2 Commonly used privacy features for app evaluations 72
3.3 Privacy evaluation based on 'Privacy Policies' 74
3.4 Privacy evaluation based on 'Tracking' 74
3.5 Mapping of literature review to the systemic breaches of the AADC 75
3.6 Mapping of our app analysis to the systemic breaches of the AADC 93

4.1 Participant demographics (Chapter 4) 111

5.1 Participant demographics (Chapter 5) 143
5.2 Speculative design ideas 146
5.3 Overview of participants' reactions 147
5.4 Requirements and challenges 149

6.1 Participant demographics (Chapter 6) 193
6.2 Requirements to improve `DataAvalanche.io` 203

A.1 Codes Organised by Themes 264

B.1 Codes Organised by Themes 288

C.1 Codes Organised by Themes 295

Contents

Acknowledgements **i**

Abstract **iv**

List of Figures **vi**

List of Tables **vii**

1 Introduction **1**
- 1.1 Research Questions 6
- 1.2 Contributions 10
- 1.3 Thesis Outline 13
- 1.4 Dissemination 15

2 Background **16**
- 2.1 Introduction to Digital Childhood 17
  - 2.1.1 Outline 19
- 2.2 Children and Privacy 20
  - 2.2.1 Theories of Privacy 21
  - 2.2.2 Children's Data Protection Frameworks 27
  - 2.2.3 Children and Privacy 38
  - 2.2.4 Summary 40
- 2.3 Data Tracking and Privacy in Mobile Apps 41
  - 2.3.1 Tracking: A Working Definition 42
  - 2.3.2 Tracking on Smartphones 42
  - 2.3.3 Unique Identifiers 44
  - 2.3.4 Tracking Detection 45
  - 2.3.5 Tracking in the Mobile Ecosystem 46
  - 2.3.6 Why Data Tracking and Sharing is so Pervasive 47

2.4 The Attention Economy . . . 48
2.4.1 Persuasive Design . . . 48
2.4.2 Dark Patterns . . . 49
2.4.3 The Role of Data in the Attention Economy . . . 50
2.4.4 Harms Arising from Persuasive Design and Data-Driven Personalisation . . . 50
2.5 Advertising . . . 52
2.5.1 The Relevant Actors . . . 52
2.5.2 Real-Time Bidding (RTB) . . . 54
2.5.3 The Role of Data in Advertising . . . 55
2.5.4 Children and Advertising . . . 56
2.5.5 Harms Arising from Advertising . . . 56
2.6 Discussion . . . 56
2.6.1 Key Findings . . . 56
2.6.2 Revisiting Privacy and Being Privacy-Friendly . . . 59
2.6.3 Research Gaps and Contributions . . . 60

3 App-solutely Exposed: A Privacy Analysis of Children's Apps 62

3.1 Introduction . . . 63
3.2 Literature Review . . . 66
3.2.1 Methods . . . 66
3.2.2 Results . . . 70
3.2.3 Interim Discussion . . . 75
3.3 Privacy Analysis of Children's Apps . . . 78
3.3.1 Overview of the Method . . . 79
3.3.2 User Facing Privacy Features . . . 79
3.3.3 Third-Party Tracker Detection . . . 80
3.3.4 Our App Analysis . . . 81
3.3.5 Fourth-Party Tracker Mapping . . . 83
3.4 Results . . . 84
3.4.1 Privacy Features . . . 84
3.4.2 Third-Party Tracking . . . 89
3.4.3 Fourth-Party Tracking . . . 91
3.4.4 Interim Discussion . . . 93
3.5 Discussion . . . 95
3.5.1 Summary and Key Findings . . . 95
3.5.2 The Complexities of the Data Tracking Ecosystem . . . 96

3.5.3 Challenges in Designing Privacy-Friendly Apps for Children . . . 98
3.5.4 Limitations . . . 100
3.6 Conclusion . . . 101

4 Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives 103
4.1 Introduction . . . 104
4.2 Methods . . . 106
4.2.1 Participants . . . 107
4.2.2 Procedures . . . 107
4.2.3 Analysis of Qualitative Data . . . 109
4.2.4 Descriptive Statistics . . . 109
4.3 Results . . . 110
4.3.1 Design for Children's Best Interests . . . 110
4.3.2 Perception of Data Collection Practices . . . 113
4.3.3 The Need for Analytics and Other Third-Party Libraries 114
4.3.4 Challenges in Selecting Third-Party Libraries . . . 115
4.3.5 Challenges in Sustaining a Successful App Business . . . 117
4.3.6 Summary . . . 119
4.4 Discussion . . . 119
4.4.1 The Challenges of Using Third-Party Libraries . . . 120
4.4.2 Monetisation in a Data-Driven Economy . . . 121
4.4.3 Problems in Using Guidelines . . . 122
4.4.4 Working Towards Solutions . . . 123
4.4.5 Limitations . . . 127
4.5 Conclusion . . . 129

5 How Should We Support Designing Privacy-Friendly Apps for Children? Using a Research through Design Process to Understand Developers' Needs and Challenges 131
5.1 Introduction . . . 132
5.2 Research through Design . . . 134
5.3 Methods . . . 135
5.3.1 Ideation Workshop . . . 137
5.3.2 Design Workbook . . . 139
5.3.3 Speed Dating . . . 141
5.3.4 Data Analysis . . . 144

5.4 Interview Results . . . 146
5.4.1 Overview of Participants' Reactions . . . 146
5.4.2 Perceptions of Guideline Support . . . 148
5.4.3 Requirements for Privacy-Friendly Development Libraries 153
5.4.4 Concerns and Needs for Compliance Checking Mechanisms . . . 156
5.4.5 Concerns and Suggestions for Creating Privacy-Friendly Apps through Alternative Funding Mechanisms . . . 160
5.4.6 Challenges for Rewarding Privacy-Friendly Apps . . . 162
5.5 Discussion . . . 165
5.5.1 Summary and Key Findings . . . 165
5.5.2 Addressing the Need for Credibility and Normalisation of Privacy-Friendly App Development . . . 166
5.5.3 Users' Incentives, Behaviours and New Practices . . . 169
5.5.4 Overcoming Systemic and Structural Barriers . . . 170
5.5.5 Limitations and Future Work . . . 172
5.6 Conclusion . . . 173

6 Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps 174
6.1 Introduction . . . 175
6.2 Designing `DataAvalanche.io` . . . 178
6.2.1 Design Consideration . . . 179
6.2.2 Functionality . . . 181
6.2.3 Components and Architecture . . . 185
6.3 Implementation . . . 186
6.3.1 Privacy-Friendly Alternatives . . . 186
6.3.2 Legal Implication . . . 188
6.3.3 Children Specific Configuration . . . 189
6.3.4 Knowledge Graph . . . 189
6.3.5 Back-End Server . . . 190
6.3.6 Front-End . . . 190
6.4 Evaluation . . . 191
6.4.1 Participants and Recruitment . . . 192
6.4.2 Interview Procedure . . . 193
6.4.3 Surveys . . . 195
6.4.4 Data Analysis . . . 195
6.5 Results . . . 196

6.5.1 Alternatives are Good but Not Always Applicable . . . 196
6.5.2 Privacy Implications are Useful for Transparency . . . 198
6.5.3 Data Tracking is Not Surprising . . . 199
6.5.4 Putting `DataAvalanche.io` to Use . . . 201
6.5.5 Additional Requirements . . . 202
6.5.6 Survey Results . . . 205
6.6 Discussion . . . 206
6.6.1 Summary and Key Findings . . . 206
6.6.2 Affecting Developer Practices and Choosing Alternatives 208
6.6.3 Evaluating Privacy Implications Through Increased Transparency . . . 208
6.6.4 Improving `DataAvalanche.io` . . . 209
6.6.5 Limitations . . . 211
6.7 Conclusion . . . 211

7 Conclusion **214**
7.1 Introduction . . . 215
7.2 Review of Research Goals and Findings . . . 216
7.2.1 RQ1: *What privacy features are available in children's apps and can children's apps be considered to be privacy-friendly?* . . . 217
7.2.2 RQ2: *What are the key considerations and current practices of app developers when designing apps for children?* . . . 219
7.2.3 RQ3: *How do app developers want to be supported in designing privacy-friendly apps for children?* . . . 220
7.2.4 RQ4: *Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?* . . . 222
7.2.5 RQ: *What are the key considerations and challenges for developers when designing privacy-friendly children's apps and how can we better support them in this process?* 223
7.3 Contributions . . . 224
7.3.1 A Research Driven Methodology to Evaluating Privacy in Apps . . . 225
7.3.2 An Understanding of What Privacy Looks Like in Children's Apps . . . 225

7.3.3 An Understanding of Why Privacy in Children's Apps is an Uphill Battle . . . 226
7.3.4 Requirements to Support Developers to Improve Privacy in Children's Apps . . . 226
7.3.5 `DataAvalanche.io`: the Development and Evaluation of a tool to Support Developers to Improve Privacy in Children's Apps . . . 227
7.4 Directions for Future Research . . . 227
7.4.1 Development of Multi-Stakeholder Approaches for Building Privacy-Friendly Apps . . . 228
7.4.2 Exploring Socio-Technical Support for Developers . . . 228
7.4.3 Exploring Alternative and Ethical Marketplaces and Platforms . . . 229
7.5 Concluding Remarks . . . 229

A Supplementary Material Chapter 4 **231**
A.1 Interview Guide . . . 231
A.2 Survey Questions . . . 232
A.3 Interview Codes and Themes . . . 264

B Supplementary Material Chapter 5 **267**
B.1 Interview Guide . . . 267
B.2 Design Workbook . . . 268
B.3 Interview Codes and Themes . . . 288

C Supplementary Material Chapter 6 **293**
C.1 Interview Guide . . . 293
C.2 Interview Codes and Themes . . . 295

1 Introduction

Contents

1.1 Research Questions 6

1.2 Contributions 10

1.3 Thesis Outline 13

1.4 Dissemination 15

In early October 2021, whistle-blower Frances Haugen appeared before the United States Senate's Sub-Committee on Consumer Protection, Product Safety, and Data Security. With bold clarity and precision, she delivered an opening statement that confirmed suspicions that many people already held [1]. Her narrative is both compelling and captivating, as she risked an integral aspect of her livelihood by challenging a social media behemoth that — in her own words — had the power to "destroy" her.

Haugen had joined Facebook after one of her friends had been radicalised by it. She was part of the Civic Disinformation team responsible for identifying and preventing the spread of fake information in small and large populations. During her tenure at Facebook, she found that the services offered by the platform often conflicted with the best interests of its users: "Facebook's products harm children ... I saw that Facebook repeatedly encountered con-

flicts between its own profits and our safety. Facebook consistently resolved those conflicts in favour of its own profits" [1]. Before leaving Facebook in May 2021, Haugen had scanned and leaked over 20,000 internal corporate documents. In her testimony, she explained how internal research at Facebook had found that their services, specifically Instagram, created a toxic environment for teenagers, and that despite this knowledge, Facebook had refused to take action.

What Haugen found illustrates the delicate interplay between the ways in which technology creators commercialize their products and services, and the ways in which children experience the digital world. This is a relatively new problem. As digital devices have become smaller and cheaper, digital services have become more abundant and more accessible than ever before, leading to mass adoption of these devices by not only adults, but also by children of all ages. Children have become avid consumers of digital media, primarily through mobile devices such as tablets and smartphones [2]. The way mobile devices interface with the digital world through "apps" (applications) installed from app marketplaces such as the Google Play Store and the Apple App Store, has become a multi-billion dollar industry. With millions of apps available on these platforms, they also offer special categories of apps specifically aimed at children [3, 4]. These categories often have headings such as 'Apps for children' or 'Games for children' and also allow children to filter by age groups ('Ages up to 5' and 'Ages 6-8') [5]. Inevitably, the children's app industry has become a commercially thriving sector.

Many, if not most, of the digital services aimed at children are seemingly free. This is particularly true for the app marketplaces, as the majority of the apps can be freely installed. This raises the question of how it is possible for these apps to be free and how app developers can sustain their business in this manner. At a 2018 congressional hearing, Mark Zuckerberg was asked a similar question: how do you sustain a business model where people do not pay for the product? Zuckerberg answered: "We run ads" [6]. However, this seemingly 'simple' answer has important implications for the privacy rights of consumers. What Zuckerberg did not specify is that it is not just plain advertising that is being used by seemingly free digital services, but rather it is *targeted advertising*, a subtle but important difference. This implies that user data is analysed to serve highly targeted ads with a high likelihood of the user clicking on them. This user data is collected through a variety of means. In the mobile ecosystem, this mostly happens through the use of apps containing first and third-party data trackers [7], which collect and

subsequently share data with advertising networks and data brokerages for purposes of targeted analytics [8, 9], including advertising [10]. It is the primary objective of tech giants such as Google and Facebook to maximise the probability of serving ads that users click on, which happens through ever more sophisticated user profiling and understandings of people, made possible by the data collected about them. Data has become the new currency. Never before have commercial entities collected and shared so much data about people to influence their lives, and this has led to much debate about the role of market leaders and monopolies, specifically those that provide critical services to people's everyday lives.

The position of children in this digital world is yet to be fully understood and developed. The practices of large tech firms are considered problematic by many, as they lead to issues such as "datafication" [11] and the normalisation of a surveillance culture [12]. Children are considered to fall in a special category of consumers who merit increased protection, as their understanding of matters related to data and privacy is not fully developed [13]. In addition, children are spending more and more time alone with their mobile devices, meaning that they often install and open apps for the first time by themselves [14, 15]. This has implications for the way services and products for children should be designed, and poses questions about interactions between children and digital technologies. For example, how do developers and children negotiate consent? While there is clear evidence that children should enjoy special protections, evidence for the existence of such protection is still lacking. The misalignment between the commercial incentives of technology creators and consumers is self-evident. However, this misalignment also exists in practice, as studies show that children's apps in particular still share large volumes of data with third parties [7].

There have been a variety of responses to the concerning developments described above, both through regulatory interventions and academic outputs. For example, the European Union introduced the General Data Protection Regulation (GDPR) in 2018 [16], seeking to give consumers increased control over their personal data. The GDPR also acknowledges that children (those under 18) merit "specific protections" in relation to their data (Recital 38):

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular,

> apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

As a further clarification to this, the Information Commissioner's Office (ICO) in the UK introduced the Age Appropriate Design Code (AADC) for children in early 2020 [17] which provides specific considerations about a child's capacity to act and understand the digital world, and forces developers of online services to consider data protection as a core element of their development. While at the moment, the ICO AADC is the most comprehensive regulatory initiative to address children's privacy in digital products and services in the UK, other regulatory measures exist in other countries as well. For example, the United States has the Children's Online Privacy Protection Act (COPPA), which is aimed at operators who provide services targeted to children under the age of 13. COPPA requires that website and online service providers obtain verifiable parental consent before collecting personal information from children, and also requires them to post privacy policies and to take steps to protect the security of children's personal information.

Academic research in this field can broadly be divided into two types: technical and user studies. Technical studies aim to understand the data collection and sharing practices of apps and services. Research in this area covers a broad spectrum of topics, such as the analysis of data trackers [7, 18], consent [19], compliance with privacy policies [20], and permissions [21]. The various methods and techniques used to analyse the privacy of apps will be examined in greater detail in Chapter 3.

Meanwhile, user studies aim to understand the perceptions and behaviours of various stakeholders. Most of the research that considers users as stakeholders tends to focus on parents [22] and children [23], with the aim of trying to understand their perceptions and attitudes towards privacy and the use of digital devices. While often overlooked, *developers* too are a critical stakeholder in the mobile industry. With the implementation of more stringent regulatory frameworks, such as the GDPR and AADC, there is a growing need for developers to re-evaluate their current design practices when creating apps for children. However, this presents a significant challenge for developers, as developers frequently encounter difficulties in comprehending and applying legal requirements to their designs [24, 25, 26]. The pressing demand for privacy from developers, makes it increasingly more important to

consider their perspectives and challenges. However, research into the considerations and current practices related to creating data-driven applications for children is still in its infancy.

Existing studies that involve developers mostly focus on their understanding and perceptions of privacy practices. For example, studies have looked at how developers view and interpret privacy policies [27] and select ad networks [10, 28]. At the same time, studies do suggest a need for tools for developers [29]. Tools for developers are scarce and are primarily related to technical coding features or the generation of privacy policies [30, 31, 32]. For example, Coconut is an IDE plugin highlighting the use of privacy data types and adds automatic code annotations [32]. However, such tools fail to address some of the larger privacy issues, such as the large scale third-party data tracking. More importantly, research in this area rarely looks at the intersection of developers and *children's apps*. This is surprising, as developers play a key role in today's app marketplaces populated with data-hungry apps for children, and in choosing to integrate targeted advertising, data trackers, and other potentially harmful technologies. What is critically missing, is an understanding of how developers can be supported to meet this growing demand for privacy. To that end, the lack of research into the intersection of developers and children's apps and an understanding of this interaction is leaving a crucial gap for designing more effective and user-friendly technology for children.

This poses several open questions about the role of app developers in the current state of mobile app ecosystem which past research has not addressed yet: Why do developers create privacy-unfriendly apps for children? To what extent are they aware of or understanding the impact of their design choices on children's privacy? How can we help them better support them navigating this complex data infrastructure underlying the mobile ecosystem?

These back-of-the-envelope questions sketch an initial starting point for us to think about investigating this developer-child creator-consumer intersection as a way to understand how the future of mobile app development for children should look like. Such research directions present unique opportunities to draw from interdisciplinary research methods, engaging with both stakeholders and technologies to contribute to a rapidly evolving field. This chapter sets out formally what this looks like in terms of academic research: it begins by formulating the research questions that guide the investigations underpinning this thesis, highlights the core contributions, and outlines what the subsequent chapters cover to make it easier for the reader to navigate.

Positionality

Our primary aim in this thesis is to comprehend how data tracking in apps can be minimised, and we take the position that this practice is harmful. Nevertheless, we would also like to acknowledge the multifaceted nature of the intricate data tracking landscape. We recognise that there are valid arguments in favour of data tracking, including the potential benefits of serving users with relevant advertisements [33], its role in sustaining critical online services [34, 35, 36], and the personalisation of content to enhance user experiences [37]. Additionally, in many cases, the precise nature of the consequences stemming from data tracking may not be immediately evident, and they may not manifest in tangible, physical harm.

We recognise these diverse viewpoints and the complexity of the issue. We firmly assert the importance of safeguarding children's privacy and well-being in the digital age, especially considering their limited understanding and ability to provide informed consent [38, 39]. We discuss the exact harms and dangers associated with data tracking and sharing in depth in Chapter 2. In our approach, we actively seek out and include diverse perspectives from the children's app developers we interview, as well as other data we collect, to avoid a one-sided analysis [40]. We acknowledge the potential for bias in this research, as we approach this investigation with a predetermined view that data tracking in children's apps raises ethical concerns. Our goal is to engage in a rigorous exploration of the challenges faced by developers in creating privacy-friendly children's apps, while considering the diverse perspectives that contribute to this intricate debate.

1.1 Research Questions

In this thesis, we aim to deepen our understanding of the challenges faced by children's app developers in making privacy a key consideration in their development practices, and the potential strategies to support them. Specifically, we will address the following overarching research question:

> *What are the key considerations and challenges for **developers** when designing **privacy-friendly** children's apps and how can we better support them in this process?*

There are several terms — which we have highlighted— in this research question which we need to unpack. Firstly, we realise that the process of

creating apps is complex and can involve multiple actors. The UK ICO broadly refers to this group of actors as 'developers', but acknowledges that this can include "coders, UX designers and system engineers" [17], who are all responsible for upholding children's privacy in their development practices. We adopt a similar terminology in this thesis, and there use the term 'developer' to encapsulate all actors which may be involved in the process of creating an app. Secondly, we make use of the term 'privacy-friendly' to currently refer to upholding standards set out by data protection frameworks developers need to comply with. In Chapter 2, we more closely look at this term, to understand what it means for an app to be considered privacy-friendly, drawing on theories of privacy and through an analysis of existing data protection frameworks.

To systematically answer our overarching research question, we conduct a series of four research studies (Ch. 3 - Ch. 6), drawing from various interdisciplinary methods, such as interviews with developers, analysis of existing apps and developer-facing resources, and a review of relevant literature, to provide a comprehensive understanding of the challenges faced by developers in this area and the potential solutions to support them.

Overview at a Glance

We address this overarching research question through four sub-questions, which we motivate and explain below. Here, we provide a brief overview to orientate the reader.

1. (*RQ1; Ch.3*) We first evaluate the current state of privacy in children's apps. To do this, we draw on existing literature to establish a research-driven method for evaluating and assessing privacy in apps. We apply this method on a set of children's app to gather first-hand data to understand the current privacy landscape of children's apps. We demonstrate a misalignment between extensive privacy breaches in apps and support for children to negotiate these privacy behaviours.

2. (*RQ2; Ch.4*) To explain this disparity, we conduct an in-depth study with a large number of children's app developers to understand their design motivations and barriers to integrating privacy as a core element of their development processes. We find that developers face a series of challenges to privacy-friendly app development.

3. (*RQ3; Ch.5*) Using a *Research through Design* method [41], we identify the latent requirements for supporting developers to make privacy an integral part of their development practices.

4. (*RQ4; Ch.6*) Finally, using these requirements, we design and evaluate a web-based tool for supporting children's app developers to prioritise privacy in their development process.

Unpacking our Research Question

Our starting point to answering our overarching research question is a critical examination of the current privacy landscape of children's apps, with the aim of gathering first hand data to understand how privacy is considered in children's apps. More specifically, in Chapter 3, we address the following sub-research question and its supporting questions:

RQ1 What privacy features are present in children's apps and to what extent can these apps be considered to be privacy-friendly in the UK market?

- 1a How is the privacy of children's apps evaluated in the research community, and how is privacy conceptualised in these evaluations?
- 1b What technical and user facing privacy features are there in children's apps for them to negotiate their privacy preferences?
- 1c What are the open challenges for building privacy-friendly apps for children?

To answer these questions, we first draw on existing literature to understand the various ways privacy is assessed in apps. We use these findings to establish a research-driven method for evaluating privacy in apps that is more holistic. We apply this method on a dataset of 137 'expert-approved' children's apps and find that apps extensively engage in data tracking while providing little support to users for negotiating these privacy behaviours. We therefore wish to better understand why exactly this is case and what motivations children's apps developers have for creating apps that behave in such ways. Specifically, in Chapter 4, we investigate the following sub-research question and its supporting questions:

RQ2 What are the key considerations and current practices of app developers when designing apps for children?

- 2a What do app developers perceive as their responsibilities when designing for children?
- 2b What are the main practices adopted by developers for achieving privacy and how do they align with leading data protection frameworks from different sectors?
- 2c What are key barriers for the adoption of the leading data protections frameworks for app developers and how can these barriers be overcome?

We investigated these questions through 20 interviews and 134 surveys with children's app developers. We found that while developers do care about children's best interests, they faced several challenges which prevented them from making privacy a key consideration in their development practices. Importantly developers struggled with the complexities of the data infrastructure underlying the mobile ecosystem, particularly related to the behaviours of third-party libraries. In addition, developers perceived a trade-off between their need to monetise apps (to sustain the development practices) and to protect children's privacy. They felt that the options to monetise apps are limited to methods relying on data and targeted analytics.

We therefore next turn to examining how to support developers in overcoming these challenges and barriers. Specifically, we wish to identify requirements for concretely supporting them through the design of supportive tools. In Chapter 5, we investigate the following sub-research question and its supporting questions:

RQ3 How do app developers want to be supported in designing privacy-friendly apps for children?

- 3a What specific development tools do app developers require to enhance privacy in children's apps?
- 3b What requirements do app developers foresee for tools to support their development of future privacy-friendly apps for children?
- 3c How do app developers foresee addressing systemic obstacles imposed by major marketplaces in the development of privacy-friendly apps?

To address these questions, we made use of a *Research through Design* method [41]. We proposed designs and ideas for tools which can help in privacy-friendly app development, and evaluated them through 20 interviews with children's app developers. By doing so, were able to formulate requirements for how developers wish to be supported in making privacy a more salient quality in their apps. Not all the requirements we identified translate to technical design features, as developers expressed needs which extended to other stakeholders, such as the need for increased awareness for privacy by end users. However, the technical requirements provide us with important directions for developing support which has the capacity to directly affect developers. Therefore, in Chapter 6, we aim to answer the following sub-research question and its supporting questions:

RQ4 Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?

- 4a How can we empower developers to make informed decisions about the privacy practices of different SDKs and libraries, and to choose alternatives that are more privacy-friendly?
- 4b How do tools and guidance for developers to protect the privacy of their users, including specific configurations and legal considerations, affect their choices in selecting third-party libraries?
- 4c How does providing transparency on the data sharing practices of different SDKs and libraries affect developers' practices in terms of understanding and evaluating privacy risks?

In answering these questions, we develop and evaluate a web-based tool (`dataavalanche.io`) for providing more transparency on commonly used third-party SDKs and libraries. Our evaluation provides insights into how developers wish to be supported, as well as a comprehensive list of additional requirements developers would like to see in our tool to encourage the adoption of privacy-friendly design features in their apps.

1.2 Contributions

This thesis contributes to the understanding of how children's app developers consider privacy in their development practices and how to support them in

making it a key element of their design choices. Specifically, we make the following research contributions:

A research-driven methodology to evaluating privacy in apps. We conducted a systematic literature review to evaluate the current landscape of children's apps and identify commonly used privacy features. Upon aligning the results of our review with the ICO's Age-Appropriate Design Code [42], it became apparent that past research has not sufficiently addressed the user-facing dimension of app privacy. To address this gap, we present a method for evaluating privacy in apps based on a user-facing and technical dimension. The technical dimension of our methodology focuses on understanding the extent of data tracking in apps, while the user-facing dimension aims to understand how well users are supported in negotiating the privacy practices in apps. This methodology is timely and important as it addresses the growing demand for improved privacy from consumers and regulatory bodies. By providing a comprehensive framework for evaluating privacy in apps, our methodology can assist future research in understanding how the landscape of privacy in apps evolves over time.

An understanding of what privacy looks like in children's apps. We applied our two-dimensional (technical and user-facing) app privacy analysis method on a dataset of 137 'expert-approved' children's apps from the Google Play Store. The purpose of this analysis was to understand how well children are supported in understanding and negotiating their privacy within these apps. We found that the majority of these apps lack user-facing features to support children in understanding and managing their privacy, and that this lack of support was accompanied by a high degree of third-party data tracking. To further understand the implications of this lack of control, we also conducted an analysis of the fourth-party tracking ecosystem. By examining the entities with whom third-parties share data, we discovered that once data leaves an end-user's device through third-party tracking, it is sent into a vast network of data-sharing entities. We call this phenomenon *data avalanche*, referring to the uncontrollable large scale data dissemination that happens once data leaves an end-user's device and reaches a third-party.

An understanding of why privacy in children's apps is an uphill battle We conducted 20 in-depth interviews and 134 surveys with children's app developers to gain insight into their development practices, motivations, and barriers to designing privacy-friendly apps. Through this, we found that developers feel a strong moral responsibility to design for children's best interests, but were faced with challenges in translating this need to prac-

tice. Firstly, they felt constrained by market pressures to monetise their apps through targeted advertising and in-app purchases. They explained that marketplaces offer few privacy-friendly methods for monetising apps. Secondly, developers reported difficulty in understanding the data-related practices of third-party libraries and often rely on popular libraries provided by market leaders such as Google and Facebook, despite concerns about the transparency of their data practices. Lastly, they indicated that there are few guidelines out there to help them navigate the complexities of designing privacy-friendly apps for children. Importantly, these findings show the process of creating privacy-friendly apps is not straightforward process. The environment for developing and publishing apps, as created by marketplaces, is optimised towards rewarding those apps which make use of practices such as targeted advertising and in-app purchases. With the increasing pressure that developers face, we have to ensure that they are presented with the appropriate support to both comply with regulatory requirements while navigating marketplace challenges.

Requirements to designing technologies and assistive tooling to support developers in designing privacy-friendly apps for children. In order to understand how we can concretely support developers in overcoming the aforementioned challenges, we employed a *Research through Design* (RtD) [41] approach to identify requirements for tools to support the development of privacy-friendly apps for children. RtD is a co-design methodology that allows researchers to design and discuss ideas which may seem futuristic, disruptive and even technically infeasible to realise [41]. Through an expert-led ideation workshop, we generated 12 speculative designs aimed at supporting developers in this endeavour. We then gathered feedback on these designs through semi-structured interviews with 20 children's app developers, in order to elicit their reactions and gain insight into their latent and specific requirements for privacy-friendly app development. Our research indicates that developers have a dual set of requirements: technical and socio-technical. Technical requirements encompass the need for clarifications of marketplace and legal terms through tools like checklists and other resources. In contrast, socio-technical requirements encompass considerations related to other stakeholders and systemic changes in current market structures. This may include factors such as increasing parental privacy awareness and redefining success metrics within marketplaces.

`DataAvalanche.io`: the development and evaluation of a tool to support developers to improve privacy in children's apps. The

findings from Chapters 4 and 5 suggest a need for increased transparency on the privacy practices of third-party libraries. Therefore, in Chapter 6, we developed and evaluated a web-based tool, `DataAvalanche.io`, which helps to increase transparency on the privacy practices of commonly used third-party SDKs in children's apps. We conducted an evaluation of `DataAvalanche.io` with 12 app developers to understand how it can be improved and how they envision using it in their development practices. Our evaluation reveals how and when developers would consider adopting privacy-friendly alternatives to commonly used SDKs from major data controllers, as well as the type of legal support they require. Our participants also provided suggestions for additional features that would increase the tool's adoption. These findings concretely show us how we can support developers in designing privacy-friendly apps for children. However, they also reveal that our overarching endeavour to foster an environment for developing privacy-friendly children's apps should be attributed to a single stakeholder. Instead, it requires a multi-stakeholder effort, in which each stakeholder is limited by their awareness of privacy, market circumstances, and economic incentives. Our tool, `DataAvalanche.io`, is currently publicly available.

1.3 Thesis Outline

This thesis begins by providing the necessary background information and literature in Chapter 2, to enable the reader to fully understand the subsequent chapters. The background section begins with an overview of data tracking in the mobile ecosystem, including a brief discussion on the workings and relevance of advertising in apps. Additionally, we explore the harms that arise from the loss of privacy and delve specifically into how children understand privacy, as well as how developers incorporate privacy considerations in their development practices. We also briefly examine design patterns in apps, as they form the interface through which children interact and exercise their privacy rights. Lastly, we analyse leading common data protection frameworks from different sectors, in order to understand the expectations placed on developers. We conclude the chapter with a brief summary, highlighting the literature gaps that motivate the remaining chapters.

In Chapter 3, we conduct a systematic literature review to establish a method for evaluating privacy in children's apps. Through this review, we establish a two-dimensional approach for evaluating privacy in children's apps,

consisting of both a technical and user-facing dimension. We then apply this method to a dataset of 137 expert-approved children's apps from the Google Play Store. Our analysis reveals that children's apps commonly lack user-facing features to support children in understanding and negotiating their privacy, and are accompanied by a significant amount of third-party data tracking. We also investigate the extent to which data leaving an end-user's device through third-party tracking is disseminated to a vast network of data sharing entities, which we term 'data avalanche'. These findings provide insight into the poor privacy practices currently embedded in children's apps and highlight the need for further research in this area.

In Chapter 4, we conduct an in-depth study of children's app developers through surveys and interviews to gain a deeper understanding of their design practices, motivations, and barriers. Our findings reveal a nuanced interplay of the challenges faced by developers in balancing the interests of children and monetisation. Specifically, we find that developers perceive a trade-off between designing for children's best interests and monetising their apps through targeted advertising and data collection. In addition, developers struggle with a lack of transparency in the mobile ecosystem regarding third-party libraries, hindering their ability to make informed decisions about data practices in their apps.

In Chapter 5, we employ a *Research through Design* (RtD) approach to generate and evaluate potential solutions for supporting developers in designing privacy-friendly apps for children. We created 12 speculative designs and solicited feedback through 20 semi-structured interviews with children's app developers. Through this process, we elicited concrete requirements for supportive tools and identified areas for future research, including addressing systemic and structural challenges in the mobile app ecosystem and considering the needs and perspectives of multiple stakeholders.

In Chapter 6, we take the design requirements from the previous chapter and use them to inform the development and evaluation of a web-based tool, `DataAvalanche.io`, to support developers in making more informed decisions about the privacy implications of third-party libraries. We conduct an evaluation with 12 app developers to understand how they envision using `DataAvalanche.io` in their development process and how it can be improved. Our evaluation provides insights into when and how developers would consider adopting privacy-friendly alternatives to commonly used SDKs, and the type of legal support they are seeking. Our participants also suggested additional features they would like to see in `DataAvalanche.io` to increase

its adoption. We conclude the chapter by discussing the potential impact and implications of the tool on improving the privacy of children's apps, as well as the limitations and future work that need to be addressed.

Finally, in Chapter 7, we summarise and discuss the findings of our research and outline important directions for future work.

1.4 Dissemination

The research conducted as part of this thesis has resulted in several publications. Chapters 3 and 6 have been presented in a single paper.

- Ekambaranathan, Anirudh, Jun Zhao, and Max Van Kleek. "Understanding value and design choices made by android family app developers." *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems.* 2020.

- 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.

- Ekambaranathan, Anirudh, Jun Zhao, and Max Van Kleek. "Poster: An Analysis of Privacy Features in 'Expert-Approved' Kids' Apps." *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security.* 2022.

- Ekambaranathan, Anirudh, Jun Zhao, and Max Van Kleek. "How Can We Design Privacy-Friendly Apps for Children? Using a Research through Design Process to Understand Developers' Needs and Challenges." *Proceedings of the ACM on Human-Computer Interaction 7.CSCW2* (2023): 1-29.

- Ekambaranathan, Anirudh, Jun Zhao, and George Chalhoub. "Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 7.2 (2023): 1-24.

2 Background

Contents

2.1 Introduction to Digital Childhood 17

2.1.1 Outline 19

2.2 Children and Privacy 20

2.2.1 Theories of Privacy 21

2.2.2 Children's Data Protection Frameworks 27

2.2.3 Children and Privacy 38

2.2.4 Summary 40

2.3 Data Tracking and Privacy in Mobile Apps . . . 41

2.3.1 Tracking: A Working Definition 42

2.3.2 Tracking on Smartphones 42

2.3.3 Unique Identifiers 44

2.3.4 Tracking Detection 45

2.3.5 Tracking in the Mobile Ecosystem 46

2.3.6 Why Data Tracking and Sharing is so Pervasive . . 47

2.4 The Attention Economy 48
2.4.1 Persuasive Design 48
2.4.2 Dark Patterns 49
2.4.3 The Role of Data in the Attention Economy 50
2.4.4 Harms Arising from Persuasive Design and Data-Driven Personalisation 50
2.5 Advertising 52
2.5.1 The Relevant Actors 52
2.5.2 Real-Time Bidding (RTB) 54
2.5.3 The Role of Data in Advertising 55
2.5.4 Children and Advertising 56
2.5.5 Harms Arising from Advertising 56
2.6 Discussion 56
2.6.1 Key Findings 56
2.6.2 Revisiting Privacy and Being Privacy-Friendly . . 59
2.6.3 Research Gaps and Contributions 60

2.1 Introduction to Digital Childhood

The past few decades have witnessed a shift in activities from the physical to the digital realm. Tasks that were traditionally constrained by physical limitations can now be conducted in a more diverse and rich environment, such as commerce, education, and socialization. The concept of a life without digital technology is now virtually inconceivable. Digital technology has become so deeply entrenched within our everyday lives that participation in the digital space is essentially obligatory. Everyday tasks, such as banking, communication, and education, necessitate access to a digital device. It is now commonplace to have a smartphone on one's person in order to be connected to the internet or to complete mundane tasks.

The phenomenon of digital devices becoming extensions of ourselves is also applicable to children. Children now spend more time on digital devices than ever before [43], with mobile devices such as smartphones (72%) and tablets (69%) being the dominant form of access [15, 44]. In the UK, nearly all

children aged 3-17 have spent time online, primarily through mobile devices [2], and a majority of children under the age of 13 even have social media profiles [2]. Moreover, the age at which children are equipped with such devices is decreasing; 97% of children under the age of four are already using digital devices [45], and 82% of those aged 5-7 spend around 10 hours per week online [43]. Pre-schoolers are thought to consume media for around three hours per day as part of their daily routine [46, 47, 48], with most of this time being spent on watching videos [49, 48]. Even older children are shifting their presence to the digital space; 83% of 12-15 year olds in the UK own a smartphone, and 64% own three or more devices [43]. Mobile devices are used for a range of activities, including video sharing, messaging and calling, social media, and live streaming [2].

The use of mobile devices by children is a global phenomenon, not only limited to the UK population. Studies have demonstrated that the adoption of mobile devices by young children and adolescents is a well-established trend in Europe, the Americas, and Asia [50, 51, 52, 53]. For instance, 80% of children between the ages of two and ten in the United States use mobile devices at least once a week and one-third use them daily; 62% of three-to-four year olds make use of smartphones, 81% of five-to-eight year olds make use of a tablet, and 17% of the children under eleven have their own mobile device [51]. In the Netherlands, up to 70% of the children are reported to regularly make use of tablet devices [52]. In Asia, a 2015 study with nearly 1,000 Korean elementary school children, under the age of 12, showed that 72% owned a smartphone [53].

As the presence of children online continues to be strong, the industry for children's mobile applications has seen an increase in growth. Popular app marketplaces, such as Google Play [54] and the Apple App Store [3], have categories of apps designed specifically to be used by children [4]. These sections commonly feature labels like 'Apps for children' or 'Games for children,' and they typically offer age-based filtering options ('Ages up to 5' and 'Ages 6-8') [5]. The digital world that children are growing up in offers a plethora of benefits and advantages, as apps are designed to address a variety of problems that children may encounter. For example, there are apps intended to improve children's mental and physical wellbeing [55, 56, 57], help those who have special needs [58, 59, 60, 61], or improve education [62, 63, 64].

While studies in the last decade strongly hint at negative consequences of smartphone usage [65, 66, 67], the access to free resources through digital devices and the increased availability of services to all user populations, both

marginalised and those from affluent families, has created a potential for smartphones to cater to positive needs. Smartphone apps for children have been used to improve health [55, 56, 57], address the needs of children with special needs [58, 59, 60, 61], and to provide education [62, 63, 64]. It is not necessary to make use of apps specifically designed for improvement purposes to enjoy benefits of mobile devices. Media consumption in general can have positive effects. Watching videos, for example on the smartphone, can contribute to social and emotional learning [68], skill development, and help with school-readiness [69, 70].

At the same time, the use of mobile devices and screen time can have a range of negative consequences. While this study is limited to those harms related to data collection and privacy, it is important to acknowledge that the actual range of harms extends beyond this study, including psychological and physiological harms. For instance, exposure to violence on screen in children has been linked to increases in hostility, perception of hostility in others (hostility attribution bias) and emulation of violence [71, 72, 73]. Content that is designed for older audiences can cause fear and anxiety in young children [73]. Moreover, media exposure before the age of 3 and exposure to fast-paced video content has been linked to attention disorders [74, 75], while increased screen time has been associated with increased risk of obesity [76, 77, 78], decreased imaginative play [79] and disordered sleep [80].

2.1.1 Outline

The current mobile landscape is largely commercially driven, with data being the currency used to monetise apps and services. Apps which children use often contain a data trackers which collect and share sensitive user data with third- and fourth parties [35, 7]. As a result, concerns have been expressed by regulatory, public, and human rights organisations about the extent of data collection and sharing, and the potential risks associated with them. Major platforms and commercial tech giants have come under increasing amounts of scrutiny.

In this chapter we discuss why privacy is important to children, how loss of privacy concretely occurs in the mobile ecosystem, what this data is used for, and how this leads to concrete harms for children. Specifically we discuss the following elements:

- **Children and privacy.** We first review popular theories of privacy

and how common data protection frameworks aim to protect children's privacy at the moment of writing. We then discuss why privacy is important for children and harms arising from a loss of privacy.

- **Data tracking and privacy in mobile apps.** After achieving a good grasp of what privacy is and its varying conceptualisations, we look at how the mobile ecosystem poses a threat to children's privacy. Specifically we look at how data tracking occurs in apps.

- **The Attention Economy.** Next we look at how data is used to hook children to mobile devices. We look at concepts such as *persuasive design* and *dark patterns*, and the role of data in this, as well as the harms which arise from practices.

- **Advertising.** We take a deep dive into advertising in the mobile industry, as this is one of the core objectives of large tech companies. Specifically, we look at the role of data in advertising, and the harms associated with advertising for children.

- **The role of developers.** We finally also look at what we know about developers and their role in contributing to privacy protection practices in apps for children. We discuss their privacy behaviours and some of the challenges they face when it comes to understanding legal requirements.

This chapter should familiarise readers with the necessary literature and background needed to understand the subsequent chapters of this thesis. We conclude this chapter with a summary and highlight the literature gaps.

2.2 Children and Privacy

Privacy is a central concept in this thesis as much of the research has been motivated by a lack of privacy in mobile apps. In this section, we therefore take a look at what privacy is and how it has been conceptualised according to different theories. We then examine the practical implementation of privacy through the lens of data protection frameworks specifically designed to safeguard the privacy of children, and their implications within the mobile application ecosystem. We finally also discuss the importance of privacy for

children, children's perceptions of privacy, and harms arising from a loss of privacy for children.

2.2.1 Theories of Privacy

In this thesis, we focus specifically on the threat of data tracking occurring in the mobile ecosystem, suggesting the need for *privacy-friendly* app development. The concept of *privacy* is complex and means different things to different scholars. While theoretical discussions of privacy do not lie at the heart of this thesis, as we focus more concretely on the technical aspects of data tracking, we do acknowledge that privacy and the harms arising from data tracking are closely related. Therefore, in this section, we discuss the concept of privacy, so that we can more clearly formulate later what we mean by *privacy-friendly* apps.

The concept of privacy has often been perceived as ambiguous, posing difficulties for privacy scholars to describe its exact definition [81]. One of the first definitions of privacy was given by Warren and Brandeis in 1890, with the advent of photography and mass media, and they argued that privacy is a "right to be left alone" [82]. They claimed that new technological advances called for the development of broader legal principles and their concepts of privacy were the foundations of US privacy regulation [81, 83].

Warren and Brandeis' historical definition, while historically significant, proves inadequate in addressing the complexities of contemporary digital privacy, especially within the realm of mobile apps and data tracking. A notable drawback is the limited consideration given to the nuanced factors determining what information about oneself is shared, how it's communicated, and the timing of such disclosures. This limitation becomes particularly apparent in the modern context of digital privacy. Privacy researchers have built on the theories of Warren and Brandeis to provide ever-evolving conceptualisations of privacy that are better suited to our modern digital needs. We explore these below.

Westin's Theory of Privacy

Since the 1890s, research in privacy has come a far way. One of the first psychological systematic analysis of privacy was presented in the 1960s by legal scholar Alan Westin in his seminal work *Privacy and Freedom* [84]. Westin described privacy as the "claim of individuals, groups, or institutions

to determine for themselves when, how, and to what extent information about them is communicated to others" [84]. He proposed four states of privacy an individual could achieve. The first and most complete state of privacy is called *solitude*, in which an individual is "separated from the group and free from the observation by other persons" (p. 33). The second state is called *intimacy* and describes a state of privacy in which a small group of people withdraw from larger society. For example, this may exist between partners or friends. The third state is called *anonymity*, and describes a state in which an individual is protected from identification and surveillance in public places. Lastly, the fourth state is called *reserve* and describes a mental state of privacy in which individual choose to not share information.

Westin conducted over 30 surveys between 1978 and 2004 investigating consumer attitudes towards privacy. Based on these surveys, he categorised people into three classes: privacy fundamentalists (people who were concerned about their privacy), pragmatists (people weighed their decisions against a privacy trade-off), and the unconcerned (people who were trustful and were not concerned about their privacy).

One property of Westin's conceptualisation of privacy is that it is based on voluntariness. According to Westin, privacy can only be achieved if a person *chooses* to enter one of the four states of privacy. Therefore, if one were to be forced into solitude, this cannot be regarded as privacy. Westin's theories therefore have its drawbacks. For example, in today's world, the property of voluntariness may not translate well, as the digital space is known to unknowingly collect data [7]. In addition, the static notion of privacy and its categories are often considered to be too simplistic [85]. The problem is that Westin's theory of privacy is binary in nature: privacy is something that people either have or not. Westin himself acknowledges that "individuals are constantly engaged in an attempt to find sufficient privacy to serve their general social roles as well as their individual needs of the moment" (p. 44).

Altman's Theory of Privacy

A different approach to Westin's theory of privacy was proposed by Altman [86]. According to Altman, informational privacy is not something that is static or governed by a strict set of rules. Rather it is "the selective control of access to the self or to one's group" [87]. Privacy is about control of access to one's self, and it is selective in that the demand for privacy can change over time and in different circumstances. Altman postulated six properties

of privacy. First, privacy is an inter-personal boundary control process, in which the privacy regulation process is like the "shifting permeability of a cell membrane" (p. 10). Second, privacy is about the regulation of both the *inputs* and the *outputs*. These two properties point to the fact that privacy is control-based and regulated by human interactions. Third, there is a distinction between the desired level of privacy an individual wants and the achieved level of privacy. Fourth, as a result of the former, an individual is continuously optimising their control of privacy in order to reach their desired level of privacy. Fifth, privacy involves different levels of social units. Lastly, privacy is a dialectic process, meaning that at times individual may want to interact with others while at other times they may want to withdraw.

Altman's theory of privacy is different from Westin's theory of privacy, as it considers privacy to be a dynamic process focusing on social interactions. [88]. His theory of selective boundary regulation allows for self-evaluation and self-observation [87] (p. 49). Therefore, privacy allows individuals to evaluate and give meanings to social events, set norms for interpreting the self in relation to others, and decide on courses of action.

However, Altman's theory of privacy too, can be difficult to apply in the age of the Internet. For example, to use apps and digital services, one must usually accept the terms of service and the privacy policy. However, this process often is non-negotiable, and the theory of boundary regulation can fail to acknowledge this power asymmetry.

Privacy as Contextual Integrity

In more recent work, Helen Nissenbaum describes privacy as *contextual integrity*. Nissenbaum's theory of privacy as contextual integrity is a framework for understanding how privacy should work in different contexts. According to Nissenbaum, privacy is not an absolute right, but rather a social norm that varies depending on the context in which it is being applied. She argues that privacy is maintained through the concept of "contextual integrity", which refers to the appropriate balance of information flow in a given context. Different contexts require different levels of privacy, and it is important to ensure that the right amount of information is shared in each context. For example, in a more confidential setting, a high level of privacy is expected and necessary in order to maintain trust. On the other hand, in a public space, a lower level of privacy is expected and may be appropriate. Nissenbaum's theory is grounded in the idea that privacy is a social construct, and that

it is shaped by the expectations and norms of the society in which it exists. This means that privacy norms can change over time and can be influenced by a cultural, technological, and social factors.

Nissenbaum's theory of privacy as contextual integrity consists of four elements:

1. **The flow of information**: This element refers to the movement of information from one person or entity to another. In order to maintain contextual integrity, the flow of information should be appropriate for the given context.

2. **The content of the information**: This element refers to the type of information being shared. Different types of information are considered appropriate to share in different contexts. For example, medical information is generally considered more sensitive than a person's demographic information.

3. **The relationships between the parties involved**: This element refers to the nature of the relationship between the parties involved in the information exchange. Different relationships require different levels of privacy. For example, one may share more confidential information with a close relative, such as a spouse, than with a casual acquaintance.

4. **The context in which the information is shared**: This element refers to the setting in which information exchange takes place. Different contexts require different levels of privacy. For example, a conversation at home may require a higher level of privacy than a conversation outside in public.

Nissenbaum's theory of privacy as contextual integrity is a useful framework for understanding how privacy works in different contexts and for examining the ways in which it can be compromised or protected.

Livingstone's Dimensions of Children's Privacy

Based on Nissembaum's theory of privacy as contextual integrity, Livingstone et al. formulated various dimension of children's online privacy [13]. In considering the impact of children's actions in digital environments on their

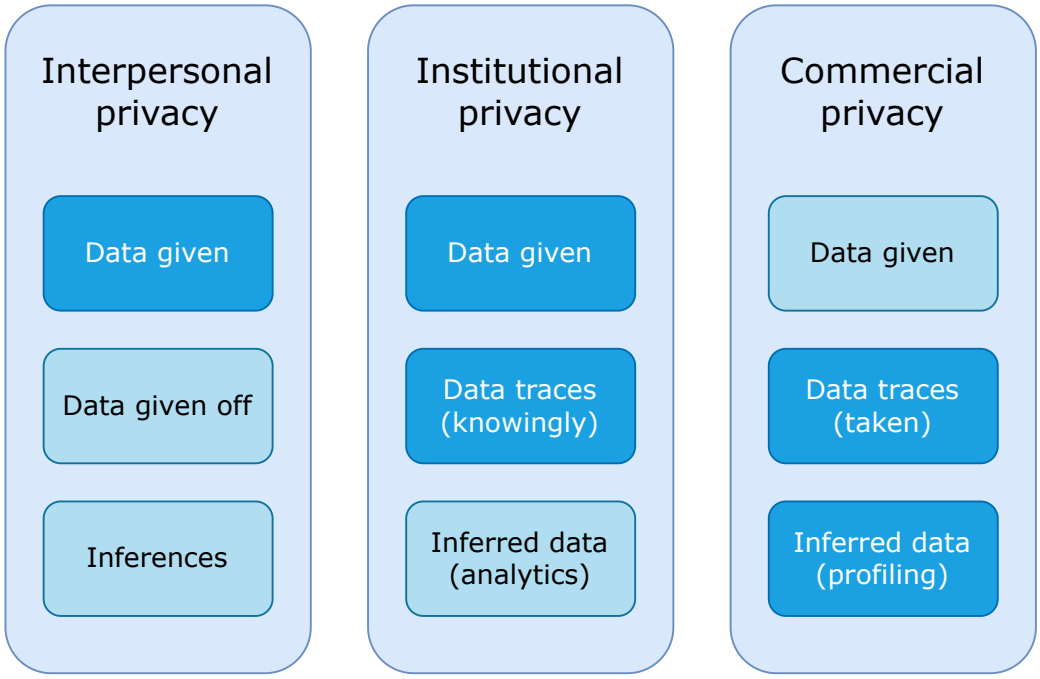


Figure 2.1: Livingstone's three dimension's of privacy, consisting of an interpersonal, institutional, and commercial dimension. The intensity of the colours represent the different degrees of 'invasiveness' [13].

privacy, they focus on the relationships and contexts in which they occur and how children understand their privacy implications. They identify three main types of relationships or contexts in which privacy is relevant, which they refer to as the dimensions of children's privacy. The first dimension is interpersonal privacy, which refers to the privacy that children expect when they are interacting with other individuals or groups online. This can include things like the ability to control who sees their personal information or how it is used, as well as the right to keep certain types of communication or activities private. The second dimension is institutional privacy, which refers to the privacy that children expect when interacting with public or non-profit organisations online. This can include things like the privacy of their personal information when it is collected or used by these organisations, as well as the right to privacy when using services or resources provided by these organisations. The third dimension is commercial privacy, which refers to the

privacy that children expect when interacting with for-profit organisations online. This can include things like the privacy of their personal information when it is collected or used by these organisations, as well as the right to privacy when using products or services provided by these organisations. This last dimensions of commercial privacy refers to the type of privacy children expect when making use of apps and operating in app marketplaces.

These three dimensions represent the different types of relationships and contexts in which children's privacy is important online, and they provide a useful framework for considering the privacy concerns of children in the digital world. Livingstone et al. adopted Simone van der Hof's typology for understanding the different types of privacy concerns that individuals may have when using digital technologies [89]. Van der Hof's typology identifies four main types of privacy concerns: information privacy, contact privacy, decisional privacy, and physical privacy. Livingstone et al. adopted this to distinguish between *data given* intentionally (though not necessarily intentionally) online, *data traces* left (usually unknowingly, e.g. cookies), and *inferred data* from analysing data given and data traces. They capture these relationship between these different types of privacy diagrammatically as shown in Figure 2.1 [13].

Summary

History has seen varying definitions and interpretations of privacy. Westin's theory of privacy emphasises the importance of individuals' ability to control their personal information and the use of that information, while Altman's theory focuses on the psychological need for privacy and the different types of privacy that individuals may seek. Nissenbaum's theory of contextual integrity (CI) emphasises the importance of considering the norms and values of a particular context when determining the appropriate use of personal information.

In thinking about privacy in mobile applications, the three dimensions of privacy as proposed by Livingstone et al. [15] allow us to be more concrete about the type of privacy breaches we wish to consider. These dimensions provide a framework for understanding the different ways in which children's personal information may be collected, used, and shared and the factors that may affect their privacy. For example, the interpersonal dimension may be relevant when considering the sharing of children's personal information with friends or family members through social networking or messaging features

within an app. The institutional dimension may be relevant when considering the collection, use, and sharing of children's personal information by app developers or other organisations, such as advertisers or analytics companies. The commercial dimension may be relevant when considering the collection, use, and sharing of children's personal information for commercial purposes, such as targeted advertising or market research.

Previous research has largely focused on children's understanding of interpersonal privacy, while their recognition and comprehension of institutional and commercial privacy remains inadequately understood. [13]. In contrast, recent data protection frameworks have exhibited a heightened focus on institutional and commercial dimensions. Therefore, in the next section, we look at data protection frameworks and how they can be used to operationalise the principles of children's privacy in mobile apps. Data protection frameworks, such as the GDPR, provide specific guidelines and requirements for the collection, use, and disclosure of children's personal information in mobile apps and other online services. By considering and implementing such frameworks, it is possible to more effectively protect children's privacy in mobile apps and ensure that their personal information is collected, used, and shared in a way that is consistent with their best interests.

2.2.2 Children's Data Protection Frameworks

In this section we present a review of five leading children's data protection frameworks from three different sectors (regulatory, private, and human rights organisations), with the aim of understanding requirements and expectations for protecting children's privacy in the mobile ecosystem. In this review, we focus on parts of the frameworks related to data collection and processing, and its recommendations for how these practices should be made clear in order to protect children's privacy. This review provides a useful comparison between privacy theories, as discussed in the previous section, and data protection frameworks, which provide specific guidelines and requirements for the collection, use, and disclosure of children's personal information. By considering both privacy theories and data protection frameworks, it is possible to more fully understand and address the complex issues surrounding children's privacy in the digital age.

To compare the requirements and expectations for protecting children's privacy across different frameworks, we use the statutory Age Appropriate Design Code (AADC), developed by the Information Commissioner's Office

(ICO) in the UK, as the benchmark. The AADC is seen as one of the most comprehensive regulatory frameworks to date and is particularly relevant for our analysis of children's apps from the UK app market. In order to compare the AADC with other frameworks, we align the data protection principles from the AADC with those from the following four frameworks:

1. *(Regulatory)* COPPA - The US Children's Online Privacy Protection Act;
2. *(Human rights)* COPFE - UNICEF's Children's Online Privacy & Freedom of Expression ;
3. *(Private sector)* Google's 'Designing Apps for Children and Families';
4. *(Private sector)* Apple's App Store Review Guidelines.

We have not included the GDPR(-K) in this, because the AADC is designed to be a clarification of the enforcement of GDPR(-K). We do give a brief overview of GDPR and before getting into the details of the AADC.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) came into effect in May 2018 [16]. Its aim was to give data subjects more control over their personal data. The GDPR defines personal data as "any information that relates to an individual who can be directly or indirectly identified" [90]. When processing an individual's personal data, under Article 5.1-2, it needs to adhere to 7 data protection and accountability principles: (1) Lawfulness, fairness and transparency, (2) Purpose limitation, (3) Data minimization, (4) Accuracy, (5) Storage limitation, (6) Integrity and confidentiality, and (7) Accountability. Data controllers need to demonstrate that they comply with the GDPR, for example by appointing a Data Protection Officer. Furthermore, processing of personal data is only allowed under certain circumstances. There needs to be a lawful basis for processing personal data or the data subject needs to have given unambiguous consent. For children under 13, consent can only given with permission of their parent. There are a few exceptions, for instance if the purpose of data processing is to save someone's life or to fulfil a legal obligation.

The GDPR also acknowledges that "[c]hildren merit specific protection with regard to their personal data", which the Age Appropriate Design Code provides more clarification on.

The UK ICO Age Appropriate Design Code (AADC)

The UK Information Commissioner's Office (ICO) is an independent authority aimed at protecting and upholding information rights in the public interest and promoting data privacy for individuals. In an effort to address privacy concerns of children in the digital world, the ICO introduced the statutory Age Appropriate Design Code (AADC) [17] [1]. The AADC aims to ensure online services safeguard children's personal data and comply with the GDPR. If services are not compliant by September 2021, the ICO can issue firms enforcement notices and fines up to 4% of their global turnover if they breach these data protection guidelines.

The AADC consists of 15 codes which take into account principles set out in the United Nations Convention on the Rights of the Child (UNCRC). The code touches on many different aspects related to design for children, including user-facing design practices (such as 'transparency', or 'high privacy' by default'), alignment with fundamental principles (such as supporting children's best interest), support for data protection in new emerging technologies (e.g. connected toys), and regulations regarding data collection and minimisation.

The focus of this review is to understand how current regulations related to children's data protection online may provide practical requirements for protecting children's privacy in the mobile app ecosystem. Therefore, we focus on those AADC codes specifically related to the technical aspects of privacy, such as 'Data minimisation' and 'Data sharing', and those related to usable privacy aspects, such as 'Transparency' and 'Nudge techniques'.

We identified eight such codes from the AADC that are directly related to regulations of processing children's data and how this should be made clear in apps. Five of these codes relate to technical privacy aspects and three of them relate to usable privacy aspects. These are summarised and explained in Table 2.1.

We excluded the following codes which did not fall under this category: (1) Best interest of the child, (2) Data protection impact assessments, (3) Age appropriate application, (6) Policies and Community Standards, (11) Parental Controls, (14) Connected Toys and Devices, and (15) Online Tools.

[1] The latest ICO Code for Age Appropriate Design is available at `https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/5-detrimental-use-of-data/`; retrieved on 4 August 2020.

We have omitted these codes from our analysis because they do not align with the primary technical and usable privacy aspects that our study aims to investigate within the mobile app ecosystem.

Table 2.1: A summary of the data protection codes in the AADC.

AADC code	**Definition**
Code 4: Transparency	Be clear, open and honest with users about what they can expect when they access your online service. Provide 'bite-sized' explanations of terms and policies in a child friendly way.
Code 5: Detrimental use of data	Does not exploit children's data for purposes that may harm their health or wellbeing.
Code 7: Default settings	Privacy settings must be set to 'high privacy' by default.
Code 8: Data minimisation	Collect and retain only the minimum amount of personal data you need to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.
Code 9: Data sharing	Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.
Code 10: Geolocation	Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation to be switched on by default, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others should default back to 'off' at the end of each session.
Code 12: Profiling	Switch profiling 'off' by default (unless you can demonstrate a compelling reason for profiling to be on by default, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).
Code 13: Nudge techniques	Do not use nudge techniques to lead or encourage children to provide unnecessary personal data or turn off privacy protections.

Table 2.2 summarises how the key aspects from UNCRC, COPPA and Apple

and Google's app development guidelines are aligned with the AADC codes previously presented in Table 2.1, as we explain in details below. For those principles which do agree with AADC, we included the definition of the principle to highlight the nuanced differences between all the frameworks.

Table 2.2: This table lists 4 leading data protection frameworks and their alignment with the data protection principles set out by the AADC. The cells without content indicate that the framework does not mention the associated AADC code.

AADC Codes	**UNICEF**	**COPPA**	**Apple App Store**	**Google Play**
4: Transparency	Information presented must align with children's literacy levels	The privacy policy for parents should be clear and understandable	Privacy terms should be clear, but this is not child specific	-
5: Detrimental use of data	Children have the right not to be subjected to attacks on their reputation	-	-	-
7: Default settings	Privacy settings must be high by default	-	-	-
8: Data minimisation	Children's data are kept to what is minimally necessary	Should not condition a child's participation on the collection of more than the personal information that is required to drive that activity	Only access to data relevant to the core functionality of the app is permitted	The collection of any personal and sensitive information must be disclosed

9: Data sharing	Refrain from sharing information that could undermine children's current or future reputation	Disclosure to third parties requires parental consent and assurance that reasonable security measures are in place	Prohibited from sending PII or device information to third parties; this includes IDFA, location, and device information	-
10: Geolocation	-	Geolocation is treated as PII and needs parental consent before collection;	If directly relevant to the features and services provided by the app	Cannot request location permissions
12: Profiling	Children enjoy protection from online profiling	The use of any persistent identifiers for the identification of a specific individual is prohibited	Third-party analytics or third-party advertising prohibited	Interest based marketing prohibited
13: Nudge techniques	-	-	-	-

The United Nations Convention on the Rights of the Child (UNCRC)

The United Nations Children's Fund (UNICEF), is an agency which is part of the United Nations and globally provides humanitarian aid to children. To support developers in realising the fundamental privacy rights, in 2018 UNICEF introduced the 'Children's Online Privacy & Freedom of Expression' (COPFE) industry toolkit, which describes five overarching principles [91, 92] to protect children's right to privacy, personal data freedom of expression, protection of reputation, and access to remedy.

This framework is largely aligned with the AADC, with a great empha-

sis on children's fundamental rights; however, the framework also discusses many additional elements on the rights for children, such as the rights to be educated, have access to resources for risk coping, and the right for parents to have access to resources to help their children. Five of the sub-codes are identified to be closely related to the set of AADC benchmark codes, with some slight different emphases.

Data profiling is discussed in COPFE, at a more general level: "Children enjoy protection from online profiling". It does not specifically give examples of profiling or explain what constituted profiling. In their checklist, profiling is placed in the context of behavioural advertising and suggests applying *"specific protection"*, as it *"involves collecting and aggregating personal data"*. As for **data minimisation**, COPFE states that collected data should be *"fit for purpose"* and limited to *"what is minimally necessary"*. The stakeholders involved in **data sharing** are explicitly named to include both *"parents or guardians"*, *"media outlets and other third parties"*, who should *"refrain from sharing information that could undermine children's current or future reputation"*. COPFE also argues against **detrimental use of data**, stating that "children have the right not to be subjected to attacks on their reputation" and "can seek the removal of content they believe is damaging to their reputation". It does not explicitly talk about geolocation or location settings.

COPFE also highlights to importance of considering children's digital literacy levels, specifically when making terms and policies clear, as well as when they wish to access reporting mechanisms: "Children have reliable and affordable access to digital technology, accounting for differences in language, literacy and capacity". It does not specifically say anything about nudging users, however it does say that settings must be kept high be default: "Children's privacy is better protected when an [application] does not share their personal data publicly by default".

The Children's Online Privacy Protection Act (COPPA)

The US Children's Online Privacy Protection Act COPPA Rule was established primarily to curb direct marketing aimed at children under 13. It first went into effect in 2000 to implement the US Children's Online Privacy Protection Act (COPPA) 1998. COPPA is aimed at operators who provide services targeted to children under the age of 13.

Broadly speaking, COPPA focuses on the enforcement of a clear online

privacy policy for services targeted at children, and supporting parents to provide consent on their children's behalf and protect their children's personal data online. COPPA has one specific rule about data handling, which describes that children's data should be retained *"for only as long as is necessary to fulfill the purpose for which it was collected and delete the information using reasonable measures to protect against its unauthorized access or use"* [93].

COPPA has an inherent **data minimisation** principle: service providers *"Should not condition a child's participation on the collection of more than the personal information that is required to drive that activity"*. It has no specific conditions on **data sharing**, apart from that it requires parental consent assurance that reasonable security measures are in place by the party the data is being shared with. **Geolocation** data is treated as personally identifying information if it can be narrowed down to street or city name, in which case parental consent is requried. Regarding data **profiling**, a service is COPPA-compliant so long as no *"specific individual can be identified profiling including through their persistent identifiers"*. Under COPPA, the use of any persistent identifiers for the identification of a specific individual is prohibited.

COPPA does say that services collecting personal informaiton of children must have a privacy policy, which is "clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials". However, according to COPPA the privacy policy should be aimed at parents, rather than children. COPPA does not specifically say anything about default privacy settings or the use of nudge techniques.

Private Sector Guidelines - Apple and Google

When publishing apps on Google's Playstore or Apple's Appstore, there are specific terms that the app has to uphold. Both Google and Apple have sections reserved for apps targeted at children in these terms.

Google has these outlined in their 'Designing Apps for Children and Families' [94] guidelines. Apps targeted at children must comply with the 'Designed for Families' programme, which lists 12 requirements apps must fulfil. The requirements cover different aspects of app design, including the content of apps, policies regarding ads, and special restrictions about the use of Augmented Reality. Advertising is only allowed through certified ad SDKs [95] and interest based advertising is not allowed. Collecting personal data

of users is allowed as long as it is disclosed to them. Google further requires apps to comply with GDPR, COPPA, and other applicable regulations.

Similarly, before publishing on Apple's App Store, apps have to comply with the 'App Store Review Guidelines' [96]. Apple has specific sections in their terms aimed at protecting children's privacy. Third-party analytics and third-party advertising for children is permitted in limited cases, given that services do not transmit personally identifiable information and have their practices and policies publicly documented.

Neither guidelines state anything specifically regarding **detrimental use of data** in the context of data processing, while both have clear requirements about **data minimisation**. Apple requires apps to only request access to data relevant to the core functionality of the app [96], and Google requires apps to disclose the collection of any personal and sensitive information [94]. This is also the same for **profiling**, where neither allow interest based marketing. Apple also does not allow third-party targeted analytics and third-party advertising. In fact, Apple does not allow any **data sharing** with third parties, while Google does not have a clear policy on this.

Geolocation is also discussed in both guidelines. In this regard, Google is stricter than both the AADC and Apple, requiring that *"Apps designed specifically for children cannot request location permissions"* [94]. Apple's stance is more aligned with the AADC and requires that location services should only be used *"when it is directly relevant"* [96].

When it comes to user facing aspects, Apple has 'Human Interface Guidelines' which stipulate that "[developers] must be transparent about the privacy-related data and resources [they] require and how [they] use them". When it comes to **Transparency**, Apples guidelines state that a "privacy policy must clearly and explicitly" describe its data collection practices. It does not explicitly mention anything about nudging or default settings.

Similarly, Google's 'Designing Apps for Children and Families' guidelines state that "[developers] must be transparent in how [they] handle user data ". When it comes to privacy policies, it must "together with any in-app disclosures, comprehensively disclose how [the] app accesses, collects, uses, and shares user data, not limited by the data disclosed in the privacy label". Google does not specifically mention anything about making it age-appropriate for children to understand, nor does it have any mention of nudging techniques or default settings.

Analysis Summary of Data Protection Frameworks

Table 2.2 summarises how the terms specific to data handling in these guidelines are aligned with the AADC codes previously presented in Table 2.1. For those principles which do agree with AADC, we included the definition of the principle to highlight the nuanced differences between all the frameworks.

It shows that regulation/guidance around data-based profiling is required by all frameworks; however, there are some nuanced emphases amongst them. The AADC takes the position that children merit specific protections with regard to the use of their personal data, and therefore requires profiling to be transparent and to be turned off by default. COPPA is stricter in this regard, prohibiting any profiling that may identify any specific individual. Apple and Google are aligned with this, and prohibit interest-based marketing, with Apple stricter than Google and the AADC, as they prohibit third-party analytics and advertising.

Data minimisation is also widely required by all frameworks, but with different emphases. Apple's is most aligned with the AADC, although it does not provide an option for children to 'make separate choices over which elements' to be activated yet. Interestingly, because of its sensitive nature, **geolocation** is specially discussed in all the frameworks except COPFE. While Apple allows the use of geolocation with reason, Google does not allow location permissions to be requested in any app directed at children.

Detrimental use of data is only discussed by COPFE and AADC, as probably both have a primary focus on children's wellbeing and best interest. It can be interesting to see with the effect of AADC in September 2020, how this may affect the current guidelines.

Lastly, the user facing codes, such as **Transparency** and **Nudge techniques**, are only mentioned in COPFE. The private sector guidelines make no mention of this, and COPPA only considers the legal elements of the privacy policies, in that they are complete and understandable. Moreover, COPPA delegates all privacy matters to parents, rather than considering children as taking control of their own data. This is one major aspect in which COPPA differs from the GDPR and AADC.

We can also analyse the frameworks through the lens of the three dimensions outlined by Livingstone et al. [13]. The interpersonal dimension is not explicitly addressed in any of the frameworks, as it pertains to children sharing data amongst each other. However, the AADC does state that children should not be 'nudged' into disclosing more data than necessary.

Although this primarily pertains to preventing products and services from collecting excessive data from their users, it can also be applied to children sharing information on platforms that rely on user-generated content, such as social media platforms. The institutional and commercial dimensions are more heavily reflected in the data protection frameworks. Specifically, the AADC has stringent requirements for handling data traces and inferred data. The guidelines by Google and Apple address this through how third-party tracking should be handled. For example, Apple prohibits any form of third-party tracking analytics and advertising, which the AADC recommends to be disabled by default.

Revisiting the AADC: Systemic Breaches

In the time following the introduction of the AADC, the 5Rights foundation sent a letter to the ICO in the UK outlining in which ways apps are not compliant with the code [97]. While the details of the study are not publicly available, the letter outlines common systemic breaches which serves as a framework to understand how apps may struggle to comply. In Table 2.3 we have summarised the breaches which are relevant to our review. Similar to our analysis of the AADC, we left out codes not directly relating to data collection and processing for developers, such as 'Connected devices'. We have formulated the breaches as a framework, since it provides a convenient lens for us to view the AADC in a simplified manner. We use this framework in Chapter 3 to inform our own app analysis framework.

Table 2.3: Common breaches of the Age Appropriate Design Code observed in apps.

#	**Breach**
(1)	Insufficient age assurance
(5)	Use of dark patterns and nudges
(6)	Age-inappropriate financial pressures
(7)	Low default privacy settings
(8)	Excessive data sharing with third parties
(9)	Lack of transparency and excessive data sharing between services and third party login providers
(10)	Published terms are not age-appropriate

2.2.3 Children and Privacy

Now that we have reviewed and compared a range of data protection frameworks and their requirements for protecting children's privacy, it is important to also consider how children perceive privacy and the importance of privacy for children, particularly in the mobile ecosystem. Children's understanding of privacy and the value they place on it may differ from that of adults and may be influenced by a range of factors, including their age, developmental stage, and social and cultural context. Understanding children's perceptions of privacy can help to inform the development of apps and other online services that are tailored to the needs and interests of children. In the next section, we will explore the ways in which children perceive privacy and the importance of protecting their personal information in more detail.

Importance of Privacy for Children

Livingstone et al. argue that privacy is a crucial element for child development [13], as they associate it with media literacy skills which play an important role in developing skills such as responsibility, trust, autonomy, and critical thinking [98, 99, 100, 101]. The digital activities and platforms that children engage with provide opportunities for them to build these skills. As children grow older, their understanding and desire for privacy also increases [102, 103, 104]. The limited understanding that young children have about privacy is what makes them a particularly vulnerable user group and that concerns have been expressed about the 'datafication' of children [11].

While children are the receiving end of the services provided by apps, they are often perceived as inherently vulnerable, because they are too young to understand privacy [38]. Their understanding of the risks associated to long term accumulation of data is still underdeveloped [39]. While they can identify certain sensitive entities, such as passwords, they find it difficult to identify dangerous or malicious actors [105]. However, they do value their privacy to enjoy their online experiences [103, 106] and to protect themselves, they draw analogies between the physical and digital world. For example, similar to how they might hide personal objects, they may choose not to share certain data [107].

At the same time, children also struggle with what is known as the "privacy paradox" [108, 109, 39]. This describes behaviours when people act contrary to their privacy preferences. For example, one may not want to

disclose their personal data, but still post photos on social media. This is common amongst both children [110] and adults [111]. For example, they realise that sharing certain information online can put them at risk of being identified, even though they are worried about it happening to them [39]

Differences in Age Groups

While some of these findings related to privacy and children can be generalised to all children, important differences exists between children of different age groups. However, it is difficult to categorise the privacy needs and understandings of children to absolute age groups. Children of the same age group might have a different understanding of privacy due to factors such as socio-economic status [112], levels of literacy, and access to digital media. Children between the ages of 5 and 7 are avid users of digital devices, engaging in a small set of activities while having a limited understanding of the risks online [104, 13]. They also have a limited understanding of how to protect their privacy online [113] and their strategies are limited to closing the app or providing fake information [103]. Children between the ages of 8 and 11 understand that sharing information online can create risks [103, 13]. However, they still have difficulties in identifying commercial content, for example advertising or sponsored content [43, 67]. They also find it difficult to understand or comprehend privacy terms and conditions [103].

Children and Apps

Despite the fact that children nowadays grow up in a digital environment, children do not understand digital risks as well as most adults [15] and they have a poor understanding of privacy related contexts [114, 103]. For example, children fail to understand why their data is valuable to third parties [115], how their data is collected [116, 117], how it is stored and analysed [118], and how it may be used in the future [119, 118, 120].

Children struggle with privacy policies the same way adults do, as they find it challenging to understand privacy terms and conditions, because of their length and legalese [121]. and feel forced to accept the terms laid out to them [115]. Children feel that targeted advertising and profiling is a part of digital life [115] and that there is very little they can change about their behaviour to prevent this [115, 120].

Considering the Role of Parents

Parents play an important role in determining young children's media consumption habits and the mediation of their children's digital practices [122, 123], because these activities start before children are autonomous [124, 125, 126]. The content that children are exposed to is heavily influenced by the parents through co-viewing, actively discussing values and attitudes about media, and by regulating types of content [127, 128, 129]. The behaviours of parents themselves are also important in this, as children tend to imitate their digital practices [130, 131]. While parents do want children to enjoy the learning potential of apps, they are also afraid of risks and negative consequences, such as addiction, sleeping disorders, and obesity [113, 132, 133]. The most reliable predictor for children's media use is determined by the parenting style [134, 135, 128, 136]. Most parents employ restrictive and enabling types of strategies [124, 137, 138, 125, 126, 71].

Generally, parents want children to consume content that is educational or that will occupy children sufficiently for them to have uninterrupted time to perform household tasks [122]. However, parental needs differ across families, as some parents prioritise educational value in media while others place an emphasis on the entertainment value. These preferences for choosing media are partially influenced by individual characteristics [139, 140]. When selecting apps for children, parents will choose apps that will provide independent entertainment, co-education, tailored content and challenges, children's familiarity with the app, and pass time [22].

There is little to no research investigating parents' behaviour with respect to data protection or privacy in choosing children's apps. While parents are concerned about children's privacy, they primarily focus on other factors, such as content [23]. This shows that there is research to be done in this space, to understand how parents assess privacy risks in apps and how we can empower them to make intelligent decisions.

2.2.4 Summary

We examined the concept of privacy and its importance for children. We began by reviewing four popular theories of privacy - Westin, Altman, Nissenbaum, and Livingstone - which provided different perspectives on privacy and the factors that may affect it, such as technology, social and cultural norms, and the context in which personal information is collected, used,

and shared. We then considered the ICO's Age Appropriate Design Code (AADC), which is a comprehensive data protection framework that sets out specific requirements for the collection, use, and disclosure of personal information in apps and other online services that are aimed at children. We used the AADC as a benchmark to understand other common frameworks used in practice. Finally, we examined the importance of privacy for children and how their understanding of privacy may differ from that of adults and be influenced by a range of factors, including age, developmental stage, and social and cultural context. By considering both the AADC and privacy theories, we gained a thorough understanding of the complex issues surrounding privacy in the context of mobile apps and how they may impact children. This included understanding the various ways in which personal information may be collected, used, and shared and the factors that may affect privacy, such as technology, social and cultural norms, and the context in which personal information is collected, used, and shared.

We have explored what privacy considerations should be taken into account when developing apps for children. In the next section, we will examine the ways in which apps behave with respect to privacy and data tracking, and how these practices may impact children's privacy.

2.3 Data Tracking and Privacy in Mobile Apps

The use of digital products and services by children has significant privacy implications, as the data traces are increasingly owned by the private sector [141]. The amount of information and personal data being collected by commercial organisations has far exceeded the capabilities of governments [92]. The methods which enable this form of mass surveillance include invasive techniques such as cookie-placements, advertising identifiers, and web-beacons [142, 143]. Children surrendering their data is often non-negotiable, as they are nudged into disclosing more data than is required [144, 145] or are forced to disclose their data to access a service [146, 115].

This section describes exactly how tracking in mobile devices happens and its relationship to the advertising industry. We also discuss regulatory responses and harms arising from such practices for children.

2.3.1 Tracking: A Working Definition

Tracking can be defined as the collection and collation of data from multiple distinct contexts and the use of that data outside of these contexts, where a context is a set of resources controlled by the same party [147]. Originally this definition, proposed by (W3C)'s Tracking Protection Working Group, was meant for the web. However, this definition can be practically used across various devices and mediums [143], including mobile, which our focus will be on. Tracking originated on the web, with the advent of web browsers and the introduction of the 'Cookie', which allowed developers to store small amounts of information on the web browsers [148]. Its original intentions were possible benign, as developers wanted to keep track of users and their behavioural activities on websites to enhance performs. As cookies are sent back to the web server while the user is navigating the various pages on a website, the server can collate these distinct page visits into a single user session. Cookies provided benefits for both developers and users. For example, cookies would allow users to remain logged into certain websites after closing the browser.

Since the introduction of cookies, tracking has come a far way. Nowadays, cookies as a means of tracking are used for large scale analytics, advertising, and other things. Furthermore, tracking also occurs outside of web browsers, such as in smartphones and IoT devices. Our focus will be on tracking in mobile devices. We begin this section be explaining how tracking on mobile devices work and the role of third-party SDKs.

2.3.2 Tracking on Smartphones

Tracking on mobile devices is easier than tracking just on web browsers. One might argue that is easier to do tracking on mobile devices than on web browsers, as mobile devices open up additional tracking vectors, such as permissions and advertising identifiers. Mobile devices primarily run one of two operating system, iOS by Apple [149] and Android by Google [150]. Users primarily interface with mobile devices through applications (or 'apps' for short). Apps are mostly programmed through OS specific environments and languages (Swift for iOS and Java for Android), and they often have access to underlying data presented to them by the OS.

Web browsers on mobile devices form just one sort of application that is available. Tracking through web browsers on mobile devices is similar to how it is performed on traditional devices such as laptops and desktop

computers. However, mobile devices often have more than app installed, and each app has the potential track and distribute data. Importantly, as mobile devices become more sophisticated they also have more sensors embedded in them. For example, smartphones and tablets these days have multiple sensors available, such as a gyroscope and accelerometer, and also often have GPS capabilities.

As such, apps are run in a sandboxed environment, meaning that apps cannot individually communicate between each other. However, apps do have access to other types of data present on the device. In order to access data or certain functionalities, developers must request permission from the the operating system. In Android, these permissions are declared during development in the manifest file, `AndroidManifest.xml` [151]. Some of these permissions are considered "normal permissions", which does not require consent from the end user to be accessed [152]. Then, there are also "dangerous permissions" or "runtime permissions", which Google considers to be sensitive, such as Microphone or Camera access, where the user needs to give explicit consent/permission for the app to use these [152, 153]. Given these permissions, apps are relatively free to run any code they like within the limits of the sandbox. This also means that they can open network connections to distribute any data they might have collected from the device. If a user has given GPS access, the app might send back to a web server the exact GPS coordinates of a user over time.

It is common practice for developers to make use of code developed by third parties. These are called 'libraries' or 'Software Development Kits' (SDKs). Third party-libraries are used for a variety of reasons, because they simplify development, provide increased functionality, and may be more secure than proprietary software modules [154]. As a result, the use of third-party libraries is unavoidable in today's landscape of app development [27]. Third-party libraries within an app behave as if they were developed by the first party. This means that once permissions have been granted to an app to access specific resources, the third-party libraries also have access to this data [155, 156]. Such libraries also have permissions to collect sensitive data [8, 9] and they frequently access location permissions. In addition, developers sometimes request more permissions than needed due to a lack of clarity about the scope of certain permissions or third-party library requirements [157]. Unfortunately, there is no way for the user to give permission access to an app while withholding this permission from third-party libraries. As discussed more in depth below, data tracking through third-party libraries is

currently pervasive in the mobile ecosystem.

2.3.3 Unique Identifiers

Apps have fine grained access to system level settings through permissions. In some cases, these permissions are granted even without user consent. In the early days of mobile devices, apps used all sorts of data and resources to keep track of users. Often these resources were hard wired into the device, such as the IMEI (International Mobile Equipment Identity) number, IMSI (International Mobile Subscriber Identity), and MAC address. These identifiers are particularly powerful, as they are hard to change or reset, meaning that once an entity has access to these identifiers, they can continue tracking users without any issues. As a result, both Google and Apple introduced specific identifiers for the purpose of advertising. In Android, this is the AAID (Android Advertising ID) and on iOS this is the IDFA (Identifier for Advertisers). These identifiers are meant to be associated with a user's device, but can be reset by the user if they wish to do so. The AAID is available to all apps (and third-party libraries embedded in apps) on the device, without requiring permissions or special consent from the user.

Both Android and iOS have systems in place to limit access to the advertising identifiers. On Apple devices, from iOS 14 onwards, Apple implemented the Apple Tracking Transparency (ATT) framework. ATT requires developers to request explicit consent from users before accessing the IDFA. Users are prompted with a consent dialogue, in which they can choose to allow 'allow [the app] to track your activity across other companies' apps and websites'. Under this new framework, it is estimated that over 60% of the users choose not to be tracked [158, 159], which has led to a lot of criticism from major technology companies which rely on targeted advertising for their revenue (most notably Facebook).

On Android, such consent is not explicit, and deep in the Android privacy settings users have the option to 'opt out of personalisation', which is enabled by default. However, before 2021, even if users opted out of this setting, developers technically still had access to this information through the developer API. They were only enforced by Google's policy to not use this identifier for advertising purposes, which meant that it could still be used for other purposes, such as attribution and analytics. Since 2021, Google updated this policy to block API level access on a technical level and "[a]ny attempts to access the identifier will receive a string of zeros instead of the

identifier" [160]. Despite this, the setting to opt out is difficult to find in the Android settings and many users are not aware of it. Less than 17% of the users had actually opted out of personalised advertising, while 30% mistakenly assumed that they had opted out [161].

2.3.4 Tracking Detection

Over the past decade, the mobile infrastructure has created the potential for large scale tracking by third parties in apps. Generally speaking, the tracking ecosystem has not been very transparent, and it is nearly impossible for individual users to know how many third-party entities apps are sharing their data with and what data this is. Instead, research broadly use two methods to uncover what apps are doing in the background: *static* analysis and *dynamic analysis*.

Static methods analyse the source code of applications, for example to detect the presence of third-party tracking libraries [162, 163, 164, 165]. Static analysis has been a popular method to identify security and privacy leaks in software. However, static analysis does not allow for any factual observations of data tracking happening, as the code is not being executed. It does however produce a hypothetical upper bound of what is possible. The biggest advantage of static analysis is that apps can be analysed on a large scale. However, developers may choose to implement techniques to prevent proper code analysis, as the runtime behaviour of an app is different from what the code may suggest. Popular techniques for this are obfuscation and altering the program flow [166, 167, 168]. In addition, in some cases code is being rendered dynamically [169], meaning that static analysis would fail to detect this code.

Dynamic methods on the other hand analyse the app while it is executing (live), for example by inspecting its network traffic and identifying third-party destinations possibly related to tracking [170, 171]. The advantage of dynamic analysis is that it is possible to observe the real behaviour of applications. Still, some apps alter their behaviour when they detect that they are being run in a virtual or privileged environment [172]. It is therefore common to run apps on real devices and make use of a VPN to inspect the network traffic [173, 174, 175].

2.3.5 Tracking in the Mobile Ecosystem

Research into tracking has shown that third-party tracking is prevalent and happens on large scale [176]. The distribution of trackers is concentrated around a few large entities, with Google being the most prominent such entity, closely followed by Facebook. Over 85% of the Android apps are estimated to have third-party SDKs from Google embedded in them [177, 178]. A 2018 report by Privacy International showed that 61% of apps containing a Facebook SDK automatically sends data to Facebook the moment the app is installed, including data such as the Advertising ID, even if Facebook is not installed or the user does not have a Facebook account [179]. In general, apps contact multiple trackers the moment it is first launched [19].

Third-party trackers have permissions to collect and communicate all sorts of sensitive information [8, 9]. For example, they track call logs, browser history, and contact information, even if that was not the intended functionality of the app [180]. Studies have also shown that over the lifetime of app, it accumulates permissions, requesting additional permissions approximately every three months [181]. Data tracking is not any different or better for children's data, as apps in the "Family" category of the Google Play Store have shown to have the second highest number of data trackers associated with them [7].

A leading factor for the use of third-party libraries and trackers is that developers rely on targeted advertising for generating revenue [34, 35, 36], which in turn uses third-party libraries to collect targeted data. These advertising libraries often also collect sensitive data, such as location [182]. This data is sent to data brokers, organisations which collect and analyse user data, and sell it to advertisers. Paid apps which do not make use of advertising or give the impression of increased privacy to users, do not deliver a significantly reduced amount of data tracking and collection in their apps [183, 184, 185]. Third-party libraries not only collect data in free apps but also from paid apps [183, 186].

Addressing these trackers is not trivial on mobile applications, as Android and major other smartphone operating systems do not provide end users the freedom to control third-party tracking through apps. Users are therefore dependent on privacy regulations and app review processes of marketplaces [187] to protect them. Google and Apple can thus exert control over the third-party tracking ecosystem. However, review processes are not always transparent, and Google and Apple have thus far been poorly incentivised to

exert control over the data tracking ecosystem, as they hold a vested interest in the advertising industry [188].

2.3.6 Why Data Tracking and Sharing is so Pervasive

The need for data tracking in digital consumer facing products can largely be attributed to the 'attention economy' companies are competing for [67]. Ultimately, technology companies generate revenue by sharing personal data with advertisers, enabling them to refine their targeting strategies. This data is gathered through user interactions, providing valuable insights into individuals' interests and behaviours. Consequently, these companies prioritise user engagement, with the ultimate aim of accumulating more data.

Sean Parker, the former President of Facebook, raised concerns about the approach of maximising user attention to achieve these objectives [189]. He highlighted the potential impact on the cognitive development of younger users, emphasising the need for critical examination. As he explained, the philosophy of designing digital services was centred around: "How do we consume as much of your time and conscious attention as possible?" [189].

Within the domain of social media design, there are three primary commercial goals: increasing user acquisition, extending user engagement on the platform, and promoting higher levels of content generation and interaction [190]. Designers recognise that any measures to reduce user attention invariably lead to decreased revenue [191], which further underscores the importance of user engagement as a pivotal driver of these platforms' profitability.

Data collection in the digital realm operates in two key stages: the first stage involves gathering data to enhance user experience and platform retention through personalisation and persuasive design measures. This stage is primarily focused on improving user satisfaction and engagement. The second stage is centred around leveraging the accumulated data for targeted advertising, allowing advertisers to precision-target products and services. These two objectives, user satisfaction and revenue generation, guide the strategies of technology companies, ultimately shaping the experiences of users, including children, in the digital landscape. In short, increased time spent on devices mean increased exposure to advertising, which is how tech companies generate revenue [188]. In the next sections, we will be exploring these two stages in more depth.

2.4 The Attention Economy

Tech companies have a primary objective: to hook users and keep them engaged with their digital devices. The competition for individuals' limited attention and time is also often termed the 'Attention Economy' [192]. Achieving this is often realised by the implementation of reward mechanisms. Human responses to the allure of rewards are deeply ingrained, leading to the release of dopamine in the brain [193]. These rewards can take various forms, some obvious such as receiving a 'Like' or comment from another user, while others are more subtle, like indications that someone is typing. The anticipation of a reward is what triggers a small release of dopamine.

Children in particular are susceptible to such habit-forming rewards due to their innate inclination toward seeking immediate gratification, which is characterised by their developmental stage [194]. For example, children between the ages of 10 and 12 find it challenging to consider long-term consequences and prioritise immediate rewards over other essential daily activities, such as sleeping or eating [195].

From an evolutionary perspective, humans are naturally alert to external stimuli like noises and movements [196]. Tech companies capitalise on this by employing strategies to trigger this inherent alertness. These strategies are implemented in various forms, such as notifications and vibrating alerts. Children find it difficult to prioritise more important competing demands and, as a result, often respond promptly to the newest stimuli, reinforcing a habit of reacting to "the new" [197].

The implications of these persuasive design tactics can be profound, especially for children, as habits and routines formed in their formative years tend to persist into adulthood [190]. The concept of designing something with the intention to *persuade* someone, is aptly named *persuasive design*.

2.4.1 Persuasive Design

Interface designs that guide end-users into certain behaviours through interaction flows, are part of a larger body of research called persuasive design and nudging [198, 199, 200]. Persuasive design within HCI has varying interpretations and framings, depending on the context or the discipline within which it is applied. Some stipulate that all design is inherently persuasive, as designers intentionally directly or indirectly induce behavioural changes [201, 202, 203]. Such definitions of persuasive design often are limited the-

oretical discussions within academia and do not extend to the practical impacts within applications. Others propose persuasive design to be a separate method of designing interaction, aimed at making or preventing certain behaviours from happening [199, 204]. Persuasive design can produce benefits and social good, as it can help in reinforcing good habits and enforcing socially acceptable behaviour. However, more recently, persuasive design, especially amongst practitioners and the media, has come to be associated with ethically questionable principles to keep consumers hooked to products and devices [67, 205].

2.4.2 Dark Patterns

"Dark patterns" fall under a specific type of persuasive design, often associated with persuading users to perform actions which negatively affect them. The term was originally coined by the UX practitioner Harry Brignull to describe "a user interface carefully crafted to trick users into doing things they might not otherwise do" [206]. Brignull developed a taxonomy of 12 different types of dark patterns which he curated in his "hall of shame" [207]. Some of these categories include, *misdirection* (misdirecting one's attention to distract from something else) and *hidden cost* (adding unexpected charges during a a checkout process). Subsequent work has added patterns and proposed alternative taxonomies. Bösch et al. propose a classification of 8 "dark strategies" [208], uncovering several new dark patterns, such as *Privacy Zuckering* (you publicly share more than necessary) and *Bad Defaults* (the default settings are not favourable to the user). Mathur et al., through an empirical analysis of 11K shopping websites, uncovered 15 types of dark patterns which they describe through 7 broad categories grounded in psychological biases [209].

Dark patterns have not only been discussed in the HCI and privacy literature [208, 210, 204, 209], but they have also been widely reported on by consumer protection organisations [211], white papers [212], and the popular press [213]. The notoriety of dark patterns has led the European Union and data protection officers to identify specific common examples, such as privacy-intrusive default settings and illusory or take-it-or-leave-it choices, as non-compliant with the GDPR.

2.4.3 The Role of Data in the Attention Economy

The practice of data collection and sharing intricately connects with persuasive design, forming a cornerstone of the attention economy. The key concept is something called "personalisation", and it plays a pivotal role in shaping online experiences of users. App and game developers are able to collect large amounts of highly sensitive information about users. This data also includes real-world details, such as a user's voice, physical attributes, location, and their social network [214]. Developers also track in-app actions, allowing for the creation of in-depth profiles, which have embedded in them cognitive abilities and personality traits [214]. The data collected on users is fed through machine learning and artificial intelligence systems. These system learn when users are most likely to respond to stimuli from their digital devices. They dispatch notifications at the 'optimal time', i.e., when users are most likely to open them, with the aim of increasing open rates and engagement [215]. (We will see a similar concept being used for advertising, called "micro-moments"). This continuous cycle of data collection and profiling has become the norm in the digital landscape, a phenomenon called 'dataveillance' [11].

One of the problems with such personalisation systems is that they make assumptions about the characteristics and nature of children at a time when they are still experimenting with and establishing their identities. By interfering with this process, such systems not only observe the behaviour of children, but also participate in shaping it in a way to maximise commercial profits [216]. Without oversight and 'scientific neutrality', a child's life and their opportunities will increasingly be affected by such 'social sorting' mechanisms [11].

2.4.4 Harms Arising from Persuasive Design and Data-Driven Personalisation

This intricate interplay of data and persuasive design shows the potential for profound implications on children's development and well-being. We look at some of the issues and harms arising from this below.

Mental Health Impact

There is a growing body of evidence highlighting the adverse impact of the intertwining of persuasive design and data-driven personalization on children's mental health. This convergence has been associated with a range of detrimental effects, encompassing mood disorders, diminished well-being, and the exacerbation of existing mental health conditions among teenagers [65]. Internal research from Facebook, disclosed by whistleblower Frances Haugen (who was introduced in Chapter 1), has shown that among teenage girls experiencing suicidal thoughts, 6% in the US and 13% in the UK, attribute these thoughts to Instagram [1]. Additionally, a third of teenage girls believe that Instagram negatively affects their body image [217].

Interpersonal and Behavioral Challenges

Beyond concerns about mental health, online sharing culture has resulted a range of interpersonal issues. These include feelings of self-doubt, anxiety, and a decline in self-esteem, as well as an increase in interpersonal aggression and cyberbullying [218]. In the UK, approximately 1 in 8 social media users aged 11 to 16 report being victim of cyberbullying. Among those with a 'probable mental disorders', this is reported to be over 25% [219]. Similarly, in the US, almost half of teenage girls reported being victims of cyberbullying in 2022 [220].

The health issues also manifest in various physical and behavioural forms. A 2019 study demonstrated that approximately 25% of children and young people display problematic smartphone use, akin to addictive behaviour [221]. This conduct is strongly associated with detrimental mental health symptoms like depression, anxiety, elevated stress levels, and sleep disruptions. Notably, younger individuals are more susceptible to developing mental health issues, and issues stemming from childhood can have enduring impacts on an individual's life [221]. Such consequences have been reported in other studies as well. It has been shown that excessive internet use detrimentally affects a person's general welfare, resulting in consequences like isolation, self-neglect, unhealthy eating habits, and increased family conflict [222]. Moreover, a study conducted with adolescents aged 10 to 16 in the UK identified a significant positive connection between problematic internet use and substance abuse [222].

Cognitive Development and Digital Addiction

Finally, longitudinal studies show a strong correlation between habitual 'checking behaviours' and alterations to the "neural sensitivity to anticipation of social rewards and punishments" in the brain [223]. Children feel that they are addicted to the Internet and cannot put down their devices [224] and describe a sense of feeling 'obliged' and 'panicked' [67].

2.5 Advertising

Many of the apps offered on the Google Play Store and the Apple App Store are free to be installed by users. However, this does not mean that money is not being moved around. The most popular way for developers to monetise their apps is through advertising [34], with estimates suggesting that over 77% of the Android apps contain a form of advertising [225, 226]. Since the early 2000s, with the introduction of programmatic advertising, the industry has grown to generating around $60 billion of revenue per year [36], with many different entities participating, collecting, and analysing large volumes of data [35].

Advertising nowadays is highly tailored to individuals. For a lot of tech companies, such as Facebook and Google, advertising is their primary source of revenue. Their advertising objective is to maximise the probability that a user clicks on an ad. This is done by ensuring the ads are relevant to a user and appear at a moment that they are mostly likely to engage with them. These tailored ads are also called *targeted ads* and are a result of something called *behavioural* or *programmatic advertising*. This type of behavioural advertising is believed to increase conversion rates and profit revenues [227]. In addition, it has the advantage that less money is being spent on advertising targeted at the wrong or irrelevant consumers, which is considered to be a flaw in traditional advertising methods as seen on TV or radio [228].

2.5.1 The Relevant Actors

The advertising industry is vast and complex network consisting of many different actors. The actors in the adtech industry can broadly be separated into four categories [229]. These categories are not mutually exclusive, as some actors take up various different roles. The categories are: major platforms, third-party vendors, marketers, and publishers.

Publishers are the entities providing digital services where consumers may directly interact with ads. This can range from anything such as websites to music streaming services. In our context, the publishers are the app developers. *Marketers* are the entities who wish to have an ad placed to influence consumers. Examples include, retail stores, travel agents, politicians, and telecom. Publishers and marketers are not mutually exclusive, as publishers may become marketers as well. For example, in many cases app developers may place ads for users to persuade them to install their other apps.

In between publishers and marketers sits a vast network of interconnected entities known as *third-party vendors*, such as advertising networks, analytics vendors and data brokers. These entities form the bridge between marketers and publishers, and process vast amounts of personal data to ensure the right marketer and ad, reaches the right publisher and consumer. Publishers and marketers have little control of this and consumers are often not aware of how this data is being processed [230].

Lastly, the *major platforms* are the big technology firms consumers are generally familiar with: Google, Facebook, Twitter, etc. These entities often take on multiple roles within the adtech infrastructure. For example, Google acts as a publisher when advertising on YouTube or their search engine. Similarly, Facebook and Twitter also act as publishers when showing sponsored content. At the same time, these major platform also fulfil roles as third-party vendors. For example, Twitter had their own advertising platform called MoPub, which was acquired by AppLovin [231]. Similarly, Facebook runs an advertising platform [232] as well as an audience network [233], and Google takes up multiple roles as third-party vendor through services such as Google AdMob [234, 235].

The third-party adtech vendors are collectively responsible for providing the technical infrastructure which allows for this data exchange to happen. All these entities are all committed to ensuring that the probability a consumer clicks on an ad is maximised, through analysing vast volumes of personal data and delivering highly targeted ads [236]. There are even specific entities, called *data brokers*, whose role it is to simply collect, analyse and distribute data to further third- and fourth parties. Data brokers typically do not obtain their data from consumers directly, but rather purchase it from other companies for purposes of analytics [237]. Data brokers have been collecting vast amounts of personal data from millions of consumers over the course of many years [238]. This data is used to create highly sophisticated profiles of users, containing data such as gender, age,

habits, race, political opinions, sexual orientation, and website visits, which are then sold or licensed to other third-party vendors for purposes of advertising. Consumers are categorised according to *audience segments* of people sharing similar characteristics. These are then used to score consumers according to their perceived value for advertisers [239]. Data brokers may have more than tens of thousands of different audience segments [238]. As an example, Adobe lists over thousands of health related audience segments on their website [229, 240]. Data brokers may get their data from a variety of sources, including credit card companies, financial institutions, and other data brokers [241]. The advertising industry has become so lucrative that big tech firms have spent a significant amount of money acquiring adtech companies [242].

2.5.2 Real-Time Bidding (RTB)

When an ad is being displayed in an app and seen by the user, called an *impression*, it is probably underpinned by a complicated process called *real-time bidding* (RTB). Publishers offer auction remnant ad space on an open auction while hundreds of parties bid to have their ad placed on that space in a matter of milliseconds. The highest bidder wins the ad space and has their ad placed on the user's screen. This happens so quickly that by the time a user opens and loads an app, the ad is often already there. In this short time span, large volumes of data are being exchanged and analysed.

There are several different actors involved in this process. *Supply side platform* (SSPs) collect and aggregate information of ad spaces and consumers to auction it to the highest bidder [243]. *Demand side platforms* (DSPs) buy these ad spaces from the SSPs for the purpose of showing relevant ads to users. When an app needs to load an ad, a *bid request* is broadcast through the SSPs to various DSPs on an open auction. This request contains data about the user, including the device, app, geolocation, and various other identifiers so data brokers and other entities involved in the RTB process may identify the individual. This means that data that is transmitted through the bid request is collected by other third-party vendors apart from the DSPs.

Advertising modules are integrated in apps through SDKs. Generally, developers choose advertising mediation platforms, which connects to multiple advertising networks on behalf of the developers. This way, developers do not need to integrate a different SDK for each advertising network. The ad-

vertising networks must compete for the app's inventory and only the highest bidder has their ad displayed [244].

The RTB process means that all entities involved in the adtech, from developers to marketers, are all incentivised to gather and compile highly sophisticated profiles of users. It is unsurprising that the digital advertising industry is a multi-billion dollar industry. For example, Google's main source of revenue relies on advertising, with 80% of its revenue, $147bn, stemming from advertising [245], of which more than half is from mobile devices [246].

2.5.3 The Role of Data in Advertising

In today's advertising landscape, data plays a central role, driving effectiveness and emphasising a data-driven and performance-oriented approach. Digital advertising leverages data to analyse online user behaviour, enabling the creation of personalised and precisely targeted messages that are more relevant to individual consumers [247, 248, 249]. Advertisers use techniques like behavioural and facial recognition to infer consumer emotional states [250]. They pinpoint optimal moments for delivering ads, known as "micro-moments," to maximise impact. This approach allows advertisers to tailor messages to the unique characteristics of users [251, 252].

This high level of personalisation helps in establishing lasting interactions with child consumers. Aligning commercial messages with consumer interests and behaviours helps in developing a positive brand attitude, as messages are perceived as less intrusive and more relevant, ultimately increasing purchase intent [253, 254]. In general, behavioural targeting and advertising result in higher click-through and improved conversion rates [255].

To achieve this level of personalisation, apps often collect and share personal information with third parties. In turn, the extensive profiling conducted by advertisers helps them create sophisticated audience segments. Large data controllers can exploit these segments to target vulnerable individuals, such as teenagers with low self-esteem, victims of specific traumas, or children interested in sensitive topics [256, 257, 258]. The enhanced relevance of such advertising, combined with children's limited understanding of it, can subconsciously influence children in adverse ways [259].

2.5.4 Children and Advertising

In the context of advertising and children, research indicates that young children, specifically those aged 7 and under, have limited comprehension of the persuasive intent behind advertisements [260]. It is only between the ages of 7 and 11 that children begin to recognise television advertising, often with parental guidance, but may still struggle with understanding advertising as a broader commercial concept [260]. Moreover, the recognition of persuasive intent does not necessarily translate to the ability to resist marketing, especially for products that are highly appealing. Marketers often employ emotional or subconscious tactics, including trusted characters and celebrities[261], to engage young consumers [262]. This is particularly effective, as children as young as 2 can identify with such characters [263].

In the digital age, advertising has become more integrated and interactive, blurring the lines between media content and advertisements, making it challenging for children, especially the very young ones, to distinguish and critically assess advertising [264].

Modern Internet marketing practices, including "advergames," have emerged, where users are rewarded for watching ads or making purchases [265]. However, some of these practices are less overt and may include hidden ads within children's apps, such as interstitial ads and ads that provide in-game incentives, often encouraging in-app purchases [266].

Children, particularly preschoolers, are considered vulnerable to advertising's influence due to their limited consumer socialisation skills [260]. Advertising literacy, a crucial aspect of consumer socialisation, pertains to a child's ability to recognise and critically evaluate advertising. It tends to improve with age, with older children showing a better understanding of advertising [260, 267].

2.5.5 Harms Arising from Advertising

2.6 Discussion

2.6.1 Key Findings

In this chapter, we have explored important aspects of privacy in the mobile ecosystem. We began by looking at popular theories of privacy, such as Westin, Altman, Nissenbaum's CI, and Livingstone, which provided different

perspectives on privacy and the factors that may affect it, such as the role of technology, social and cultural norms, and the context in which personal information is collected, used, and shared. We found that Livingstone's three dimensions of privacy - interpersonal, institutional, and commercial - provided us with an initial grounding in conceptualising privacy in the modern digital age of mobile apps. These dimensions helped us to understand the different ways in which personal information may be collected, used, and shared and the factors that may affect privacy, such as social and cultural norms, technology, and the context in which personal information is collected, used, and shared.

We then examined data protection frameworks to look more concretely at how these aspects of privacy should be implemented. We reviewed five leading frameworks from regulatory, private, and human rights organisations, with a focus on parts of the frameworks related to data collection and processing and the recommendations for how these practices should be made clear in apps. By considering these frameworks, we were able to gain a more complete understanding of the specific requirements and expectations placed on developers when it comes to protecting children's privacy in apps.

We then examined data protection frameworks, including the ICO's Age Appropriate Design Code (AADC), which set out specific requirements for the collection, use, and disclosure of personal information in apps and other online services that are aimed at children. We also considered the importance of privacy for children and the ways in which their understanding of privacy may differ from that of adults and be influenced by a range of factors, including their age, developmental stage, and social and cultural context. By considering these issues, we gained a comprehensive understanding of the complex issues surrounding privacy in the context of mobile apps and the ways in which these issues may impact children.

Having gained an understanding of how privacy should be implemented in apps through the review of theories and data protection frameworks, we next examined how apps behave in practice. We found that data tracking is prevalent in many mobile apps, including those aimed at children, and that such practices may have negative consequences for children's privacy. We looked at the ways in which personal information may be collected and shared through data tracking, the ways in which these practices may impact children's privacy, and the potential risks and negative consequences that may arise from such practices.

Lastly, we turned our attention to the role of developers in creating apps

for children. We found that there is a lack of research examining developer behaviours and practices in app development, particularly in relation to children's privacy. This lack of research is a significant gap in our understanding of the ways in which developers may impact children's privacy and the steps that can be taken to protect their personal information. We also found that developers may use techniques such as dark patterns and manipulative design to deceive or manipulate children into disclosing personal information or engaging in other behaviours that may compromise their privacy, and that such practices may have negative consequences for children's privacy. However, we also learnt that developers may not always be aware of these practices.

Especially with the introduction of the AADC, which sets out specific requirements for the collection, use, and disclosure of personal information in apps and other online services that are aimed at children, it is more important than ever to study the role of developers in creating apps for children for a number of reasons. First, developers have a significant impact on the privacy of children who use mobile apps. By designing and building apps that collect, use, and share personal information in transparent and appropriate ways, developers can help to protect children's privacy and ensure that their personal information is handled responsibly. On the other hand, developers who are careless or irresponsible with children's personal information may put children at risk of harm, such as identity theft, stalking, or other forms of abuse.

Second, understanding the behaviours and practices of developers is crucial for policymakers and regulators who are seeking to develop and enforce effective privacy protections for children. By understanding the ways in which developers may impact children's privacy and the challenges they face in building privacy-friendly apps, policymakers and regulators can better design and implement policies and regulations that balance the needs of developers with the interests of children and their families.

Finally, studying the role of developers is important for researchers and advocates seeking to understand the ways in which technology and digital media are shaping children's lives and to identify opportunities for positive change. By examining the behaviours and practices of developers, researchers and advocates can identify best practices and areas for improvement, and work to create a mobile ecosystem that is respectful of children's privacy and rights.

2.6.2 Revisiting Privacy and Being Privacy-Friendly

Throughout this thesis, we make use of the term *privacy-friendly* to refer to the way we wish apps to look. Using the ICO's Age Appropriate Design Code (AADC), a concrete understanding of how data is being tracked in mobile apps, and the aforementioned theories of privacy, we can conceptualise what we mean by a privacy-friendly app, with a focus on the dangers and harms arising from third-party data tracking. We conceptualise *privacy-friendly* along multiple axes.

1. From our analysis of data protection frameworks, we know that different regulatory bodies and marketplaces have different requirements for privacy in children's apps. For any app, product, or digital service, developers have an obligation to upholding these requirements. Therefore, we firstly include *privacy-friendly* to uphold these regulatory standards.

2. We also looked technically at how data tracking occurs in apps, and have found that apps routinely contain third-party data trackers to collect data for the purposes of analytics and advertising. We have seen how such behaviours can lead to concrete harms amongst children. Therefore, we secondly emphasise the need to minimise data collection in apps through the use of third-party trackers.

3. Lastly, we have also found that many services make use of dark patterns to persuade children into obtaining consent and disclosing more information than necessary. Therefore, we emphasise the need for a user facing component, which takes into account the affordances of children to negotiate their privacy preferences.

Broadly speaking, a privacy-friendly app would not use personal information for commercial purposes without properly negotiating this with children in a way that is age-appropriate. It would also not engage in practices such as targeted advertising or data mining that may compromise users' privacy for the benefit of the app or its developers.

However, we should also acknowledge that an exact definition of privacy-friendly will vary depending on the specific context, needs, and expectations of users, particularly children. While the AADC and the aforementioned theories of privacy provide a useful starting point for understanding privacy-friendly practices, they may not address every aspect of privacy in the context

of mobile apps or account for the unique needs and perspectives of different groups of users. For example, children's privacy needs will vary depending on their age, developmental stage, and socio-economic background. Some children may have more advanced understanding of privacy concepts, regardless of age, and may be able to make more informed decisions about their personal privacy preferences, whilst others may need more guidance and support. In addition, the definition of privacy-friendly may also evolve over time as technology and social norms change, and what is considered acceptable or appropriate in one context may not be in another. Therefore, it is important to approach the concept of privacy-friendly with a degree of flexibility and to be open to revisiting and adjusting our understanding of privacy-friendly practices as needed.

Despite the potential for variations in the definition of privacy-friendly, it is important to have a clear and consistent understanding of what it means in the context of mobile apps for children. In our work with app developers, using a combination of the AADC and the aforementioned theories of privacy can provide a useful starting point for defining privacy-friendly practices.

2.6.3 Research Gaps and Contributions

There are significant research gaps in our understanding of developer practices for privacy in children's apps. While there has been some research examining the ways in which apps for children collect, use, and share personal information, there is little information about the motivations, behaviours, and practices of developers in relation to children's privacy.

One research gap that we aim to address in this thesis is the lack of knowledge about the design choices made by developers when creating apps for children. It is not clear how developers understand and interpret privacy laws and regulations such as the ICO's AADC, or how they balance the need to protect children's privacy with other business goals and incentives. In Chapter 4 we investigate the design choices made by developers in relation to children's privacy and to identify factors that may influence such choices.

Another research gap that we aim to address is the lack of information about the requirements that developers need to be supported in creating privacy-friendly apps. It is not clear how developers engage with children and their parents to obtain consent for the collection and use of personal information, or how they communicate about privacy in general. In Chapter 5 we investigate the types of support and guidance that developers need

in order to create privacy-friendly apps for children, and to identify best practices for supporting such efforts.

In addition to these research gaps, we also aim to address the lack of information about the tools that developers need to create privacy-friendly apps for children. Few tools currently exist to support developers in this task, and there is little information about how such tools are used or how effective they are. Based on the findings from the previous steps, in Chapter 6 we develop and evaluate our own tool to support developers in creating privacy-friendly apps for children. This tool will be based on the best practices and guidelines identified through our review of existing data protection frameworks and our analysis of the ways in which developers can be supported in creating privacy-friendly apps.

By developing and evaluating our own tool, we aim to contribute to the existing literature on tools for supporting developers in creating privacy-friendly apps for children, and to identify any areas in which further development or improvement may be needed. Through this work, we hope to provide valuable insights and recommendations for policy makers, app developers, and other stakeholders who are interested in promoting privacy-friendly practices in the mobile ecosystem.

3

App-solutely Exposed: A Privacy Analysis of Children's Apps

Contents

3.1 Introduction 63

3.2 Literature Review 66

3.2.1 Methods 66

3.2.2 Results 70

3.2.3 Interim Discussion 75

3.3 Privacy Analysis of Children's Apps 78

3.3.1 Overview of the Method 79

3.3.2 User Facing Privacy Features 79

3.3.3 Third-Party Tracker Detection 80

3.3.4 Our App Analysis 81

3.3.5 Fourth-Party Tracker Mapping 83

3.4 Results 84

3.4.1 Privacy Features 84

3.4.2 Third-Party Tracking 89
3.4.3 Fourth-Party Tracking 91
3.4.4 Interim Discussion 93
3.5 Discussion 95
3.5.1 Summary and Key Findings 95
3.5.2 The Complexities of the Data Tracking Ecosystem 96
3.5.3 Challenges in Designing Privacy-Friendly Apps for Children 98
3.5.4 Limitations 100
3.6 Conclusion 101

3.1 Introduction

In Chapters 1 and 2 we had a preliminary look at what the mobile privacy landscape looks like for children and formulated several research gaps. In this chapter, we present our critical examination of how children's mobile privacy has been examined in existing research and implemented in practice [1]. This section provides a summary of the motivation and context, and reiterates the research questions.

To summarise our findings from Chapter 2, we saw that children have become avid consumers of media and information through mobile devices such as smartphones and tablets. They are spending more time on digital devices now than ever before [268, 15, 43], which has facilitated the creation of a market for mobile apps specifically aimed at children. Prominent app marketplaces like the Google Play Store and Apple's App Store have categories of apps dedicated to children. These categories often have headings such as 'Apps for children' or 'Games for children' and also allow children to filter by age groups ('Ages up to 5' and 'Ages 6-8') [5]. However, over the past decade, the use of mobile apps has come under increasing scrutiny due to their large scale and systematic practice of collecting and sharing sensitive personal data [8, 9, 269, 7]. It seems that in today's app market,

[1] This Chapter has been published as: Ekambaranathan, Anirudh, Jun Zhao, and George Chalhoub. "Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 7.2 (2023): 1-24.

data tracking and loss of privacy have become almost inevitable, largely due to the presence of third-party libraries and advertising modules [7], which are considered essential for development [270]. Despite the presence of such trackers, it has also been shown that apps do not sufficiently allow for children to negotiate such privacy practices, for example through consent and notices [19]. This is particularly concerning for children, as their understanding of digital risks is not as developed as that of adults [15]. For example, children may not fully understand how their data is collected or why it is useful to third parties [115, 116]. Privacy is a crucial element for child development, as media literacy skills play an important role in developing skills such as responsibility, trust, autonomy, and critical thinking [98, 99, 100, 101].

As a result, privacy issues associated with large scale data tracking has become a priority for regulatory bodies responsible for protecting consumers' data and privacy. For example, the EU introduced the General Data Protection Regulation (GDPR) [16] in 2018, and in the UK the Information Commissioner's Office (ICO) introduced the Age Appropriate Design Code (AADC) [17] in 2021, forcing products and services aimed at children to prioritise data protection as an integral part of their offering. The introduction of the AADC mandated specific requirements in children's apps from the perspective of developers. For example, the AADC takes the stance that apps aimed at children must be transparent about the privacy practices in a way that makes it accessible for children. However, after a year since the AADC was introduced, it remains largely unclear whether apps are compliant with the code and what the state of privacy is in children's apps.

Therefore, in this chapter, we aim to sketch the landscape of mobile privacy for children from both a research and empirical perspective. We start with a literature review of recent studies of app privacy analyses to understand how privacy in apps can be and has been evaluated. We align this with the AADC to understand which areas of privacy in apps have been understudied. Through the review and analysis, we establish our own method for evaluating app privacy, consisting of a technical and a user facing dimension. Next, through applying this method, we look at how privacy is currently considered in children's apps. First, making use of a cognitive walkthrough, we investigate what user facing privacy features are present in apps. For example, are children presented with a privacy notice that is bite sized and easy for them to understand? Secondly, we examine any data tracking that is happening in apps. By investigating this intersection of user facing and technical privacy, we aim to establish whether the data tracking

happening in children's apps is justified by the user facing privacy features. More specifically we aim to answer the following research questions.

RQ1 What privacy features are present in children's apps and to what extent can these apps be considered to be privacy-friendly in the UK market?

- 1a How is the privacy of children's apps evaluated in the research community, and how is privacy conceptualised in these evaluations?
- 1b What technical and user facing privacy features are there in children's apps for them to negotiate their privacy preferences?
- 1c What are the open challenges for building privacy-friendly apps for children?

To answer these questions, we first present a systematic literature review of 48 studies. Through this literature review we establish how different studies conceptualise privacy and which features they use to assess the privacy in apps. We found that the 'Privacy Policy' and need for 'Dangerous Permissions' are the most commonly used features to assess how privacy-friendly apps are. We found that there is a lack of focus on children's apps as well as user facing privacy features.

We use the findings of the literature review to inform our empirical app analysis method, which we subsequently applied to examine privacy features of 137 'expert-approved' children's apps from the Google Play Store. We performed a cognitive walkthrough to identify and establish what privacy features are present in children's apps. We complemented our cognitive walkthrough of the user facing features with a data tracking analysis. Through an analysis of the third-party trackers embedded in the apps, we mapped a part of the fourth-party tracking ecosystem onto a tracker knowledge graph. This graph shows data sharing relationship between entities involved in the mobile ecosystem. We show that by sharing data with a single third-party entity, it is possible for this data to reach over 2,973 fourth-party entities. In general, our analysis shows that there is a misalignment between the data tracking that happens in the background of apps and the support provided to children when they engage with the apps. Finally, we use the AADC as a baseline framework to assess whether apps can be considered privacy-friendly and what breaches are commonly occurring. We use this analysis to make

recommendations for future children's app development and to motivate the research we conduct in the following chapters.

This chapter makes several scientific research contributions. Firstly, we provide a comprehensive overview of the current state of approaches for assessing the privacy practices of children's apps. Our literature review identifies gaps in the existing research and highlights areas that require further investigation.

Secondly, we develop and apply a two-dimensional app analysis method that considers both technical data sharing practices (through a tracker analysis) and user-facing features in children's apps (through a cognitive walkthrough). Our analysis provides a detailed examination of the privacy practices of children's apps in a leading marketplace in the UK and how they may impact children's privacy.

Thirdly, we map our findings onto the AADC framework and provide evidence of how and where current children's apps breach the AADC standards. This helps to inform regulatory efforts and provides guidance for developers in creating apps that are compliant with the AADC.

3.2 Literature Review

In this section, we present a review of recent studies that conducted a privacy analysis of mobile applications. Our goal is to understand how app analyses are performed in the research community and to identify the features and methods used in these studies. By examining these studies, we can gain insight into how privacy is conceptualised in the process of conducting app analyses.

3.2.1 Methods

For our systematic literature review, we sought to identify articles that focused on performing a privacy analysis of applications. We maintained a broad focus without narrowing down on definitions of privacy, so that we could understand which aspects of privacy researchers focus on when analysing applications. We also did not exclude any app genres, to provide a snapshot of the types of apps which are currently receiving attention in matters of privacy.

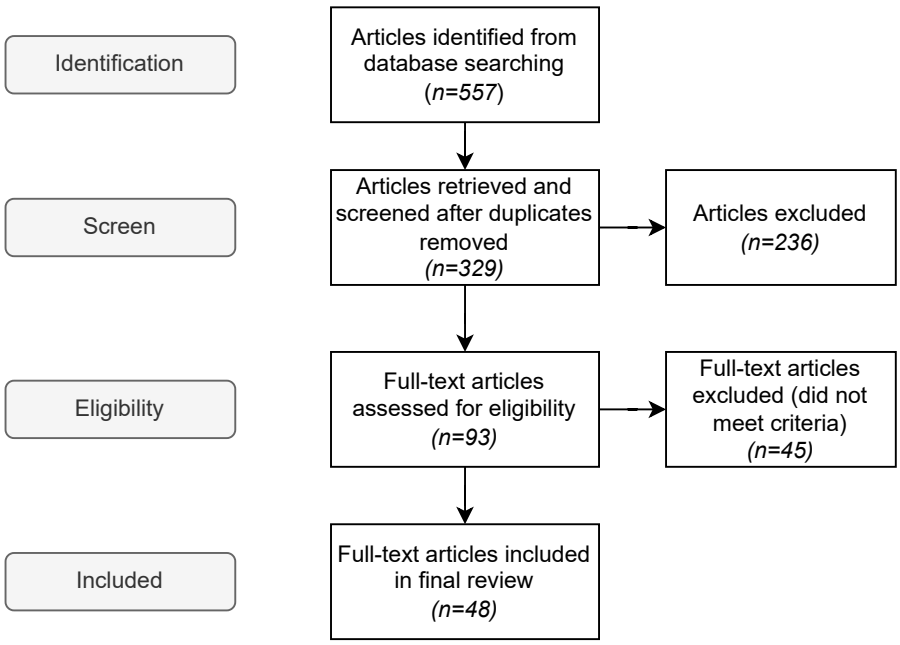


Figure 3.1: Our search strategy for identifying articles focusing on privacy analyses in mobile apps.

We guided our search strategy based on the PRISMA method (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [271]. As the mobile ecosystem is ever-evolving, we limited our search to peer-reviewed and English articles published from 2016 onwards. By retrieving articles which were recently published, we ensured that they were relevant and up to date with the latest developments in the rapidly changing mobile ecosystem. We searched four popular and reputable databases: ACM, Scopus, IEEE Xplore, and Web of Science.

We made use of the search term (*apps* OR *app*) AND *privacy*, and checked that this term is present in either the abstract or the title. This approach generated a comprehensive search that encompassed articles exploring various aspects of the connection between apps and privacy. We intentionally opted for a broad term because more specific queries, such as including terms like *children* or *evaluation*, yielded a highly restricted selection of articles. Therefore, we chose to broaden the search scope and subsequently conducted manual filtering to exclude any articles that did not meet our eligibility criteria.

We did not include word stems in our search criteria to maintain consistency and precision in the search results.

Upon running the search query, we retrieved 557 articles from the four databases and were left with 329 articles after removing duplicates. The screening and eligibility assessment was done by one researcher (myself). We screened each article by reading the title and abstract to ensure that articles performed an app privacy assessment. We excluded articles that perform user studies (for example, investigating privacy awareness or providing privacy education), developed or implemented privacy-performing methods for apps, developed a privacy specific app (for example, a tracker blocker), performed literature reviews, and other articles which did not specifically perform a privacy app assessment. After the screening phase, we were left with 93 articles which we read in full to assess its eligibility. We excluded 45 articles that: evaluated or proposed new app analysis tools [272, 273, 274], had unclear methodologies where it was not sufficiently explained how feature data was collected for it to be reproducible [275, 276, 277, 278, 279], we could not access or find [280, 281, 282, 283], focused on theoretical or conceptual matters [284, 285, 286, 287, 288], exploited specific security vulnerabilities with the purpose of leaking data [284, 289, 290, 291, 292], or were identified as duplicates (with different titles) [293].

In the end, we were left with a total 48 articles for the final review. Our search process is depicted in Figure 3.1.

Table 3.1: This table contains the results of our literature review. We make use of the following symbols: Android - ◐; iOS - ◑; Android & iOS - ●. We marked an evaluation as aimed at children's apps if they explicitly mentioned this in their methods.

Study	**OS**	**Kids**	**Genre**	**# Apps**	**Feature**
[294] (2016)	◐	●	Children	1,000,000	Data sharing features; Consumerism
[295] (2016)	◐	○	mHealth	176	Tracking; Privacy policy
[296] (2016)	◐	○	Popular	17,991	Privacy policy
[297] (2016)	◐	○	Unclear	900	Permissions; Tracking
[298] (2016)	◐	○	Random	1021	Permissions
[299] (2016)	◐	○	Popular	17,000	Permissions
[300] (2016)	◐	○	Popular	100	Tracking

[301] (2017)	◐	○	Arab	2,255	Tracking
[302] (2017)	◐	○	Unclear	10	Permissions
[303] (2017)	◐	○	Malware	168	Tracking
[304] (2017)	◑	○	mHealth; Fitness	72	Privacy policy
[305] (2017)	◐	○	Popular	15	Permissions
[306] (2017)	◐	○	Popular	2,800	Tracking
[307] (2017)	◐	○	Popular	261	Tracking
[308] (2018)	◐	○	Health	64	Privacy policy; Consent; Data access; Data sharing features
[309] (2018)	◐	○	Malware; Popular	4,500	Tracking
[310] (2018)	◐	○	Popular	500	Permissions
[311] (2018)	◐	●	Children	1,200	Privacy policy
[312] (2018)	◐	○	Popular	512	Tracking
[313] (2018)	◐	○	Popular	445,668	Tracking
[314] (2019)	◐	○	Fitness	10	Privacy policy; Permissions
[315] (2019)	●	○	(m)Health	36	Privacy policy; Tracking
[316] (2019)	●	○	mHealth	369	Privacy policy
[317] (2019)	◐	○	Popular	100,000	Hidden privacy settings
[318] (2019)	◐	○	Unclear	50	Permissions
[20] (2019)	●	○	mHealth	61	Privacy policy; Permissions; Data sharing features
[319] (2019)	◐	○	Random	28	Tracking
[320] (2019)	●	○	mHealth	116	Privacy policy
[321] (2019)	○	○	Dating	2	Data sharing features
[322] (2020)	◐	○	All	2,865,553	Permissions
[323] (2020)	●	○	German	225	Data access
[324] (2020)	◐	●	Locator	41	Tracking
[21] (2020)	◐	○	Open source	100	Permissions
[325] (2020)	●	○	COVID	41	Tracking

[326] (2020)	◐	○	mHealth	31	Privacy policy
[327] (2020)	◐	○	Popular	5,473	Privacy policy
[328] (2020)	◐	○	mHealth	27	Privacy policy
[329] (2020)	◐	○	COVID	7	Privacy policy
[330] (2021)	◐	○	COVID	39	Privacy policy
[331] (2021)	◐	○	COVID	9	Tracking
[332] (2021)	●	○	COVID	70	Tracking; Permissions
[333] (2021)	◐	○	Popular	2,500	Privacy policy
[334] (2021)	◐	○	COVID	28	Permissions; Privacy policy
[335] (2021)	◐	○	Health	497	Permissions; Privacy policy; Consumerism
[336] (2021)	◐	○	Health	36	Permissions; Trackers
[337] (2021)	◐	○	COVID	7	Permissions; Tracking; Consent; Tracking
[338] (2021)	◐	○	COVID	63	Privacy policy
[339] (2022)	◐	○	All	1,945,056	Permissions

Data Collection

In our analysis of the articles we gathered, we focused on two pieces of information. Firstly, as the aim of the literature review was to understand how app analyses are performed in the research community and to guide our own app analysis, we sought to identify the features that studies used for app analyses. In some cases, we found that studies used multiple features, such as data tracking and privacy policies, but in the majority of cases, studies used only one feature.

Secondly, we also collected metadata to understand and sketch the landscape of mobile privacy analyses in the research community. Specifically, we collected the operating system used to assess apps, the number of apps analysed, and the genre of apps which studies focused on.

3.2.2 Results

In this part we present the findings of our literature review. We first present the findings related to the metadata, after which we present commonly used features in app analyses.

Android vs iOS

We found that most studies focus on Android apps (39/48), one study focuses solely on iOS apps, and eight studies consider both Android and iOS. It is not always clear why some papers chose to focus on one platform over the other. These papers implicitly assume that the focus of the paper is on the Android operating system [294]. We found that studies chose to focus on Android primarily for three major reasons. Firstly, they indicated that the open source nature of Android gave them access to APK files and other important resources for analysis: "The reason we focused on the Android platform was because of the availability of APK files, which were publicly accessible or obtainable from other websites unlike iOS" [330]. Apple ecosystem is less accessible, making it a more difficult target for rigorous technical privacy analyses. Secondly, studies selected Android because of its large user base and "the reliance of many users on it for daily activities" [301]. Thirdly, studies selected Android simply because of the scope of the research question and aimed to investigate something specific related to android (e.g., [322]).

Studies which focus on both Android and iOS do not specifically indicate why they chose this, except when they aim to compare the differences between the two marketplaces [320]. Similarly, the study which focused on iOS [304] does not provide a reason why it did so, however it does indicate that the apps they selected are available across most marketplaces. This suggests that perhaps the researchers only had access to an iOS device, however this cannot be concluded definitively. We identified one study which does not specifically indicate the underlying operating system [321]. However, this study focuses on user facing data sharing features and they make the assumption that this is the same across the two marketplaces.

App Scope

We found that studies had a variety of ways to sample apps for their analysis. In many cases, the scope of the study dictated which genre of apps should be sampled. One of the most popular genres in our review was the 'Health and Mental Health' genre, which was selected by 11 studies. One of the main reasons why studies select health apps is the sensitive nature of the data that may be collected [320, 326] or that users of such apps are part of a vulnerable population who merit special protection. For example, one study states that such apps may target "people with dementia, whose cognitive impairment

puts them at increased risk of privacy breaches" [304].

From 2020 onward, there is a sudden rise and focus on COVID related apps. The specific focus of these studies are the nationally approved official contact tracing apps, motivated by a concern of what data is being shared by such apps. In addition, some studies indicated that privacy concerns slowed down the adoption of contact tracing apps, indicating the need to investigate them [337].

Apps which did not select a specific genre or focused on a specific demographic sampled from the most popular genres and top ranking apps (12 apps in total). However, the scale and method of doing so also differed per study. Four studies performed what we can consider 'large-scale' analyses, where they sampled over 100,000 apps. The largest study selected 2,865,553 apps [322]. In such cases, these studies aim to sample as many apps as possible. In cases where such large samplings are not possible, studies for example sample $\tilde{1}00$ apps from each genre [306].

In our review, we also kept track of studies which focus on children's apps and we only found three such studies [294, 311, 324], out of which one is focused on Family Locator Apps [324] and arguably less aimed at children rather than families. The other two studies provide two main reasons why it is important to focus on children's apps. Firstly, they indicated that children are increasingly becoming a larger market segment for mobile applications while privacy in this area remains unexplored [294]. Secondly, the responsibility of children's privacy is often put on parents, while children increasingly are online without parental supervision [311].

In studies which sampled apps on a large scale or from popular genres [296, 313, 340], the researchers would have undoubtedly sampled children's apps as well, however no specific mention of this is made in the articles.

Table 3.2: Commonly used features used for privacy evaluations in apps and their explanation. In the third column of the table, # refers to the number of articles making use of the feature.

Feature	**Explanation**	#
Tracking	Collection of unnecessary data by third-parties.	20
Privacy policy	Analysis of privacy policies in various ways, including readability and compliance.	19
Permissions	Analysis of permissions, including the use of unnecessary dangerous permissions.	17

Data sharing features	Features within the app which allows users to share data with other people.	4
Consumerism	The presence of in-app purchases and (targeted) advertising.	2
Consent	Whether the app asks for consent for data collection through a dialogue box.	2
Data access	Whether and how people are able to view the data they have provided.	2
Hidden privacy settings	Privacy settings which are hard to find/reach.	1

Privacy Features and Evaluation

In the privacy analysis of apps, studies maintained different conceptualisations of privacy and used different features to support this. Table 3.2 shows a list of all features used for the analysis of apps in our review and its explanation. We find that privacy policies and permissions are one of the most commonly used features, which is unsurprising as they are also the most readily available ones. For example, the privacy policy can often be retrieved without having to install or download an app. Permissions are sometimes available from the marketplace as well, or is available through the `AndroidManifest.xml` file [151].

The use of privacy policies is particularly common amongst studies which investigate mHealth apps [320, 20, 316, 315]. No specific reason is mentioned as to why privacy policies are selected as the main privacy feature, apart from them being used to assess to what degree information is shared and disclosed. A few studies do acknowledge that the practices outlined in a privacy policy may not reflect actual app practices, and therefore complement the privacy policy analysis with a network traffic analysis [315].

In general, using Privacy Policy as a feature, we have found that studies use different evaluation and analysis methods. We list the most commonly used methods to evaluate privacy policies in Table 3.3. We can see that varying levels of sophistication are used to assess privacy policies, ranging from automated and machine learning techniques [327, 333], to simply checking for the presence of privacy policies where this feature is used part of a larger analysis [330].

The most common used feature to assess the privacy in apps is what we labelled as 'Tracking', which is used by 20 studies. However, we do find a wide variety in the methods used to evaluate this feature. For example, while some studies look at the network traffic to find out what data is being transferred[331, 315], others focus on the input data entered manually by the user [295]. In many cases Tracking was evaluated alongside other features such as the Privacy Policy or Permissions [315, 337, 295], for example to evaluate how and whether the actual privacy practices aligned with the disclosed privacy practices [295].

There are also a few features which are less commonly used and serve to specifically cater to the scope of a study. For example, [323] sent out 30 GDPR Data Subject Access Requests and investigated how vendors responded to them. They used this is as a feature to understand how users can exercise their privacy rights. Another example is the identification of hidden privacy settings (privacy settings which are not present in the usual location) [272], which is only found in one study.

Table 3.3: Showing common evaluation methods using 'Privacy Policies' as a baseline feature.

Evaluation methods using Privacy Policies	**Articles**
Automated methods of assessing app compliance with privacy policy.	[327, 333]
Assess the privacy policy according to several heuristics	[315]
Evaluating the accessibility based on word count, summary, headings, lay language, etc.	[20, 311]
The presence of a privacy policy (yes/no).	[330]
Using manual heuristics to analyse whether privacy policies are compliant with GDPR.	[338, 334]
Researcher judgement to assess the privacy based on privacy policy.	[20]

Table 3.4: Showing common evaluation methods using 'Tracking' as a baseline feature.

Evaluation methods for Tracking	**Articles**

Data leakage caused through inter-app communication.	[307, 309, 319]
Location data sharing and collection.	[325, 336, 306]
Analysis of the network traffic flowing out of the app.	[331, 315]
Analysis of apps adhering to the principle of minial data collection.	[337]
Inconspicuous data exfiltration against marketplace guidelines.	[324, 301, 300, 312, 313, 297]
Manually entered data by the user (e.g., through forms).	[295]
Other forms of tracker analyses, such as the identification of third-party libraries.	[337, 336]

3.2.3 Interim Discussion

Our literature review of past research performing app analyses has given us a broad overview of how app analyses are performed in the research community. We have identified features and their evaluation methods to inform our own app analysis, but we have also identified gaps in the literature where we can improve on. Firstly, we found that few former studies focus on children's apps specifically. While a few studies do correctly motivate that children merit special protections and are an under-explored demographic in privacy research, research in this area is still sparse.

Furthermore, our analysis also highlighted several privacy features that are are under-explored in the existing research, even though they are deemed crucial in the AADC. In the following, we show how we use the AADC as a baseline framework to compare the features which we identified in the literature review here, and to see how they align with what the ICO perceives to be important. In Section 2.3, we introduced how a recent study has revealed some crucial breaches of the AADC by a review of mobile apps [97]. Table 3.5 shows the mapping of these systemic breaches and the privacy features studied in the literature, highlighting the gap between research and regulatory practices.

Table 3.5: Mapping of privacy features observed in past research to the systemic breaches of the Age Appropriate Design Code.

Breach	**Feature mapping**

(1)Insufficient age assurance	None of the studies which we reviewed looked at age assurance as a part of privacy.
(5) Dark patterns and nudges	Studies which looked at 'Data sharing features' and 'Hidden privacy settings' specifically looked at dark patterns in user facing design features.
(6) Age-inappropriate financial pressures	We identified two studies which analysed 'Consumerism' in apps by evaluating the presence of targeted advertising and in-app purchases.
(7) Low default privacy settings	None of the studies which we reviewed looked at default privacy settings as a part of privacy.
(8) Excessive data sharing with third parties	Many of the studies used 'Tracking', 'Permissions', 'Privacy Policies', and 'Data sharing features' to assess how and to what degree data is being shared.
(9) Lack of transparency and excessive data sharing between services and third party login providers	While none of the studies look specifically at login providers, through 'Data sharing features' some studies do look at social media integration.
(10) Published terms are not age-appropriate	Many of the studies which used 'Privacy Policies' assessed the readability and accessibility of the terms and conditions as a way to assess privacy.

As shown in Table 3.5, the areas of the AADC which have received the most attention in the existing research are those related to excessive data sharing with third parties (8), which have looked into data sharing through four different features: 'tracking', 'privacy policies', 'data sharing features', and 'permissions'. It is important to note that while excessive data sharing with third parties is an important issue that should be addressed in research, it is also important to consider other areas of the AADC.

Meanwhile we can also see that certain critical areas are missing attention. To start with, none of the studies we examined looked specifically at age assurance mechanisms (1) and default privacy settings (7). On the surface,

age assurance mechanisms may seemingly not directly be related to privacy. However, they help to protect children's privacy by ensuring that they are not inadvertently sharing their personal information with others. For example, if a child is able to access a social media platform that is intended for adults, they may be more likely to share personal information with others without fully understanding the implications of doing so. Age assurance mechanisms can help to prevent this by verifying the age of users and ensuring that children are not able to access age-inappropriate content or services. If age assurance mechanisms are not adequately assessed in research studies, it can be difficult to understand the effectiveness of these mechanisms in protecting children's privacy and data protection.

Similarly, the AADC also emphasises the importance of low default privacy settings, as these give children the ability to control the extent to which their personal information is shared. Low default privacy settings, on the other hand, may make it easier for children to inadvertently share their personal information with others, which can have significant implications for their privacy and data protection. From a research perspective, the lack of focus on default privacy settings can also make it more difficult to identify any patterns or trends in the way that these settings are used, and to understand the factors that may influence their effectiveness in protecting children's privacy and data protection. This can limit the ability of researchers to develop effective strategies or interventions to address these issues and improve children's privacy and data protection online.

The last area of the AADC which we found to receive little attention in research is related to inappropriate financial pressure (6). We found two studies which evaluated this by looking at the presence of targeted advertising and in-app purchases. However, there are other example of this which can be considered, such as 'pay walls' and 'limited-time' features creating an sense of artificial scarcity. These types of techniques can be particularly manipulative and may be used to encourage children to make purchases or provide personal information in order to access certain content or features.

The mapping of our identified features with the AADC informs us how we can guide our own app analysis. Firstly, we find that few studies analyse children's apps specifically. Many studies have focused on general app usage or data collection practices, rather than specifically examining the ways in which children's apps may be collecting and processing data. This can make it more difficult to understand the specific risks and vulnerabilities that children may face when using these apps, and to develop effective strategies or

interventions to address these issues. With the introduction of the AADC, it is particularly important to understand the privacy design practices in children's apps in order to develop effective strategies for guiding developers. By gaining a deeper understanding of these practices, we can help developers create products and services that protect children's privacy and contribute to a safer and more secure online environment for them.

Secondly, we find that most analyses focus on evaluating technical features, particularly related to tracking. While tracking is certainly an important aspect of privacy and data protection to consider, it is also important to examine user-facing features that may have a more direct impact on children's privacy and data protection. User-facing features were largely concentrated around the analysis of privacy policies, which have received a lot of attention in research. However, it is well established that privacy policies are rarely read and that users often consent to them without reading them, as they prioritise accessing the service over their privacy [341, 342, 343, 344]. Therefore, it is important to consider other user-facing features that may have a more direct impact on children's privacy and data protection, such as age assurance mechanisms and default privacy settings. These features can help to ensure that children are able to negotiate the extent of data sharing and protect their privacy to a greater extent.

3.3 Privacy Analysis of Children's Apps

Based on our literature review, we propose a two-dimensional app privacy analysis consisting of both technical and user-facing components. Our method addresses critical areas of privacy which our review indicated to be understudied. We demonstrate how this method can be applied to the analysis of a selection of carefully chosen children's apps. Furthermore, we examine fourth-party tracking to illustrate the implications of losing control over privacy for children. Our proposed approach allows for a more comprehensive understanding of children's online privacy and data protection, taking into account both technical and user-facing factors that can impact children's privacy and data protection online.

3.3.1 Overview of the Method

We propose a two-dimensional approach to evaluating privacy in apps. Firstly, as discussed in Chapter 2, different design features, such as persuasive design or dark patterns, have been commonly identified in children's apps. However, as we showed in Section 3.2.3, there is a lack of systematic understanding of the application of these patterns in children's apps on the app market and how they contribute to the state of privacy. Therefore, for an effective privacy analysis, it is important to identify and assess embedded privacy features in children's apps.

Secondly, it is also important to consider the technical side of privacy related to data tracking and sharing. This can be done, for example, through the analysis of the presence of data trackers. The presence of trackers in apps means that children should be supported within apps to negotiate how these trackers behave, what data is collected, and how it is processed.

It is particularly important to balance a technical analysis with a user-facing analysis, as the potential for data tracking in apps by themselves do not necessarily indicate poor privacy in apps as long as children are sufficiently supported to negotiate these practices. By considering these two components, it is possible to better understand the privacy practices of an app and how they may impact children's privacy and data protection. This can be especially useful for developing regulatory interventions or guidelines for developers, as it allows for a more comprehensive understanding of the factors that contribute to children's privacy and data protection online.

3.3.2 User Facing Privacy Features

We draw on previous research in identifying features in children's app to inform our methodology [345] and thus propose the use of a grounded approach to identifying and compiling a feature list [346]. Furthermore, to ensure consistency in the way that data is explored, we suggest the use of a cognitive walkthrough process [347, 348], a common method typically used to assess the usability of systems. During a cognitive walkthrough, one or more evaluators work through a series of tasks using the system and ask a set of questions from the users' perspective. For the analysis of children's apps, this method can be used as an approach to simulate what a child would experience when they use an app. In the cognitive walkthrough, we suggest executing the following list of tasks:

1. Ensure that other applications are closed and launch the expert-approved application which is to be analysed.

2. Engage with the main content of the application and use it for a minimum of 5 minutes.

3. Explore all features using a depth-first search procedure from the home screen.

4. Navigate to the home screen of the tablet and let the app run in the background for a minimum of 5 minutes.

We recommend letting the apps run in the background as they may frequently share data through trackers in such circumstances. This is important for the second component of our method.

3.3.3 Third-Party Tracker Detection

Apart from the usable privacy features within the app, we also propose analysing the technical privacy behaviours of the app. By considering the technical elements, it is possible to identify whether there is a gap between the data tracking that is happening in apps and the ability for users to negotiate these behaviours. Based on the literature review, we found that the most common method for doing this is by analysing the presence of trackers. There are several methods that can be used to detect third-party trackers in apps.

Code review. One approach is to manually review the code of the app to identify any third-party tracking libraries or SDKs that may be included. This can be a time-consuming process, but it can provide a detailed understanding of the tracking practices of the app.

Static analysis. Another approach is to use static analysis tools to scan the app for third-party trackers [162, 163, 164, 165]. These tools can analyse the code of the app without executing it, and can identify any third-party libraries or SDKs that may be included.

Dynamic analysis. Dynamic analysis involves running the app on a device or emulator and monitoring the network traffic to identify any third-party trackers that may be sending or receiving data [173, 174, 175]. This can provide a real-time understanding of the tracking practices of the app,

but may not identify all third-party trackers that are included in the app code.

Third-party databases. There are also a number of third-party databases and tools that can be used to identify third-party trackers in apps [19]. These tools may use a combination of code review, static analysis, and dynamic analysis to identify trackers, and may provide a more comprehensive understanding of the tracking practices of the app.

3.3.4 Our App Analysis

In this section, we present an application of the above proposed method to analysing apps. For our own analysis we focus on children's apps, as our literature review showed that these apps are currently understudied.

Scope

In this study, we focus on so called 'expert-approved' apps from the Google Play Store's children genre [4], which is a category of apps targeted at children under the age of 12. According to Google, expert-approved apps have been specifically designed for children, and have been approved by teachers and children's media specialists to ensure they are 'age appropriate' and 'thoughtfully designed'. These apps are promoted by Google to enjoy improved protection, which may give the impression that they seem more safe for children to use. The Google Play Store does not provide a description about the exact methodology used to assess these apps by experts, nor how experts are chosen. We chose these apps specifically because of this duality: a strong campaign suggesting that they are intended and safe for young children, which is the focus of our study, while remaining opaque about its privacy practices.

Selecting Expert-Approved Apps

In March 2022, we scraped the Google Play Store children's category to create an initial dataset of 1038 expert-approved apps, along with their meta-data (developer, reviews, genre, category, etc.). The apps we scraped were directly accessible from the Google Play Store homepage by clicking on at most one link, such as 'Browse more apps like these'. We selected these apps as they are most likely to be visible to users. Subsequently, using the number of

reviews as an indicator, we sorted the apps according to their popularity. We ensure that we (i) selected a diverse range of apps by selecting at least one app from each genre and (ii) avoided apps from duplicate developers and studios (as they often tend to have similar design features and one privacy policy for all their apps). We also limited ourselves to apps which were free to download (due to funding limitations) and which clearly had an age rating. After this, we were left with 470 apps, of which we selected the top 150 most downloaded apps for manual analysis. During our analyses we encountered various issues with 13 of these apps. For example, several apps were not in English, some turned out to be premium, and a few did not open after installation. We ended with 137 apps in total.

Cognitive Walkthrough

For the first part of our analysis, we sough to identify and extract privacy related user facing features in our apps. For each app, we first started by launching the application and letting it naturally load or navigate to the homescreen. From there, we engaged with the main content of the app for a minimum duration of 5 minutes. We did this because often certain features only appear after a certain amount of time. For example, cross-promotion ads will appear towards the end of a game level. Next, starting at the homescreen, we explored all features within the app. We explored features by clicking on available buttons and made use of a depth-first search procedure. For example, after navigating to the 'settings' screen, we explored all features within this screen. Lastly, we navigated back to the homescreen of the tablet, while letting the app run in the background. This was necessary to detect any trackers which the app may contact while it is not active.

As we explored each app, we specifically looked for *design features* within the app which were related to privacy or may inform privacy aspects, such as features related to privacy policies or privacy settings. We recorded these features in a spreadsheet by tracking the apps column-wise and the features row-wise. We created a new row in the spreadsheet for each new feature which we had not encountered before.

We clustered the features into seven axes, related to their support of *privacy permissions, privacy policies, social networking, privacy settings, parental control, age assurance*, and *ads and in-app promotions*. We then performed several iterative rounds of coding to compare the codebook and document with more details about how the features were presented.

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

Third-Party Tracking

For our tracker analysis, we made use of a third-party tool called TC Slim, which can dynamically identify third-party trackers[2] [19]. Using the TC Slim app we identified all associated trackers and libraries for the 137 expert-approved apps. For each of the third-party trackers and libraries, we also read the API documentation and specifically looked for the need for special configurations when the API is used for children's apps. In such cases, the documentation often explicitly states than when apps are aimed at children or are part of the 'Designed for Families' programme in Google, that they need to add certain lines of code. For example, this is the case for the Adjust library [349], so that they are compliant with COPPA.

Technical Set-Up

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

3.3.5 Fourth-Party Tracker Mapping

In addition to these parts of our privacy analysis, we also sought to explore what the implications are of third-party tracking in apps. Specifically, we aimed to map the fourth-party tracking ecosystem. We define fourth-party entities as data sharing partners of third-party entities. For example, if a third-party entity, such as Unity, were to share this collected data with their partners, these partners would be considered fourth-party trackers. To do this, we first identified the most commonly occurring trackers in our dataset

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

of children's apps, which we found out to be Google and Unity. We read the privacy policies and legal documentation publicly available on their websites and specifically looked for any mentions of data partners to understand how data is being shared and to which entities it is being shared with. We found that Google has a list of over 1000 sharing partners, while Unity has a more manageable list of 71 partners. We used Unity's list of data sharing partners as a starting point to manually map a portion of the fourth-party tracking infrastructure.

For each of Unity's data sharing partners, we read the privacy policies and other legal documents publicly available on their websites in order to, in turn, determine *their* data sharing partners. In some cases, this information was not readily available. For example, a list of data sharing partners was simply not available anywhere on the partner website, or it was incompletely presented pictorially rather than textually. Oftentimes, we encountered the same partners from multiple sources, resulting in a dense network of data sharing partners. Subsequently, we manually cleaned up the data to reconcile naming differences from different companies.

Finally, we cross referenced companies with existing public knowledge bases, such as Crunchbase and Rocket Companies, to augment our dataset with additional metadata, such as the company's location, number of employees, target market, etc. Using this method, we created a knowledge graph of over 3000 nodes, representing data sharing relations between commonly used app SDKs and third- and fourth-party libraries.

3.4 Results

3.4.1 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*. For each of the themes we briefly describe the features associated with it, as well as how they presented themselves in the apps we analysed.

Permissions

During opening and using the apps, at times we were prompted with a dialogue box requesting certain permissions. In total, 24 apps requested various

permissions during or right after the app had loaded. Out of those, ten had a preliminary dialogue box explaining that the user would be prompted with a consent dialogue to grant permissions. They also explained why the permissions would be needed so that the user would be more likely to grant the permission. Two of these dialogue boxes contained a clickable url leading to the privacy one. One contained an address of a privacy policy which the user could not copy or click on and would have to manually enter in a web browser. One app was made using web technologies and requested consent to place cookies instead of requesting Android permissions. None of the permissions and their associated dialog boxes were age protected and did not require parental supervision. Children could grant permissions by simply clicking on the 'confirm' button without any restrictions in place.

Social

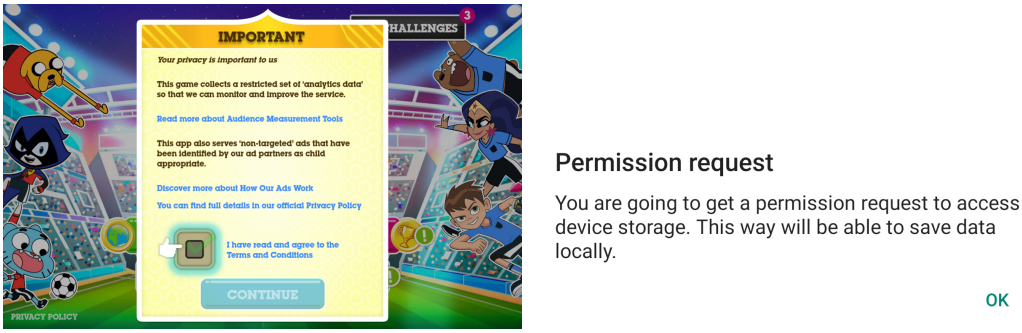
We encountered several apps making use of either social media integration or linking to various social media websites. In total, 15 apps had the feature to share content of progress made within the app through social media, of which four apps had this feature to be age protected. In addition, one app nudged parents to share in-app progress on social media. Sharing was possible through various apps, including email and commonly used messaging apps. Furthermore, we found 13 apps linking to social media platforms, by making the icons available on either the homepage or a secondary page. Only five of these links were age protected.

Upon launching the app, in five instances apps tried to automatically sign the user into their Google Play account. In our case, because we were making use of a child account, this was automatically prevented. In addition, two apps allowed users to optionally sign in using Google Play, and one app offered the option to sign in using a social media account.

Privacy Policies

We also kept track of where and how privacy policies were presented to the users. In total, 69 apps had a link to their privacy policy available within the app. We found no consistency in the places the privacy policy or the link to the privacy policy was embedded in the apps.

In the majority of the cases, this link was available in the settings page (35 apps), in 12 apps this link was available on the home screen, and in 11



(a) (b)

Figure 3.2: In (a) we can see children being nudged into accepting the terms and conditions, and privacy policy. In (b) children are being explained that they will face a permission dialogue box.

apps it was available in the 'about' or 'info' sections of the app. In eight apps there was a link which was presented to the user when the app was launched for the first time. In three cases the link was available during an introductory segment or a tutorial, however in these cases the privacy policy link font size was extremely small and tucked away at the bottom of the screen. However, we also found that 31 of the cases access to the privacy policy was protected by an age gate, meaning that they were not intended for children to see. We assume this is because privacy policies often needed to be opened by a browser, leading the user away from the app.

In 9 apps, the user was presented with a privacy dialogue, providing information on how their data would be used. However, in 11 apps, the user was required to explicitly agree to the privacy policy or the terms and conditions before being able to proceed using the app. In 3 of these cases, users were nudged into accepting these terms. An example of this can be found in Figure 3.2a.

Only 16 of the apps with a privacy policy, the policy was available within the app itself, meaning that user did not have to navigate to an external website to view it. However, only 7 of these apps had their privacy policies presented in bite sized sections in a way that aligned with what is described in the AADC [350]. One app had a specific privacy page which explained how data was being used.



(a) (b)

Figure 3.3: In (a) we can see that children are presented with advertising popups in which they are nudged into buying premium versions of the product to remove ads. In (b) we can see that children are being explained that the game contains IAPs, but that it requires adult supervision.

Privacy Settings

We also kept track of settings pages/sections within apps, as this is generally where one can expect to find options to view and delete any user data. However, we found that 40 apps had no settings page at all and 74 apps had a settings page without any privacy settings. In addition, 32 of these settings pages were age protected, meaning that they were not meant to be accessed by the children using them. Features related to erasing or handling user data were all related to the app content. For instance, we found features to 'delete all your progress' or 'reset the game', rather than features relating to user privacy settings, such as deleting the accounts on the servers. We found only 1 app which had the option to disable 'sending anonymous usage statistics to improve the service'. However, not only was this option enabled by default, but it was also protected by an age gate. In two instances, the user was presented with a consent box whether they would like to receive personalised ads.

A small minority of the apps had additional settings for users. Two apps had a settings page where the user could withdraw permissions granted to the app. And lastly, two apps had a contact form to get in touch with the developers in case of any questions.

Parental Controls

We parental controls and parental settings as in some cases developers might choose to reserve privacy features for parents rather than children. We found that six apps required parental supervision during setup. In these cases, apps either instructed children to call their parents or clearly indicated that this part of the app was aimed at parents. However, only in two cases the apps required parents to verify the use of the app through a Google Play parent account. In other cases, children would be able to technically proceed without parental supervision.

In 18 apps there was a parent specific section which was protected by an age gate. In most cases, these parts were similar to 'setting' or 'about' pages observed in other apps, but they often linked to other apps, for example allowing users to rate the app and leave reviews, and did not contain any privacy settings. In two apps, parents could set a maximum play time for their children, and in one app parents could set a pin code to access the app.

Age Assurance

During our cognitive walkthrough, we came across various age assurance mechanism to restrict children from different parts the app. For example, as mentioned above, in many cases children were restricted from accessing privacy settings or the privacy policy.

In total, we observed 13 different age assurance mechanisms used in our 137 apps. The most commonly used methods were: asking for the year of birth (12 apps), multiple choice maths question (11 apps), typing in or selecting the numbers which were displayed textually (11 apps), and a (non-multiple choice) math calculation (10 apps). Some of the methods were more robust than others. For example, six apps required the user to simply press and hold down a button while it filled up, and one app simply asked whether the user was over a certain age (yes/no button). Seemingly, the most robust method, used by one app, required the user to enter both the age and date of birth, where the app would determine whether the age indeed matched the date of birth.

Ads, Cross Promotions, and In-App Purchases

Finally, we also kept track of advertisements and other monetisation features, as they are strongly tied to data collection and targeted analytics. We found

in general that apps strongly made use of advertising and cross promotions. In 11 apps we were presented with advertising popups to 'remove ads'. Upon clicking those it would automatically attempt to perform an in-app purchase. Since we were making use of a child account, these attempts were blocked by Google. One app showed an ad upon launching the app nudging the user to buy the premium version of the app in order to have all ads removed. One app also offered the option for the user to view ads in order to unlock more content in the game.

A further 46 apps made use of cross promotions by providing a link to other apps by the same developers, available in various parts of the app. Of those links, only 24 were age protected. In 12 apps we encountered a 'More apps' button or icon, leading us to a custom page displaying more apps by the same studio or developer. In 28 apps we encountered ads promoting the user to buy or install apps from the same developers. In 36 apps we found links leading to the Play Store to leave a review for the app. Only 19 of those links were age protected, and in six apps users were nudged into leaving a review.

We encountered in-app purchase attempts in 47 apps, which were age protected through Google and were actively prevented because we made use of a child account. In addition, 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 from making a purchase, for instance through an age gate.

22 apps nudged users into buying their premium versions and 3 apps had an ad offering their premium version upon starting. We found one app which had an age protected feature to donate to the developers, and one app which had an age protected link to an external webshop for users to make purchases.

Lastly, we found 7 apps which were privacy certified, e.g. through ESRB, Privo, or KidSAFE, however the apps did not make it clear what the implications of this were for privacy and data protection practices.

3.4.2 Third-Party Tracking

We furthermore kept track of third-party trackers while using and analysing the features. We found that 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 3.4 shows the distribution of the most commonly occurring

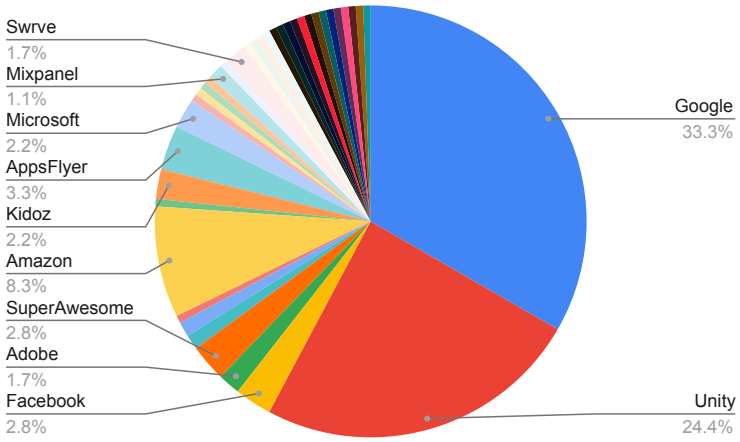


Figure 3.4: Distribution of most commonly occurring trackers in children's apps.

libraries which engage in tracking practices, including *advertising*, *analytics*, *fingerprinting*, and *social* functions (such as social media).

Google SDKs, such as Google Analytics, Crashlytics, and Google Ads are the most commonly occurring tracking libraries (33.3%). Surprisingly, several apps also had Facebook integrations (2.8%), 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 AppsFlyer (3.3%), SuperAwesome (2.8%), Mixpanel (1.1%), and Amazon (8.3%).

API Configurations

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[3]. It is not clear whether apps complied with this.

[3] `https://help.adjust.com/en/article/apps-for-children-android-sdk`

3.4.3 Fourth-Party Tracking

We were also interested in understanding whom the third-party trackers shared their data with, and so we mapped a part of the fourth-party data sharing ecosystem. To do this, we analysed 71 data sharing partners of Unity, as it was one of the most commonly occurring trackers, and it had a manageable list of 71 data sharing partners listed in their privacy policy.

Transparency and Accessibility

In trying to uncover the data sharing practices of fourth-party libraries, we came across several accessibility issues which are worth noting.

Almost all the company privacy policies which we analysed stated to share data with affiliates and business partners. However, we found that 37/71 of the companies did not have a list of their data sharing partners anywhere in the privacy policies or terms and conditions. Furthermore, 15/71 of the companies listed their partners pictorially on a separate page without any hyperlinks, meaning that it was not possible to navigate to their respective web pages without looking them up through a search engine. We also determined that 6/71 of the companies had an incomplete list of partners. We could infer this either through language in the privacy policy, which only gave examples of partners rather than a complete list, or through discrepancies between the number of stated partners on the website and the number of partners we could find on the website. For example, a company would claim to have over 200 partners, but we could only identify a handful anywhere on the website.

Companies did not specify what information exactly they shared with their partners, and the exact nature of the partnership was often not known. In general, we found that most companies made it difficult to access this information and often had it hidden away in the website.

Tracker Knowledge Graph

Using the 71 fourth-party companies from Unity as a starting point, we constructed a dense network of 2973 nodes and 14872 edges. An image of the data sharing partners of Unity alone is shown in Figure 3.5. From the whole network, the companies with the most number of data sharing partners are Xandr (1942 partners), Google (1067 partners), and Centro (163 partners).



Figure 3.5: The tracker knowledge graph showing the data sharing partners or Unity. The blue nodes are the direct partners of Unity, the green nodes are their data sharing partners in turn.

We also mapped the countries of incorporation of all companies. We found that in total data is shared with 40 unique countries. For 66% of the companies we could not determine the country information, as we could not find it in a public registry. Of the remaining companies, 17.3% are from the US, 4.3% from the EU, 0.6% from China, and 0.2% from Russia.

Our graph shows that by sharing data with a single company such as Unity, it is theoretically possible for this data to reach 2973 companies in total. To describe this phenomenon of uncontrollable large scale data dissemination, we use the term *data avalanche*. The rest of the network can be viewed and analysed using our tool, by visiting `DataAvalanche.io`.

3.4.4 Interim Discussion

Through our app analysis we showed that children's apps do not sufficiently support children in understanding and exercising their privacy rights. Importantly, the amount of data tracking that occurs in apps, are not justified by features in apps to negotiate this data tracking. We have aligned our findings against the AADC Systemic Breaches framework which we introduced in Section 2.2.2 in Table 2.3. Table 3.6 shows this summary. We have shortened the description of the breaches in order for it to properly fit the table. For brevity, we have also omitted breach (9), which is related to social logins, as social logins were not required in any of the apps we analysed.

Table 3.6: Mapping of our app analysis to the systemic breaches of the Age Appropriate Design Code.

Breach	Feature mapping
(1)Insufficient age assurance	We encountered **13 different types of age assurance mechanisms**, which protected unnecessary and vital parts of the apps, including parts where crucial privacy information is presented. Age assurance methods are easy to bypass.
(5) Dark patterns and nudges	We encountered nudges with **privacy policies**, **consumerism** (buy premium version of the app), **cross-promotions** (rate the app on the marketplace), and sharing content through **social media**.
(6) Age-inappropriate financial pressures	Children are requested to make **in-app purchases**, view **ads** to unlock content, and are **nudged** into installing more apps by the same studio or developer.
(7) Low default privacy settings	**Privacy settings** were mostly not available in apps. In the few apps that did encounter, **data sharing features** were enabled by default.

(8) Excessive data sharing with third parties	Over 78% of the apps we encountered made use of **third-party trackers**. These in turn shared data with their partners into a vast commercial network.
(10) Published terms are not age-appropriate	Most privacy terms were aimed at adults. Only a handful of apps presented **privacy policies** in bite-sized segments appropriate for children.

Firstly, by comparing Tables 3.6 and 3.5 (the mapping from the literature review), we can see that our analysis is more comprehensive. We provide evidence and a more comprehensive understanding of how the standards of the AADC are breached. Breaches 1, 5, 6, and 7 were understudied in past research. In our analysis we have been able to understand the various methods for age assurance (1), the presence of dark patterns and nudges (5), how children face inappropriate financial pressure through consumerism in apps (6), and how settings were used in apps to support privacy (7). Our findings contribute to a better understanding of these areas, which have previously received little attention in research.

Secondly, through this analysis, we also have a better understanding of the delicate balance between technical data sharing practices in apps and user-facing features that allow for negotiation of these privacy behaviours. In particular, we have been able to examine how technical data sharing practices, such as the presence of third-party trackers or data sharing features, interact with user-facing features such as privacy policies or permissions. Our analysis shows that user-facing features generally do not adequately support children in negotiating data tracking practices in apps. For instance, privacy settings were mostly unavailable and privacy information was not presented to children in a manner that could be deemed age-appropriate.

Through our analysis we have provided concrete evidence of how children specific apps do not uphold the standards set out by the AADC and how their privacy is at risk through the use of such apps.

3.5 Discussion

3.5.1 Summary and Key Findings

The introduction of the AADC by the ICO in the UK gave us hope for a more privacy-friendly digital space for children. It set out how services aimed at children should consider data protection and privacy as a core element of their designs. However, our findings suggest that the current state of apps for children do not align well with the principles set out in the AADC.

We started this chapter with making a snapshot of common methods of evaluating privacy in apps. We performed a literature review of 48 papers to understand how the academic world conceptualises privacy in apps and what features they use to evaluate privacy. Our findings show that privacy analyses are concentrated around using a few features, namely privacy policies and permissions, to understand whether apps are privacy friendly. Only a handful of studies specifically focus on children, even though they constitute an important market segment. Moreover, many studies focus on technical features, rather than features relating to usable privacy, aimed at understanding how well users are equipped to understand and exercise their data rights. The few studies which did focus on usable privacy, primarily limited themselves to the accessibility of privacy policies.

In this chapter, we developed and applied a two-dimensional method for analysing the privacy of children's apps. Our method is informed by the findings of our literature review and guided by the recent data regulation frameworks, and consists of two components: a user-facing analysis of privacy features, and a technical analysis of data tracking and sharing practices. We applied this method to a set of 137 expert-approved children's apps, using a cognitive walkthrough to simulate a child's experience with the app.

In our analysis, we found that children's apps frequently lack privacy features that support children. Additionally, we observed that many children's apps use inappropriate financial pressure and nudges to encourage children to disclose more information than necessary. We also performed a tracker analysis and found that most children's apps extensively make use of trackers, but do not have features to negotiate data tracking or delete data. Finally, we analysed the data sharing partners of third-party trackers and found that data may often be shared with a large network of commercial entities.

To further understand the implications of our findings, we mapped them onto the AADC breaches framework. This allowed us to examine how our

findings aligned with regulatory expectations and identify specific areas where children's apps may be in breach of AADC standards. Through this analysis, we were able to provide concrete examples of how and where children's apps fail to meet the standards set by the AADC in terms of protecting children's privacy and data protection.

Overall, our findings suggest that there is a need for further research and regulatory intervention to ensure that children's privacy is protected in apps.

3.5.2 The Complexities of the Data Tracking Ecosystem

While previous research has analysed third-party trackers, we specifically looked at trackers in children's apps and were the first to map the fourth-party tracking ecosystem. Our findings show that there is a vast network of data sharing entities outside of the app stores and marketplaces that consumers and developers are not aware of, which does not come without its consequences. We have identified three challenges arise as a consequence of this phenomenon.

Firstly, the problem with such a densely connected and vast network is that once data is transmitted to a fourth-party, it will be forever recorded and near impossible to retrieve or have it deleted. GDPR rights of consumers seem ineffective, as it has been shown that even sending out a handful of GDPR Data Subject Access Requests and negotiating with companies can be an arduous task [323]. What we showed in our study is that one would have to send thousands of such requests to retrieve/delete or even verify that data has been shared. In addition, data is also being shared with companies which fall outside the EU jurisdiction, meaning that they are not under pressure to comply with the GDPR. In such cases, it may even be impossible to have the data retrieved.

Secondly, there is no transparency for either consumers or developers about how and where data is being shared. In our own processing of uncovering and mapping this ecosystem, we found that many companies did not list their data sharing partners or the nature of their relationships. The true extent to which sharing happens is therefore relatively unknown. Furthermore, since we as 'expert' researchers had difficulties uncovering parts of this network, it cannot be expected for children to understand or comprehend this phenomenon. This lack of transparency has implications for both

consumers and developers. Consumers may not be aware of the scale and permanence with which their personal data is being shared. Developers may not realise that the use of certain third-party libraries can bring irreversible harm to consumers.

Thirdly, while third-party tracking is still prevalent and ubiquitous in children's apps, they are still advertised to be appropriate for them. For example, despite the privacy concerns to be expressed for children's apps, Google still labels them as 'expert-approved' promotes them to the safe and appropriate for children. Google is not entirely clear on what it means for apps to be expert approved. However, the information that they do provide alludes to content based approval, rather than technical features in the app [4]. Moreover, the apps are approved by teachers and media experts, rather than privacy experts. The Google 'expert-approved' category is not the only place for parents and children to find apps. For example, Common Sense Media (CSM) is another popular resource which lists reviews and recommendations for children's apps [351]. However, while CSM reviews are done by experts and include criteria which are not considered by Google, such as 'Consumerism', it still does not consider privacy or data protection. With what is known about the extent of data tracking in apps, it may be important to include privacy as a key consideration in app recommendations for children. Google has made several changes in this regard, for example they introduced the Data Safety section in apps [352], which allows developers to self report what type of data is collected and shared. While it does include what types of data is being collected, it does not inform users about which parties it is being shared with.

These challenges and problems strongly hint at the need for certain changes in this space. We make two recommendations which may offer partial solutions to aid developers navigating this complex data infrastructure.

Firstly, we recommend that there is an increased need for transparency in the data sharing ecosystem. Currently, there exist no tools which explain how third-party libraries behave, whom they share data with, and what data they may be collecting. In such cases, it is possible that developers default to the most commonly used third-party libraries, which in many cases will be developed by market leaders and major data controllers, such as Google and Facebook.

This leads us to our second recommendation, to provide resources which offer privacy-friendly alternatives to commonly used SDKs and third-party libraries. There are alternatives to popular analytics services, such as Piwik

[353], which claims to be a privacy-friendly alternative to Google Analytics. However, such alternatives may not be the most obvious option for developers and regulatory and public bodies, including the ICO, may want to consider compiling a directory of services which they seem appropriate as an alternative to privacy-harmful mainstream solutions.

3.5.3 Challenges in Designing Privacy-Friendly Apps for Children

Through our analysis of privacy features in apps, we have gained a deeper understanding of how children are supported in understanding and exercising their privacy rights. This has highlighted a major challenge in creating privacy-friendly apps for children: their lack of awareness and understanding of the importance of such features. We have broadly identified three ways in which privacy is inappropriately negotiated with children.

Firstly, in many cases, privacy was treated as a legal necessity in apps, rather than as an effort for children to benefit from it. For example, children were presented with or referred to long complex privacy policies. Children had no other option than to give consent, or else they would not be able to access this service. In this way, giving consent for online privacy terms and conditions is not a mutual exchange. It's a one-way agreement where the company can monitor and use your information, and the user has no choice but to agree or lose access to the service. One could argue that this essentially represents the "cost" one must bear to enjoy free apps. It is important to note that this study exclusively focused on free apps, making it difficult to definitively conclude that these concerns do not exist in premium apps. Nevertheless, research has indicated that even premium apps that abstain from advertising still extensively collect user data [183, 184, 185].

Secondly, we have also observed cases where privacy is entirely disregarded or not mentioned. For example, there may be no privacy settings or information provided about the data collected. In such cases, the app may be collecting and using personal information without the knowledge or consent of the user, or it may not engage in any data collection practices. In either situation, normalising this practice can create a false sense of security in users, making them believe that their data is not at risk when it actually may be. This can lead to individuals sharing sensitive information with the app, which can be used for malicious purposes. Moreover, normalising this

practice can lead to a general disregard for privacy and the erosion of trust between individuals and developers. It is thus critical for developers to prioritise making privacy transparent through and provide clear and accessible information about data collection and usage, even if they do not engage in any data collection practices.

Lastly, we have also seen instances in which privacy is just limited to parents, for example through age-assurance mechanisms being applied to privacy settings and and the disclosure of privacy information. Our analysis of data protection frameworks in section 2.2.2, has revealed that this stance is more in line with the regulations established by the COPPA, which entrusts parents with the task of protecting their children's privacy. The AADC however, takes an alternative approach to this, advocating that the complexities of privacy should be simplified to a level at which children are able to comprehend and interact with it. This includes providing age-appropriate explanations and clear, easy-to-use controls, rather than only targeting parents with privacy information and controls.

This leads us to consider what we can do to potentially address these issues in apps, as well as which stakeholders should be involved in this process. We believe that marketplaces have a role to play in guiding developers. Marketplaces should set out strict requirements for user-facing privacy features, which should be implemented in apps. Until now, privacy has been treated predominantly from a technical perspective. For example, both Google and Apple mainly evaluate privacy in terms of third-party tracking and analytics, but often neglect to take into account children's capability to negotiate these. Therefore, we must consider that marketplaces have a critical part to play in informing developers about which user-facing privacy features should be included in apps and how they should be communicated to users. This initiative can take various forms, from providing wireframes and software development kits (SDKs) to creating designer guidelines. The UK ICO has adopted a similar approach, providing developers with a range of tools, such as data process mapping [354].

This brings us to our second point. While it is easy to recommend that developers simplify privacy terms and make apps more privacy-friendly, it is clear that they are hindered by legal privacy requirements [24, 25]. This indicates a need for more suitable tooling, and potentially implies that there is a need to collaborate more closely with developers to consider their role and motivations when designing apps for children. This is an issue that we investigate further in Chapter 4.

3.5.4 Limitations

We would also like to point out several limitations of our study method.

Firstly, during our literature review, we conducted a search using the keywords "app" and "privacy," which may have led to the exclusion of studies that used different terminology or focused on different aspects of privacy. This could potentially limit the generalisability of our findings and the comprehensiveness of our review. It is possible that there are other studies that would be relevant to our analysis but were not included due to the limitations of our search query. However, for the purpose of our study, we focused on examining the privacy practices of children's apps, and our search query was specifically designed to identify studies that were relevant to this topic. While it is possible that our search may have missed some studies that used different terminology or focused on different aspects of privacy, we believe that our review provides a thorough and comprehensive overview of the current state of research on the privacy practices of children's apps.

Secondly, we limited our sample to apps from the Google Play Store and only selected apps from the 'expert-approved' category due to technical limitations, as we only had access to an Android device. Additionally, Android has a dominant market share, making it the most relevant platform to focus on for our study. However, it would be interesting for future research to explore whether there are any differences in the privacy practices of children's apps between the Android and iOS platforms. This could provide a more comprehensive understanding of the privacy practices of children's apps and how they may vary across different platforms.

Thirdly, while we focused specifically on children's apps in this study, it is important to recognise that privacy concerns are also present in apps for adults. It would be beneficial for future research to examine the privacy practices of apps for adults and compare them to those of children's apps in order to understand whether there are any differences in the way that data is collected and privacy rights are exercised. In this study, we focused solely on free apps. While previous studies have suggested that paid apps do not significantly differ in their privacy practices from free apps, it would still be worthwhile to investigate whether there is any difference in the financial pressure placed on children through paid apps compared to free apps. This could provide a more comprehensive understanding of the privacy practices of children's apps and how they may vary depending on the pricing model.

3.6 Conclusion

In this chapter, we set out to explore the privacy landscape of apps for children. We did this in a two-fold manner. First, through a systematic literature review, we examined how privacy is conceptualised and evaluated in apps in the research community. By aligning the features we identified with the AADC, we found that past research has understudied several critical areas of privacy for children. We used these findings to establish a more holistic method for the privacy analysis of apps, consisting of a user-facing and a technical dimension. We subsequently applied this method to a dataset of 137 'expert-approved' children's apps, to understand how privacy is considered in apps which are supposedly approved and safe for children to use.

Our findings show that privacy-friendly features are greatly lacking and barely present in apps. This suggests that a finer balance is needed between the technical and user facing privacy features within apps, either by reducing the amount of data tracking or by improving the user facing privacy features. While regulatory responses seem to be slow in this regard, several commercial entities have taken the initiative. For example, Apple has blocked all third-party tracking in children's apps, and now under the App Tracking Transparency framework [355] users can also choose to block third-party tracking all together. Google is still lacking in such measures and it is unclear if they will ever follow suit, especially considering that advertising and data tracking forms a large part of their revenue [245]. This means that consumers may not always be able to rely on either market leaders or regulators to protect them in this regard.

Meanwhile, the analysis in this chapter highlighted the open challenges for building privacy-friendly apps for children, including users' limited exposure of such risks and thus their awareness and recognition of their importance, the difficulty to navigate a complex (3rd- or 4th-party) data tracker network and the diverse usable and technical privacy features that are needed to create privacy-friendly apps for the children. While this chapter provided a good understanding of the current privacy landscape of apps for children and how privacy is strongly neglected in this process, we do not fully understand yet app developers' current practices which may contribute to apps in such ways and how they could probably be better supported. We have been able to hypothesise on this, based on what we found in the apps, however more clarity on this is still needed. Therefore, in the next chapter we dive into this, by performing a qualitative study with app developers to understand

their current motivations and design choices for creating apps for childen.

4

Identifying Barriers to Better Privacy in Children's Apps From Developers' Perspectives

Contents

4.1 Introduction 104

4.2 Methods 106

4.2.1 Participants 107

4.2.2 Procedures 107

4.2.3 Analysis of Qualitative Data 109

4.2.4 Descriptive Statistics 109

4.3 Results 110

4.3.1 Design for Children's Best Interests 110

4.3.2 Perception of Data Collection Practices 113

4.3.3 The Need for Analytics and Other Third-Party Libraries 114

4.3.4 Challenges in Selecting Third-Party Libraries . . . 115
4.3.5 Challenges in Sustaining a Successful App Business 117
4.3.6 Summary 119
4.4 Discussion 119
4.4.1 The Challenges of Using Third-Party Libraries . . 120
4.4.2 Monetisation in a Data-Driven Economy 121
4.4.3 Problems in Using Guidelines 122
4.4.4 Working Towards Solutions 123
4.4.5 Limitations 127
4.5 Conclusion 129

4.1 Introduction

In the last chapter, we conducted a mixed-method study to understand the landscape of children's apps. We performed a literature review and an app analysis, focusing on data tracking and user-facing privacy features. We found that children's apps engage in data tracking and do not support children to negotiate these behaviours. This aligns with previous research showing that data trackers and third-party libraries in apps commonly collect sensitive data [7, 18], including location information, which can be sent to data brokers for profiling [8, 9, 269]. We do know that developers make use of third-party libraries because it simplifies development [154] and they rely on targeted advertising for income [34, 35, 36, 10].

However, the last chapter shows that even apps specifically designed for children suffer from poor privacy features and support. While we now have a better understanding of how privacy features are considered in this children's apps, relatively little is known about the considerations and design choices made by app developers. Therefore, in this chapter, we take a closer look at this, and investigate developers' design considerations and any challenges they may face for creating *privacy-friendly* apps for children [1]. Similar to Chapter 2, we conceptualise privacy-friendly as a design paradigm

[1]This Chapter has been published as: 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.

which upholds expectations from data protection regulations, and minimises the amount of personal data collection and sharing through the use of data trackers, often used in apps as third-party libraries and advertising modules. Specifically, we aim to answer the following research questions:

RQ2 What are the key considerations and current practices of app developers when designing apps for children?

- 2a What do app developers perceive as their responsibilities when designing for children?
- 2b What are the main practices adopted by developers for achieving privacy and how do they align with leading data protection frameworks from different sectors?
- 2c What are key barriers for the adoption of the leading data protections frameworks for app developers and how can these barriers be overcome?

To answer these research questions, we conducted 20 interviews and 134 surveys with children's app developers to understand their design considerations and challenges and how we can better support developers [270]. Our findings show that developers feel responsible for designing apps with the best interests of children in mind, including that children's privacy should be respected and thus data collection should be minimised. However, we also identified several barriers which were in the way of realising best practices set out in the data protection frameworks.

First, developers find it difficult to navigate the complex and opaque landscape of third-party libraries. There is a lack of awareness of privacy-friendly libraries, forcing developers to choose major data controllers as their third-party service providers.

Second, developers struggled to monetise their apps in ways that did not rely on advertising. The market pressure and competition made alternative and potentially privacy-friendly business models, such as offering premium apps, unsustainable.

Third, there was a general lack of awareness of guidelines for designing for children, resulting in developers relying on terms and requirements set out by market leaders, such as Google, which are not always aligned with the best interests of children.

We found that the data protection frameworks, which we introduced in Section 2.2.2 did not provide all the transferrable/practical guidance that is needed by developers in addressing these barriers. Based on our findings, we make recommendations to help improve the state of app development for children. We propose to include concrete recommendations in guidelines regarding selecting data controllers, advertising networks, and third-party libraries. Furthermore, we also advocate for heightened support for both end users and developers through tools which can shed light on the otherwise opaque data economy. Lastly, this chapter also highlights the importance of needing industry support to make major changes to the app development landscape.

4.2 Methods

In this chapter, we seek to understand what developers perceive their responsibilities to be in creating apps for children, and how such perceptions impact app development practices. To this end, we conducted 20 semi-structured interviews and 134 surveys with them in the summer of 2019.

There are several reasons why qualitative methods, especially interviews, are an effective choice for finding out about participant practices, design motivations, and values. According to Creswell [356], these methods are particularly well-suited for studying complex social phenomena and exploring the meaning that individuals attach to their experiences. Through open-ended questions and follow-up probes, researchers can gather rich, detailed data about participants' practices, motivations, and values, providing a deeper understanding of these aspects of participants' experiences than might be possible through more quantitative methods. Additionally, qualitative methods can be useful for generating new insights and theories by uncovering new themes and patterns through in-depth interviews [357]. These methods also allow researchers to delve into the context in which participants' experiences take place and provide insights into the underlying reasons and considerations that drive their practices, motivations, and values [358]. Overall, the flexibility and in-depth data gathering capabilities of qualitative methods make them an effective choice for finding out about participant practices, design motivations, and values.

4.2.1 Participants

In this study, we specifically focused on app creators from the UK market. We chose this market, because at the time of the study the UK had recently introduced the Age Appropriate Design Code, which sets out specific requirements for the design of online services that are likely to be accessed by children. By focusing on app creators in the UK, we were able to examine how they are responding to these new requirements and how they are prioritising children's privacy in the design of their apps. All of our participants, while not always located in the UK, still developed apps for the UK market.

Participants were recruited through direct email communications using the address they made publicly available on the Google Play Store. We contacted developers whose apps were declared from the 'family' and 'education' genres (not excluding apps with particular age ratings), available in Europe. We then extended this to developers of parental control apps, as they are increasingly used by families and children. They were retrieved using keyword search [345], including terms such as 'parental control', 'online safety' and 'online privacy'. We included developers of both paid and free apps.

We sent out a total of 11,000 emails and received 134 survey responses (S1-S134). In our recruitment email, we asked participants whether they would like to fill out the survey and if they were interested in participating in an interview. It typically takes six participants for stable themes to begin to emerge and 12 participants to achieve data saturation in an interview study [357]. However, we decided to stop recruiting after we reached 20 interview participants in order to ensure that we had sufficient data to draw meaningful conclusions from our study. All participants which were interviewed also filled out the survey.

4.2.2 Procedures

The interview and survey included similar open-ended questions to allow developers to process the ideas from the survey before elaborating on them during the interview. We refrained from conducting a pilot study for either the survey or the interview. However, we employed an iterative approach in which the interview structure was subsequently adjusted based on the preliminary findings obtained from the survey. This approach allowed us to refine our interview questions to better align with the specific insights and concerns identified in the survey results.

Both the interview and survey were designed to capture developer perceptions of risks online for children, their views on data collection practices by third-party libraries and trackers, and their development practices.

Interviews

The interviews for this study were conducted remotely via Skype between July and November of 2019. Participants were not compensated for participating in the interview, but they did provide their consent to be audio recorded. The interviews ranged in length from 24 to 43 minutes.

The interviews consisted of three parts. In the first part, participants were asked to provide background information about their development experiences, the motivation behind their app development, and the functionality of their app. In the second part, we asked questions about their perceptions of risk for children online and their views on data collection practices in the mobile ecosystem. In the final part, we inquired about their personal data collection practices in app development and their current practices regarding the use of third-party libraries, including any information factors, quality assessment procedures, or decision-making processes involved in choosing and incorporating these libraries into their app.

Surveys

The online survey for this study was distributed to participants in late July 2019. Before beginning the survey, participants had to give their consent, indicate that they were over the age of 18, and confirm that they had read the accompanying information sheet. The survey was designed to take approximately 15 minutes to complete and included closed, open-ended, short answer, and likert-scale questions.

The survey consisted of several parts. In the first part, we asked background information about the participants' development experiences, including whether they had developed apps for children and the purpose of these apps. In the second part, we asked about the privacy practices of their development practices. In the third part, we inquired about how they inform their design choices, such as through market research or stakeholder engagement. In the fourth part, we asked about the use of third-party libraries. Finally, we asked for demographic information. Participants were not compensated for completing the survey.

This study was approved by the research ethics committee of the university. The full survey and the interview questions are available in Appendix A.

4.2.3 Analysis of Qualitative Data

The audio recordings were transcribed with all personally identifiable information anonymised. The transcripts and the open-ended survey questions were analysed in two iterations by two HCI researchers: myself and a second researcher.

First, using Thematic Analysis [359], I and the second researcher independently coded six different transcripts. Following this, we convened to consolidate themes and derive a common codebook. Subsequently, the next eight transcripts were coded independently using the codebook until an inter-rater reliability score, calculated using Cohen's kappa [360], reached 0.85.

After achieving reliability, I re-coded the initial six transcripts, coded the remaining six transcripts, and coded the open-ended survey questions. In total, 78 unique codes were generated. Code saturation, where no new codes emerged during coding, was achieved after analysing 11 transcripts. The codebook, containing all 78 codes used in the analysis, is available in Appendix A.3.

4.2.4 Descriptive Statistics

Surveys

88% of the survey participants identified as male and 27% of the participants was between 30 and 39 years old, representing the largest age demographic. 25% of the participants was between 40 and 49, 22% was between 23 and 29, 15% percent was between 18 and 22, and 11% of the participants was over the age of 50. English was the native language to 26% of the participants. Most of survey respondents originated from Europe (40.5%) and Asia (34.4%), with others from North America (10.7%), South America (9.3%) and Africa (4%).

Interviews

The total duration of the interview recordings is 698 minutes. The average interview length is 34.5 minutes (Sd = 6.5). The shortest interview was 24

minutes and the longest 43 minutes. The app characteristics and developer demographics are summarised in Table 4.1. Although we did not intentionally recruit for a specific gender, it ended up that all of the participants in our study were male. Even though all participants developed apps for the UK market, we also had a lot of oversea developers. This may be due in part to the fact that app marketplaces are international markets, attracting developers from all over the world. It is also possible that the UK market for children's apps is particularly competitive and connected, drawing in developers from other countries.

4.3 Results

In this section, we report our qualitative and quantitative results that provide us an insight about children's app developers' data protection practices, situated in the context of their app development motivations and awareness of current guidelines and regulations.

Our thematic analysis of the data shows that there have mainly been four major themes: (i) developers' perceived responsibilities and motivations in designing for children's best interests; (ii) perceptions of data collection practices; (iii) reliance on third-party libraries; and (iv) the need to earn money.

We make use of the descriptors 'S' and 'I' to refer to the surveys and interviews respectively.

4.3.1 Design for Children's Best Interests

The majority of developers reported that designing apps for children comes with moral responsibilities (15/20) and they believed that apps for children should be designed 'differently' than apps for adults. More specifically, developers emphasised the responsibility to make apps age-appropriate and take children's developmental needs into consideration (10/20):

> *"So we interact with the child, as the app interacts with the kid during a very sensitive period, when all the behavioural patterns are formed for the future. So compared to general app, or an app that an adult can use, we think we bear a much more responsibility for the user."* – I10

Table 4.1: Table containing descriptive characteristics of the apps developed by our developers. App 4 was removed from the Google Play Store and App 18 was in development at the time of the interview.

#	**Country**	**Play Store Category**	**Age range**	**App description**
1	Turkey	Tool	PEGI 3	Parental control.
2	United States	Entertainment	PEGI 3	Parental control.
3	Canada	Parenting	PEGI 3	Parental control.
4	Bosnia	-	-	Parental control.
5	Canada	Tools	PEGI 3	Parental control.
6	Austria	Education	PEGI 3	App teaches children programming.
7	Germany	Education	Ages 6 - 12	Teaches children mathematics.
8	Lithuania	Educational, Pretend Play	PEGI 3	Teaches children about every day aspects of life.
9	Macedonia	Casual, Brain Games	PEGI 3	Game based on reflexes.
10	Russia	Education	Ages 8 & under	Educational games.
11	Russia	Education	Ages 8 & under	Educational games.
12	Russia	Education	Ages 8 & under	Educational games.
13	Bangladesh	Education	PEGI 3	Various tools for school.
14	Tunisia	Education	PEGI 3	Educational game to learn about health.
15	United Kingdom	Parenting, Education	PEGI 3	Augmented reality to enhance outdoors learning.
16	Portugal	Education	PEGI 3	Assists in school planning.
17	Austria	Education	PEGI 3	Artistic game to compose drawings.
18	The Netherlands	-	-	-
19	Germany	Education	Ages 6 - 12	Media streaming for children.
20	Columbia	Action	PEGI 3	Action game.

However, when developers sought to design age-appropriate apps for children, they faced a range of challenges. More than half indicated that they struggled to find suitable and specific design guidelines (11/20). Guidelines provided by the app marketplaces provide limited discussions on how to design for children's developmental needs:

> *"There are some general guidelines, like the posts which say, above a certain age you are allowed to show violence, but nothing specific to the education process itself: not pedagogical recommendation, no tutorial design recommendations, nothing of the sort. We wouldn't mind if such things existed and were paid attention to."* — I11

Developers also indicated that following guidelines has not always been possible, as they constantly changed, and provided insufficient support for smaller companies or individual developers (7/20).

> *"We are aware of codes, but they are constantly - the guidelines - they are constantly changing, and our problem is, since we are in another country, here the laws are different. We usually get and try to read every guideline and everything since we are only two people and we don't have any lawyers or any law advice from lawyers, we sometimes can miss few guidelines."* – I9

As a result, they defaulted to following Google's Guidelines on "Designing Apps for Children and Families" (11/20), as it was the most "accessible" or "required" (10/20). However, the principles from these guidelines referred to are primarily centred around app publication requirements, such as the use of specific ad SDKs:

> *"Google Play wants to be sure about if you wanna advertise a parental control or child oriented application, it is much easier to obey these rules. You have to accept these restrictions to publish your applications"* – I1.

In the end, only a small number of developers used specific methods or techniques for designing for children. A few survey respondents (3%) and interviewees (3/20) consulted professionals to help them with the app design:

"We have a very good network of scientists who take a look at what we are doing and steer us in the right direction. For example, we are working together with a professor who knows about a lot of gamification." – I7

4.3.2 Perception of Data Collection Practices

Survey respondents generally believe that the privacy of children should be respected, in terms of data collection, data sharing, and third-party analytics. The majority of them reported to *not collect personal data* of the users (90%) and almost all developers indicated to *not share data with third parties* (95%). Similarly, they strongly felt that it is unethical, even for the purpose of sustaining the business, to sell children's data (90%) or make use of targeted advertisements containing third-party trackers (85%):

"I was approached by about 10 companies to add tracking libraries to my app in exchange for a payment of about 100$ to 400$ per month from each company. Since I find this unethical I refuse to do so by so far. " – S11

Some interviewees were opposed to any data collection in apps due to the associated risks and potential privacy problems (8/20).

"I strongly oppose to data collection, especially if its an app directed at children, I don't think any data should be collected. I think it should be turned off. And there should be very strict policies on that." – I17

However, a few interviewees stated that limiting collection to non-personal data is not necessarily harmful (4/20) and a small number of them even said that data collection does not affect individuals at all (2/20).

"Its not always bad. For example, we have to collect some data for our own analytical purposes to design the app better, and these are oftentimes anonymised data; these are not personal data to children." – I12

"On an individual basis, I can see this (data collection) being very damaging. [...] But on a mass scale, I just don't see the risks and the likelihood of the risk being that great." – I5

Apart from their beliefs about data collection, they were also faced with technical constraints (7/20), such as increased costs of hosting a storage server, and liability issues (4/20) in collecting data:

> *"Initially, [we] collected a lot of additional data, like IP addresses of users when they uploaded things, published geographic location, and so on. [..] With the European, you know, all the law changes and so on, we decided okay, lets not do that. We'll only collect the absolute minimum that we can."* – I6

4.3.3 The Need for Analytics and Other Third-Party Libraries

Developers also mentioned several important goals which could only be realised through third-party services (13/20). For example, some of them expressed the need to further understand user behaviour and interests to improve the app performance and usability (9/20):

> *"So when a child [uses our app], it gets a dedicated individual training. And in order to deliver something like this we need to collect training data from the child. But only in order to improve the training for the children."* – I7

Two developers also indicated that children's data is not very "reliable" (I1), as children's behaviour is erratic, because "they don't even know what they are doing on the phone" (I1). Another developer explained that children's data does not serve a useful function:

> *"I don't see the value in it [collecting data] as much as adults, because adults have a lot more capital to spend. So... to be honest with you. So I see the privacy issues on one side, on the other side I don't see why you'd even want to capture information of people who don't even have a lot of money."* – I5

At the same time, developers realise that data-based service optimisation is a sensitive topic, especially where it concerns children and happens through third-party services.

Others stated they needed third-party services to simply maintain efficient core services for their apps (5/20), e.g. *"We use like Firebase for push*

notifications" (I4). This was also reflected in the survey data, as the majority of the developers reported to make use of third-party libraries (63%). The primary reasons for this were 'Convenience' (72%), 'To reuse existing software modules' (52%), for 'Targeted ads' (21%), and to "Gain insight into user behaviour" (S53) (6%).

In the trade-off between collecting data to provide core services and avoiding data collection, developers used various strategies to support children's privacy needs and minimise data collection. Survey respondents indicated to avoid collecting unnecessary data (68%), put privacy settings high by default (37%), and did not nudge users into making privacy reducing choices (31%). Similarly, developers reported to avoid collecting personal data (6/20) and limit themselves to collecting anonymous data without affecting 'individuals' (9/20):

> *"I don't collect any children information; we use Firebase Analytics for app usage statistics, which is required for product improvement."* – I2

4.3.4 Challenges in Selecting Third-Party Libraries

Beyond the conflicting views developers had about the need and appropriateness of data collection for children, they also faced challenges in selecting data controllers and third-party service providers. In particular, the opaqueness of the data economy made it extremely challenging to navigate the APIs and SDKs that are available on the market (13/20). For example, it was unclear to developers what libraries are doing in the background (10/13) and what organisation are secretly doing with the collected data (3/13):

> *"We were in this situation where we were so convinced that we don't show [ads] and don't do anything wrong. I mean, we didn't* knowingly *gather any data, we didn't run any campaigns, we didn't use any marketing techniques or anything. So there was nothing of that [data colletion] in our ads. [...] For example, Unity, which we use to make our apps, they have this solution to deliver in-app purchases. So we use it. Now we found out that whenever there is a purchase, Unity takes some personal data, to make this transaction possible. So, and its not cool with us, but there is no other way to do this."* – I8

Developers expressed that they wished data controllers would be more transparent and accountable, but doubted that current governmental regimes would be likely to help achieve this (6/20):

> *"Well, I'd love if companies took a little bit more responsibility. But they are not going to; I mean they don't think twice of increasing user rate. [..] It doesn't seem that politicians nowadays have a vague understanding of how the internet works, or how digital works. And it seems for me to be impossible for them to impose the correct laws."* – I17

Survey respondents reported to have no internal policies regarding the choice of libraries or third-parties. The majority of them chose libraries themselves (39.3%) or discussed this amongst colleagues (26%). A small number of participants needed approval from their manager or supervisor (16%).

In making this choice, developers were left with relatively little information to base their decision. Thus, they resorted to relying their perceptions of the trustworthiness and quality of the software typically produced by third-parties as a basis for selecting them (11/20):

> *"I trust Google. I used a lot of their tools, and I think they are well developed and are maintained constantly. I use Facebook SDKs and its also very good and well developed library."* – I14

Such providers were also the most popular and prominent, which further made it likely they would be selected by developers. Thus, unsurprisingly, the majority of both interviewees (13/20) and survey respondents (64%) selected libraries from Google. Survey respondents further indicated that *"Google libraries should be safer than any others"* (S29) and that they *"only select reputable libraries from large companies"* (S113). As a result, 65% of the survey respondents and 9/20 interviewees reported to use Google's libraries by default, such as Google Analytics (59%S) and Firebase (22%S).

> *"We are typically using libraries from Apple of Google. Rarely do we use like something we found on a developer network forum, where you could potentially get in trouble. So yeah, the libraries we use are primarily from major parties that have created their own stuff."* – I3

Only a few survey respondents indicated to look at the security aspects, for example by performing 'Pentesting' (4%), 'Internal Testing' (1%), reading the Terms of Service and Privacy Policies (6%), or considering any reported security issues (4%): *"We read the terms of use and if it a code library, we do a quick code review to identify any security vulnerabilities"* (S47).

4.3.5 Challenges in Sustaining a Successful App Business

Understandably, sustaining a viable business was one of the primary objectives for developers to support sustained development (13/20), because by the *"end of the day you've gotta make money. Money makes the world go around"* (I3). This sentiment was reflected by the majority of survey respondents as well, who reported that commercial success of the app was an important factor in development (60%). In fact, 63% said they relied on app development as a major source of income, either through the revenue the software generated (37%), third-party investments (16%), or through contract work (10%). As a result, the majority (79%) of them monetised their app, either through ads (32.6%), a pay-to-download model (25%), in-app purchases (21.2%), or subscriptions (18.9%). Approximately a fifth of the developers, however, did not make use of any monetisation features (21%) and were running the app for 'non-profit', stating to *"develop for fun and learning"* (S46).

Almost all interviewees who did monetise their apps wanted to do this in an age-appropriate way. They felt a moral obligation to not make use of harmful techniques (17/20), such as the use of *"manipulative flashing lights, button that move, sparkling colours"*, because then *"of course [a] child would click on in app purchases: they would get pleasure from it"* (I9). In monetising their apps, developers found it important to take children's developmental needs into consideration:

> *"We want to make sure that we also have a sensitive side where we take the users into account, and we don't want them to be like, 'oh I've gotta check my phone again, who knows if I have another like'."* – I18

In attempts to monetise apps in an age-appropriate way, they faced several major challenges. First, apps not based on ads, i.e., paid apps, did

not earn enough for developers to sustain their business or earn a sufficient income (15/20):

> *"Well the first app, I made a free version, which only has about half of the elements to choose from. And then I made a paying version. Turns out, that [I] do not earn any money at all. I earned like 40 euros last year."* – I17

Second, several interviewees and survey respondents discussed that users often revolted against paid apps, using rating systems to pressure developers to make them available for free (3/20):

> *"You know, 100,000 people in Russia give you 1 star, just because they are used to seeing ads instead of paying money and you don't offer this opportunity to them. This impacts your global rating; and this impacts your global sales in territories where you don't show ads and are dependent on sales. [...] In order for us to make revenue, your game design has to be focused around showing ads."'* – I8

> *"The primary reason to adopt child-safe advertising was an outrage on the app store comment/ratings that resulted in low ratings of our paid (premium) games just because it's paid. We were forced to react and offer some alternatives to appease those users, including the display of child-safe ads."* – S54

Lastly, one discussed the cutthroat and sinister nature of marketplaces: even if you tried to use age-appropriate methods and became successful, it was likely that some clone-maker would duplicate your app and use privacy-invasive (but higher-yield) monetisation methods in it instead. That was particularly the case for paid apps, which were often cloned, turned into ad-based monetisation vehicles, and released for free (3/20):

> *I can find and show you dozens of apps that are clones of our games, so someone somewhere took our app, re-skinned it a little bit, and then left it as it is, with all the game design and whatever, and offered it on Google Play, and show all kinds of ads: safe, unsafe, whatever. [...] So if this continues, essentially it means that users who are looking for free stuff and so on, they will still be able to find whatever they want. [...] It's not even David vs Goliath, it's a Flea vs Goliath. "* – I8

As a consequence, many accepted that, while using ads did not align with their goal to limit data collection, they conceded there were few options, as these were a *"necessary evil to keep the business afloat"* (I3) (14/20). As a result, interviewees felt that commercial success of the app often came at a cost of the best interests of children (10/20), because *"the two things don't align very well, I suppose, and its kind of hard to do them both ways: to have an ethical thing and have the biggest payout in your app"* (I18).

Several others expressed that whilst they tried methods other than advertising, sooner or later they had to resort to it in the end:

> *"We were completely driven by the good for the end user. And then we ran out of money each time. And then we realised there has to be a balance of some degree of commercial success that will allow the app to sustain itself, and earn money to continue to operating and be as responsible for the end user."* – I10

> *"We didn't want ads. If the market would allow us, if there was a possibility to still exist and do what you love, by offering paid apps, for 2.99, we would gladly remain in that field. Its just that the business there became impossible and unsustainable."* – I8

4.3.6 Summary

Developers recognise their responsibility in designing apps for children and strive to create apps that consider the best interests of children while also sustaining their app development business. However, they face several practical challenges in achieving these goals. Firstly, there is a lack of specific guidelines for children's apps, leading developers to rely on their intuition or follow practices set by major marketplaces. Secondly, the data collection infrastructure of the mobile ecosystem can be complex and opaque, leading developers to rely on third-party libraries from prominent data controllers such as Google. Lastly, developers indicated that it can be difficult to monetise apps through privacy-friendly means, resulting in a reliance on methods such as targeted advertisements.

4.4 Discussion

From our findings we identified three key challenges in designing privacy-friendly and age-appropriate apps for children: (i) navigating the complex

and opaque landscape of third-party services and their underlying data economy, (ii) the lack of viable monetisation options not relying consumer data, and (iii) the lack of awareness and applicability of regulatory guidelines. Below we discuss why these challenges interfere with best practices set out in data protection frameworks and how they fail to address these issues.

4.4.1 The Challenges of Using Third-Party Libraries

Our findings show that developers extensively use and rely on third-party libraries to provide core services and gain user insight. More specifically, our participants often relied on libraries from major data controllers, like Google Analytics (58.5%), Google Firebase (22%), and Facebook APIs (29.3%). These findings are consistent with former research. Large scale analyses of Android apps has shown up to 82% of these apps and 60% of all code in these apps is from third-party libraries [361, 362]. Use of third-party libraries has been shown to be critical in saving development time and efforts [363, 364, 365].

While developers demonstrated to care about children's privacy, it also well known that third-party libraries can be a major gateway to global data tracking and profiling networks [7, 18]. Products like Google Analytics and Firebase, which were popular amongst our participants, are free so that it can "provide confidence and prove the value of online advertising to potential new advertisers" [366], meaning they rely on the profiling of large volumes of user data. These issues are also addressed by the data protection frameworks we analysed in Section 2.2.2. The use of analytics and storage libraries relates to requirements about *data sharing* and *profiling* (see Table 2.1). Both the AADC and COPPA require that data should not be shared with third parties unless there is a compelling reason to do so and the AADC only allows profiling under the assurance that reasonable security measures are in place.

This is not to say that app developers should never make use of such third-party libraries, but it does have important implications for efforts addressing 'age-appropriate' design. Firstly, our findings show that developers have conflicting perceptions of major data controllers. They realise that, on the one hand, data controllers are nontransparent and potentially harmful in their data handling practices (13/20), whilst simultaneously relying on them to produce high-quality and unmalicious software (13/20). This forced trade-off highlights the complexity and lack of guidance in navigating the often treacherous landscape of third-party services. Data protection guide-

lines, such as the AADC and COPPA, do not provide sufficient support to developers in this regard. For example, they do not concretely state which libraries are simultaneously reliable and 'age-appropriate'.

Second, developers generally perceived the use of libraries such as Google Analytics and Firebase as harmless and non-detrimental to children's privacy (8/20). This demonstrates the lack of a clear definition of what 'privacy-friendly', 'age-appropriate', or 'safe' third-services are supposed to be. While these boundaries are not clearly defined in data protection frameworks, both developers and regulators cannot make sound judgements in selecting or auditing third-party libraries.

Lastly, developers also indicated that third-party libraries often behave in unpredictable and unknown ways (13/20). This demonstrates that even if developers have the best of intentions, they cannot always enforce their well intended principles of designing for children. The AADC and COPPA require developers to ensure that third-party services have reasonable protections in place, for example by examining their privacy policies. However, what they fail to take into account is the widely accepted fact that privacy policies are rarely read [367] and that developers have difficulties understanding the legal language presented in them [368, 27].

4.4.2 Monetisation in a Data-Driven Economy

Our participants expressed their aim to monetise their apps in a privacy friendly way without using advertisements. This sentiment is consistent with the key message in the data protection frameworks we examined. The AADC mentions personalised marketing and advertising in their *profiling* section, stating that parental consent is required for behavioural advertising, as "'legitimate interests' is unlikely to provide a valid lawful basis for processing for this purpose" [17]. Similarly, Google and Apple do not allow third-party personalised advertising, with or without parental consent. Apple actually provides additional information for developers on business models and explains how best to implement these models [369]. However, they are geared towards maximising revenue by emphasising the importance of "optimizing with analytics" and "extensive user acquisition marketing campaigns" [370], which is slightly misaligned the principles advocated by the AADC, COPPA, and COPFE.

A few developers tried to adhere to the principles set out above, by making use of non-advertisement based monetisation. However, they faced several

barriers:

First, earning a sustainable income through subscriptions or pay-to-download business models, requires a large number of downloads, which is difficult to achieve for the average developer in a marketplace with over 3 million apps. Approximately 40% of the apps never gain more than a handful of users [371] and adding paywalls or making the app pay-to-use increases the threshold for a user to download it. It is also for this reason that a large number of our interviewees indicated that apps do not earn enough (10/20).

Second, merely having in-app purchases or subscription options is not enough. Participants expressed that earning money through in-app purchases or subscriptions also requires persuading users into making these purchases. At the same time, they felt morally conflicted in doing this.

Third, business models based on premium apps are not always accepted by the larger end user community. Several of our participants faced pressure to make their paid apps free, as their users could not afford to pay for it. Users either leave negative reviews or simply switch to a different app which can also fulfil their requirements. The competitive nature of the Google Play Store has put developers in a position to oblige with user's requests, and users generally want free apps. Developers are then forced to implement ads as the only alternative.

As a result, many developers in the interview study reported that they had to rely on in-app ads or sharing of data with third-parties to retain a business viability (14/20). This was further supported by our survey data, which shows that more than 79% monetised their app.

This phenomenon demonstrates the problem that guidelines do not address developers' need to monetise apps, nor do they provide enough guidance on this matter. First, while the need for advertising is evident, they do not specify which and when advertising networks are appropriate to use. This lack of regulation in the mobile advertising industry makes it challenging for developers to judge the boundaries of 'safe' and 'privacy-friendly' monetisation. Second, there is conflicting information between commercial guidelines, which focus on 'user acquisition' and data processing, and principles set out by the AADC and COPFE, which is not discussed by any of the frameworks.

4.4.3 Problems in Using Guidelines

Finally, we identified the lack of awareness and accessibility to guidelines as a key challenge for developers (11/20). As a result, our participants reported

to default to making use of terms and conditions set out by Google as a framework for child appropriate development (10/20).

However, there are a few problems with relying on recommendations made by Google. First, Google's "Designing Apps for Children and Families" guidelines are not directly aligned with the AADC. Importantly, they do not adequately address *data minimisation* principles which are core to the AADC. For example, the "Ads and Monetization" policy for children, by Google, is primarily focused on content based restrictions, such as 'inappropriate ad content', 'multiple ad placements', and 'use of shocking or emotionally manipulative tactics' [372], instead of addressing any privacy implications of ad-based monetisation.

Second, Google's guidelines and tutorials place their own products in the limelight, such as Google AdMob and Google Ad Manager [373], thereby increasing the adoption rate of third-party libraries in children's apps by major data controllers.

4.4.4 Working Towards Solutions

Our study has given us a detailed understanding of challenges developers face in designing privacy friendly and age-appropriate apps for children. Based on our findings and analyses, in this section we make concrete recommendations to address some of the problems highlighted above.

Include Developers as Stakeholders

One of the key challenges faced by app developers in designing apps for children is the lack of specific guidelines for this purpose, leading them to rely on their own intuition or follow practices set by major marketplaces, which may not always align with the best interests of children or prioritise their privacy. Our work highlights the importance of including app developers as stakeholders in the creation of design guidelines [368], as it is widely recognised that design guidelines should reflect stakeholders' values [345, 374] and be co-developed with key stakeholders [105, 375], such as children and families. Developers are the individuals who are directly responsible for creating and implementing the features and practices of apps, and their input can be crucial in developing guidelines that are feasible and practical for them to follow. By involving app developers in the development of design guidelines, it may be possible to address the specific challenges and needs of this group

and create guidelines that are more likely to be effectively implemented in practice. Including app developers as stakeholders can also help to ensure that the guidelines are informed by the realities and practicalities of app development, which is important in ensuring that the guidelines are relevant, useful, and applicable to the app development process, rather than being overly burdensome or unrealistic. Overall, the involvement of app developers as stakeholders in the creation of design guidelines can be valuable in promoting the ethical and responsible design of apps for children.

The Need for Supporting Documents

In order to promote the ethical and responsible design of apps for children, it is important to provide app developers with the necessary clarity, support, and resources. As our study found, app developers face several challenges in designing and implementing privacy-friendly practices in children's apps, including the lack of specific guidelines and the complexity of the data collection infrastructure of the mobile ecosystem. In order to help developers navigate these challenges, organisations like the ICO can play a crucial role in providing clarity and specific requirements for what constitutes "age-appropriate" or "privacy-friendly" libraries. This could include the development of a knowledge base of resources and services approved by regulatory bodies, as well as concrete recommendations for selecting privacy-friendly libraries.

In addition to providing clarity and support for app developers, it is also important to consider the motivations and incentives that drive app development practices. Our study found that app developers face practical constraints in designing and implementing privacy-friendly practices, such as the need to monetise apps through targeted advertisements. In order to promote the ethical and responsible design of apps for children, it may be necessary to address these underlying drivers and consider alternative business models that prioritise privacy and child well-being. This could include the development of best practices and resources for privacy-friendly magnetisation, as well as the promotion of alternative business models such as subscription-based models or in-app purchases. By providing app developers with the necessary clarity, support, and resources, as well as addressing the motivations and incentives that drive app development practices, it may be possible to create a more conducive environment for the ethical and responsible design of apps for children.

Additional Tools for Developers

Many developers mentioned that they do not fully understand how data is handled by data controllers and market leaders, or the libraries they use behave in unpredictable ways. This highlights the need for additional support through practical tools and resources.

Usability tools can be a valuable resource for app developers in promoting the ethical and responsible design of apps for children. By providing developers with clear and concise information about the potential risks and benefits of different approaches to data collection, usability tools can help developers make informed decisions about data collection and use [368]. This can be particularly important in helping developers to understand the implications of their decisions and make choices that align with their values and the best interests of children.

In addition, practical resources and guides can help developers understand the potential risks and benefits of using third-party libraries [376], and can provide them with guidance on how to evaluate and select libraries that align with their values and the needs of their apps. This can be especially useful in helping developers to navigate the complex and opaque landscape of data collection and use in mobile apps [377]. By providing app developers with the necessary tools and resources, it may be possible to support the ethical and responsible design of apps for children and promote a more privacy-friendly mobile ecosystem.

Overall, usability tools and practical resources and guides can be an effective way to support app developers in navigating the complex app development ecosystem and making informed decisions about data collection and use. By providing developers with the necessary support and resources, it may be possible to help them create apps that prioritise children's privacy and well-being, and contribute to the development of a more ethical and responsible mobile ecosystem.

Need for Industry Support

History has shown us that it takes a market leader to move the market. For example, in 2019 Apple restricted all third-party advertising and analytics. Similarly, their new iOS 14 operating system will require apps to explicitly ask its users permission to allow tracking services [96]. This approach to technology design has impacted companies whose business model centres around

data collection and sharing, such as Facebook [378]. For data tracking to come to an end on the Google Play Store, Google will have to push for similar policies. While the need for industry support is evident, it is unrealistic for Google to adopt such principles. Apple can afford to do this, because their advertising revenue is believed to only make up a small part of their total earnings [379]. Google, on the other hand, produced 83.3% of the 2019 revenue through the advertising industry [188], which is strongly grounded in data tracking and profiling.

While industry support is lacking, the HCI community plays in an important role in facilitating change in the ecosystem. For example, by raising awareness of privacy risks, making these risks more comprehensible, and facilitating the adoption of privacy preserving tools amongst (young) end users.

Alternate Monetisation Methods

The need for privacy friendly monetisation methods is already recognised by the wider community. For example, Apple has an initiative which facilitates privacy-friendly monetisation, called Apple Arcade [3]. End users have access to a set of apps through a monthly subscription, without in-app purchases or advertisements. While this is a good initiative, it is not a solution to the problem of data-driven monetisation. Apple Arcade only has about 100 games and studios were paid a fee for having their game included, which does not scale well to the large number of apps targeted at children.

Similarly, business models which do not make use of ads, such as the 'pay-to-download' business model, are not automatically privacy friendly. Paid services come with their own set of problems and ethical dilemmas. Firstly, it leads to the problem that privacy becomes a rather expensive commodity, creating digital exclusion and a lack of access to those who cannot afford it. It is widely accepted that marginalised groups [380] have diminished privacy, and commoditising privacy in a densely populated marketplace would only exacerbate the problem. Secondly, numerous studies have shown that paying for apps does not significantly reduce the amount of data tracking and collection [183, 184, 185]. Paid apps still contain third-party tracking libraries and require dangerous permissions. The fact that there is no trivial solution to this, highlights the need for additional research in this area.

Support for End Users

Lastly, it is also important to consider support for end-users. Research around end users has been focused on raising privacy awareness. However, research in raising users' awareness of age-appropriate design implications is limited, which can be a key barrier to privacy-friendly technology innovation. By not depending and waiting on higher level policy changes by developers and market leaders, such as the blocking of third-party analytics, end users can exercise a finer level of control over their privacy choices. For example, there are technologies currently in existence which inform users of trackers in apps and also give them the ability to control how these apps behave. Such apps are on the rise and also popularised by mainstream products. For instance, DuckDuckGo has released an app tracker protection feature built into their search engine app [2].

4.4.5 Limitations

We are aware of several limitations and methodological decisions which constrain our findings. Below we provide a rationale for this and suggest opportunities for future research which can build on our findings.

Surveys and Interviews

There are some inherent limitations to using surveys and interviews as research methods. Response bias can affect the accuracy of data [381, 382]. Subjectivity, time, and resource constraints can hinder the depth and breadth of exploration, and social desirability bias and difficulty in recalling past experiences can introduce response biases [381, 382]. Non-response bias and non-control over the interview environment may also affect data quality [383, 384, 385]. However, we did our best to overcome these challenges by meticulously designing our survey and interview protocols, ensuring a rigorous design for the interview, and maintaining a consistent setup for each interview.

[2] `https://duckduckgo.com/app`

Recruitment

In our recruitment we limited ourselves to the Android marketplace. The primary reason for this is that Android is the dominant operating system with a global market share of 75%[3]. Also, our research is motivated by the knowledge that Android applications are known to distribute data to third-parties on a large scale. While the presence of trackers and third-party libraries in Android applications is well researched [7, 361], the privacy landscape of iOS apps is less documented. Future research can benefit from including iOS apps and developers as well.

Additionally, we also limited ourselves to the western app development market, focusing on US and European regulations. This choice is motivated by regulatory interventions taking place in Europe, primarily ICO's enforcement of the statutory AADC, which will come into effect in 2021. These changes will have an imminent impact on developers who wish to publish apps in the UK Google Play Store.

Study Participants

Since participation in our study was purely voluntary, the participants who responded may have represented those with a better awareness of potential issues or took children's best interests more seriously than the average developer. Although this may have skewed our findings, our focus on the gaps in current practices and knowledge still provided valuable insights into a research direction of which little is known.

Similarly, our study captured only a small fragment of all Android developers. While the principles developers aimed to realise aligned with best practices, we do not claim that this is the case for all developers. It is likely that have malicious intents or are indifferent about children's privacy. However, we wanted to show that those developers who prioritise children's beneficence, well-being, and safety, are faced with real challenges and conflicts in supporting these priorities.

[3]https://gs.statcounter.com/os-market-share/mobile/worldwide

4.5 Conclusion

Through 20 in-depth interviews and 134 surveys with children's app developers, this chapter provided a much-needed developers' perspective regarding challenges and practices related to developing Android apps for children. We analysed the results of our data through the lens of 5 leading data protection frameworks which we introduced in Section 2.2.2. We sought to find out (1) what app developers perceive their responsibilities to be when developing apps for children, (2) what the main practices are to achieving privacy in apps, and (3) what the key barriers were for the adoption of privacy-friendly design features and practices set out in leading data protection frameworks.

Our findings indicate that app developers view their responsibility when designing for children as being motivated by both moral and legal considerations (RQ2.a). They recognize that the development process for children's apps differs from that of apps for adults, and that it is important to take into account children's developmental needs. To fulfil these responsibilities, developers employ various techniques to minimise unnecessary data collection and sharing, such as anonymising collected data (R2.b). Developers demonstrate a mindfulness of their role in protecting children's privacy and best interests while designing apps.

However, at the same time, we also identified key barriers and practices which stood in the way of designing for children's best interests (R2.c). Firstly, developers relied on third-party libraries from major data controllers for analytics and functionality. They often were not aware of alternatives or assumed them to be harmless to end users. Secondly, developers struggled to monetise their apps in privacy-friendly ways without relying on advertising networks. Market pressure and a lack of alternatives often forced them to adopt advertising as a primary source of revenue, thus making a trade-off between commercial success and children's privacy needs. Lastly, we identified a lack of awareness and accessibility to concrete and neutral design guidelines. Developers often relied on Google's app publication requirements, which are not always directly aligned with principles set out by the AADC. We call for (1) supporting documents to aid developers to navigate the opaque and complex development ecosystem, (2) research into alternative and privacy-friendly monetisation methods, (3) tools to support developers in auditing their apps, and (4) tools to empower end users in case developers do not keep up with age-appropriate practices.

We take these findings and recommendations forward into the next chap-

ter, where we look to draw out design requirements for tools that more concretely support developers.

5

How Should We Support Designing Privacy-Friendly Apps for Children? Using a Research through Design Process to Understand Developers' Needs and Challenges

Contents

5.1 Introduction 132

5.2 Research through Design 134

5.3 Methods 135

5.3.1 Ideation Workshop 137

5.3.2 Design Workbook 139

5.3.3 Speed Dating 141

5.3.4 Data Analysis 144

5.4 Interview Results 146

5.4.1 Overview of Participants' Reactions 146
5.4.2 Perceptions of Guideline Support 148
5.4.3 Requirements for Privacy-Friendly Development Libraries 153
5.4.4 Concerns and Needs for Compliance Checking Mechanisms 156
5.4.5 Concerns and Suggestions for Creating Privacy-Friendly Apps through Alternative Funding Mechanisms 160
5.4.6 Challenges for Rewarding Privacy-Friendly Apps . 162
5.5 Discussion 165
5.5.1 Summary and Key Findings 165
5.5.2 Addressing the Need for Credibility and Normalisation of Privacy-Friendly App Development . . . 166
5.5.3 Users' Incentives, Behaviours and New Practices . 169
5.5.4 Overcoming Systemic and Structural Barriers . . . 170
5.5.5 Limitations and Future Work 172
5.6 Conclusion 173

5.1 Introduction

In the last two chapters, we have taken a look at the privacy landscape of mobile apps and the role of developers therein. In Chapter 3 we performed an app analysis of expert-approved children's app to understand to what degree children are supported in understanding and exercising their privacy rights. We found that user facing privacy design features in children's app do not sufficiently support children to exercise any form of control over their privacy. At the same time, apps and third-party SDKs extensively track users' data, which is subsequently distributed in a vast and complex network of fourth-party data sharing entities.

In Chapter 4, we performed a study with children's app developers to understand developers' perspectives and motivations around the design practices. We found that developers in general do perceive a moral responsibility to protect children's privacy, but also face structural challenges due market

circumstances to always make privacy a priority. In addition, developers found the practices of third-party libraries and major data controllers are complex and opaque, making it difficult to make informed privacy design choices. Developers often lack practical support, for example through guidelines and SDKs, for their implementation of privacy-friendly features, and face systemic monetary constraints placed on them by marketplaces, leading to them having to make a trade-off between sustaining their business and protecting children's privacy [386, 270]. While we have a better understanding now of the practical and structural challenges developers face in creating privacy-friendly apps, few efforts have been made to support them through concrete tools.

Therefore, in this chapter we take a unique approach to understanding how these practical and structural challenges can be overcome [1]. We make use of a Research through Design (RtD) approach [387] to explore what future tools could look like to support developers in creating privacy-friendly apps for children. We were guided by the following research questions:

RQ3 How do app developers want to be supported in designing privacy-friendly apps for children?

- 3a What specific development tools do app developers require to enhance privacy in children's apps?
- 3b What requirements do app developers foresee for tools to support their development of future privacy-friendly apps for children?
- 3c How do app developers foresee addressing systemic obstacles imposed by major marketplaces in the development of privacy-friendly apps?

The socio-technical challenges we aim to address require potentially disruptive ideas to overcome the existing systems. For this reason, we made use of an RtD method, which is a co-design methodology that allows researchers to design and discuss ideas which may seem futuristic, disruptive and even technically infeasible to realise [41]. Using a set of design ideas generated by expert HCI researchers, we were able to engage with app developers more

[1] This Chapter has been published as: Ekambaranathan, Anirudh, Jun Zhao, and Max Van Kleek. "How Can We Design Privacy-Friendly Apps for Children? Using a Research through Design Process to Understand Developers' Needs and Challenges." *Proceedings of the ACM on Human-Computer Interaction 7.CSCW2* (2023): 1-29.

effectively, elicit their technological requirements for integrating privacy considerations as a part of the development process. Previous research has shown that RtD is particularly effective for identifying users' latent needs in support of 'wicked problems', which can be challenging to design for [387, 388]. To this end, we performed an ideation workshop with expert designers in which we generated 12 speculative designs aimed at supporting developers in creating privacy-friendly apps. We presented and discussed these designs with 20 children's app developers through semi-structured interviews to elicit their reactions and understand what their requirements are when envisioning the future of privacy-friendly app development.

Our findings confirmed the technical and systemic barriers identified in previous research and provided insights into specific thoughts and requirements from our participants regarding practical tools and guidance. Additionally, while participants expressed scepticism towards more disruptive solutions such as alternative marketplaces, they identified critical socio-technical barriers that hinder changes in current practices. This highlights the need for a multi-stakeholder, multi-disciplinary approach that takes into account the interplay of incentives and behaviours among parents, children, and marketplaces. Our results have important implications for design, the potential for power structure changes in the mobile ecosystem, and concrete ways to support developers.

5.2 Research through Design

The term 'Research through Art and Design' was first introduced by Frayling [389], discussing ways in which doing research could be of interest to the design community. It was not intended to be aimed at interaction design specifically, and only in later discussions was 'Art and Design', for various reasons, shortened to just 'Design' [41]. Nowadays most of the academic literature referencing 'Research through Design' (RtD) stems from the HCI community. RtD was formalised in the HCI community by Zimmerman in the late 2000s [387, 390], describing it as a "research approach that employs methods and processes from design practice as a legitimate method of inquiry". RtD is meant to be a method of generating knowledge through a design process, and is not intended to necessarily immediately produce a commercial product.

The theoretical literature on RtD is still in its formative stages, and is only recently gaining traction in the HCI community. As a result, there is no

one agreed upon definition of what RtD is, or how it should be conducted, or how knowledge through an RtD method should be generated. However, most practitioners agree that the process of doing design can constitute research and can lead to the generation of knowledge [391]: "The designing act of creating prototypes is in itself a potential generator of knowledge (if only its insights do not disappear into the prototype, but are fed back into the disciplinary and cross-disciplinary platforms that can fit these insights into the growth of theory)." [392]. Doing RtD generally involves the development of a prototype or design that shows a product which interacts with people in a way that was not possible before. This opens a discussion about how the future design space in that area could and should look like, focusing on identifying the *latent needs of stakeholders*.

RtD has been particularly useful for enabling researchers to identify opportunities for new technologies [387] by capturing a future form enabled with concrete and specific design artefacts. Previous studies have shown that these concrete embodiments have been effective for researchers and designers to explore the design space with the target stakeholders [393], such as integrating smart home devices at home settings [394] or introducing robotic care to the elderly without intimidating them [395].

For many researchers, RtD is regarded as an effective methodology for examining "wicked problems" through exploring design artefacts that are intended to transform the world from its current state to a preferred future state [387]. Wicked problems generally refer to problems that cannot be accurately modelled by the reductionist approaches of science and engineering due to conflicts between stakeholders [388]. We can regard the problem of designing privacy-friendly apps as a wicked problem, because structural and systemic features of the app economy are actively discouraging developers from creating privacy-friendly apps. By using an RtD approach we can propose provocative and disruptive ideas to developers to explore how stakeholders think the future design space for creating privacy-friendly apps should look like [41].

5.3 Methods

In this study, we seek to understand how we can best support app developers in building privacy-friendly apps and to uncover their latent needs, perspectives, and values which need to be embedded in designing future tools and

support systems. We made use of an RtD method, an alternative to other co-design methodologies, with its particular focus on gaining knowledge and research through the process of doing design. An RtD method allows us to start with creating an initial design space by involving design experts who can formulate potentially disruptive ideas [41]. The aim of this is to transgress what is currently possible within the limits of the current app ecosystem, thereby provoking developers to think about how they envision the future of privacy-friendly app development to look like and how they would like to be supported in this. This initial design space may provide a more useful starting point for particularly exploring 'wicked problems' that are challenging to capture and require creativity to imagine how the future could appear. As there is no strict definition of the experiments associated with RtD, we strengthened the robustness of our findings by drawing on existing HCI methods for our design activities and elicitation study. We made use of a three-phase process which we based on previous research using RtD [396]:

- First, we ran an *Ideation Workshop* with experienced HCI designers to explore a range of initial design ideas for supporting the creation of privacy-friendly apps, which we solidified as *Speculative Sketches* [397]. These are not intended to be perfect, but serve to quickly capture design ideas.

- Second, we converted the sketches into more intuitive and understandable illustrations, and included more detailed documentation of the design features for each idea, which we captured in a *Design Workbook*[398, 399, 400]. The design workbook is intended to work in a standalone format, where participants can engage with it and ideally understand the design concepts without needing intervention, and provide feedback through sketches and comments.

- Lastly, we conducted semi-structured interviews using a *Speed Dating* [394, 393] approach, where children's app developers were presented with the ideas from our design workbook one by one. They then expressed their thoughts, shared concerns and needs using the designs we proposed, and voted on their favourite design ideas. By using a speed dating approach, and being presented with a range of options, we aim to identify qualities participants are looking for in technologies to change the status quo [393].

5.3.1 Ideation Workshop

The key to a successful application of the RtD method is to ensure that it creates an integration between theoretical knowledge and technical engineering of the knowledge. Thus, researchers are expected to have explored the knowledge and design space *before* attempting to make a real thing. They are expected to go through an active process of "ideating, iterating, and critiquing potential solutions", to continually reframe the problem in order to get closer to "a concrete problem framing and articulation of the preferred state, and a series of artefacts—models, prototypes, products, and documentation of the design process" [387].

For these purposes, we made use of an ideation workshop [387, 396] in our study. Ideation workshops are typically short workshops that involve experienced designers from a related application domain to brainstorm and refine an initial design space. We organised a two-hour ideation and brainstorming workshop, which was initially planned to be held in person, but was transitioned to a virtual format due to COVID-19 limitations. Our workshop was based on the Design Sprint method [401], which is used to rapidly prototype and evaluate ideas, and included three stages: identifying 'How Might We (HMW)' questions, creating lightning demos (seeking for existing solutions in parallel domains), and solution sketching.

In selecting participants for the ideation workshop, we followed the Design Sprint recommendation to limit the workshop to "seven or fewer" people [401]. We were specifically looking for participants who had prior experiences in app development for children, knowledge about data protection and privacy for children, and optionally any industry experience. By maintaining these criteria, we ensured that participants could relate to the design challenges at hand and draw from their own experiences and knowledge to generate meaningful and expert-led design ideas. Using these criteria, we invited three final-year doctoral HCI researchers, a senior research associate from the same research group, a senior HCI researcher, and myself. All participants have extensive experiences in app development and user-facing designs for children. In addition two of the researchers and the research associate have industry experience in software and app development. All participants have experience in HCI research and are all very well-versed in matters relating to privacy for children in apps. The ideation workshop was not recorded, as we only needed the solution sketches to continue to the next phase.

At the start of the workshop, we contextualised the problem space by

explaining to the participants (researchers and designers) the specific social-technical challenges that app developers are facing that were identified in the previous work [270], which include the following:

- *The need for accessible privacy best practices guidance*: What can we support developers to translate existing policy guidance and regulations on privacy into practice? What should good and useful design guidelines look like for developers?
- *The need for designing tools to enforce best privacy practices*: What kind of technical toolkits are needed by developers for building privacy-friendly apps?
- *The need for addressing systemic issues in marketplaces*: How would developers like to be supported in a market undervaluing responsible development for users' best interests and an ecosystem lacking reward and recognition for such practices?

HMWs. In the first stage of the workshop, all the participants were asked to identify problem areas for these challenges by individually writing down "How Might We" (HMW) questions (e.g., "How might we make data protection regulations more accessible to developers?"). This was followed by participants reading through their HMWs to the group so that each participant could vote on the three most interesting ones they wanted to tackle as a group. The three top voted HMWs were used as a starting point to brainstorm solutions in the next stage.

Lightning demos. In the second stage of the workshop, participants were asked to go online and seek existing solutions to the HMWs from similar problem domains to inspire ideas for solution sketching. These were then presented in short demos for all participants so that they could become familiar with them. It was key that all participants had prior knowledge and experience with designing mechanisms to promote better user privacy awareness or translating data protection guidelines to more actionable design candidates, to ensure the effectiveness of this stage.

Solution sketching. In the last stage, each participant was asked to reflect on the proposed design options and individually create 2-3 low-fidelity *Speculative Sketches*. This was followed by a general discussion as a group reflecting on useful features and design rationales.

5.3.2 Design Workbook

After the workshop, I and the senior HCI researcher went through all the sketches and categorised them according to the three social-technical challenges presented in the ideation workshop. To ensure the collection of sketches as a whole would uniformly represent the research questions, we merged closely related concepts and discarded concepts which did not directly address the research question. For example, we discarded the initial sketch of a Privacy Guard concept, which was aimed to block network traffic to and from any advertising and tracking domains, because we felt this was aimed more at children rather than supporting developers.

We were left with 12 design concepts, which were redrawn to ensure uniformity. We added brief descriptions to highlight the core concepts and interaction features, and ended up with 12 concepts as our design workbook, illustrated in Figure 5.1. The full design workbook is available in Appendix B. A summary of the designs can be seen in Table 5.2.

These designs address the three identified problems in the following ways:

- **Supporting accessible development guidance.** Our first three ideas were aimed at reducing the complexity of guidance for privacy-friendly design [270]. The first design, a *Dos and Don'ts Checklist* `[D1]`, was aimed to concretise and simplify requirements set forth in common legal documents, such as GDPR and ICO's AADC. This way, complex principles are broken down into technical requirements, which developers have been shown to struggle with [25, 24]. We also proposed a more formal *training course* `[D2]`, providing them with an opportunity of self-education and certification. This would allow developers to get a more holistic and broad understanding of important aspects in designing for children, including rationales and motivations about why certain design features would be important. Lastly, *Requirement Matrix* `[D3]` was proposed to collate requirements from various marketplaces and legal frameworks. As apps are often launched into an international market, such a matrix can potentially enable developers to quickly assess their compliance with requirements from different marketplaces (e.g., Google and Apple) and different jurisdictions (e.g., US and EU).

- **Providing tools to support best practices.** This category of designs was aimed to support simplifying compliance assessment and

proposing SDKs that can improve transparency and act in children's best interests. We proposed three methods to help in matters related to compliance. Firstly, we wanted to involve additional stakeholders (such as parents) in a crowd sourced mechanism to assess compliance with common data protection requirements, e.g., the AADC (*Wisdom of the Crowds* [D4]). Secondly, we proposed an automated method of doing this (*Machine over Mind* [D5]), and thirdly we proposed this compliance be carried out by an authoritative regulation/standardisation body (*Universal compliance service* [D6]). Furthermore, we also wanted to explore how developers may perceive the trade-off between carrying out additional development efforts in order to commit to transparency and children's best interests. We therefore proposed SDKs which developers could simply integrate into their apps without additional efforts, thereby removing any friction in this process. The *Plug-and-play self-control tool* [D7] adds a new interface to an existing app allowing children and parents to control screen time and change privacy settings. The *Parental assistance* [D8] tool allows developers to generate guidance for parents which subsequently can be accessed through the app.

- **Addressing systemic challenges.** In our final set of design ideas, we wanted to explore how we can overcome systemic challenges arising from marketplaces to incentivise developers to adopt privacy-friendly development principles. We looked at two approaches in achieving this. Firstly, we sought out to help developers build recognition amongst consumers. Motivated by earlier design work to help users recognise data protection practices through 'privacy labels' [402], we proposed self-certified *Public Pledges* [D9], awarded by developing technology according to certain standards, and a *Badge of Honour* [D10], provided by a credible institution for upholding certain standards. Secondly, as targeted advertising is a commonly used method for developers to monetise their apps [270, 10, 34], we looked at concretely providing alternative methods of financial support. Inspired by the open source innovation model and the decentralised data governance for promoting self-autonomy [403], we also explored how developers perceive alternative marketplace models, such as *Patreon and Crowdfunding* [D11] for privacy-friendly apps or developing an *Unlimited Arcade* [D12] for promoting privacy-friendly and age-appropriate design approaches.

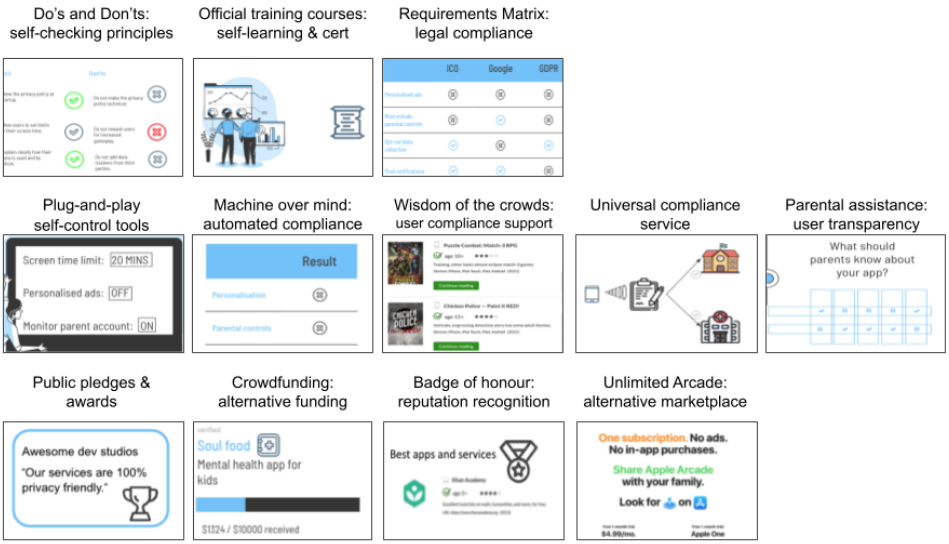


Figure 5.1: An overview of the 12 concepts included in the design workbook. The text above each image icon provides a brief title of the design approach and a detailed description can be found in the supplementary materials.

The design workbook was originally meant to be presented in a physical format, allowing participants to actively make notes and add ideas. However, as we conducted the workshops online, we transitioned to a digital format and presented the ideas as a slideshow through screen sharing.

5.3.3 Speed Dating

The speed dating design method [394, 393] draws on the analogy to a traditional social interaction that helps singles find a romantic partner, by providing rapid encounters with a series of potential romantic partners. The objective is to help participants to gain a better idea of what they look for in a partner and what they really want and need. Similarly, the speed dating design method places target stakeholders in a situation that enables them to sample a series of how the future may look like. After rapidly experiencing several possible futures, the study participants would then be guided to reflect their implicit needs and barriers for adopting these possible futures. Because speed dating allows participants to reflect on concerns and needs

which would not have arisen during fieldwork, it is effective to explore design opportunities in depth. The key for applying a speed dating design method is to put study participants under a situation that is familiar to them (such as recording TV programmes at home). Thus, during our study, when presenting each design idea to the study participants, we encouraged the app developer to imagine how they may make use of the design in their actual app design and development process.

Participants

In recruiting developers, we approached development studios, product owners, and indie developers. We specifically sought out participants who have developed apps for children or have been responsible for the development of apps for children. We therefore did not exclude participants who held executive or directorial positions, as they often have an important say in the way apps are designed.

We sought out our participants through the use of popular search engines, such as Google and DuckDuckGo, and made use of keywords such as "Kids App Developers UK", and "Game Studio UK". We verified that companies were based in the UK through the 'contact' page that was mostly available on their websites. This page also often included an email address, which we used to establish contact. In many cases, we had an initial video call with a representative at a company, such as the head of marketing or communications, who circulated our recruitment message internally. Using this method, we recruited a total of 20 participants, who were compensated with a £15 Amazon gift voucher for participating.

In total, we had 20 participants, with most participants being located in the UK. Participants not located in the UK still developed apps for the UK market. Two participants were female, the rest were all male. The participant characteristics are described in Table 6.1. Participants had varying roles in their organisations, with different levels of professional development experience in the sector, ranging from 15+ years to just starting out (¡1 year). The roles of Director, Product Owner, Manager, and CTO, held by 14 of our participants, were included in our study because they had a significant influence over what the apps should look like and which principles they ought to adhere to. These participants would have direct/close involvement in ensuring the privacy-friendly requirements set out by the ICO and the marketplaces. The roles of Developer and UX Designer were held by

Table 5.1: Table containing descriptive characteristics of the study participants. While all participants produced apps for the UK market, some were located in a different country.

Participant	**Country**	**Gender**	**Role**	**Years of Exp.**
P1	UK	M	Director	16
P2	UK	M	Operations director	15+
P3	UK	M	Head of product	10+
P4	UK	F	Head of production	9
P5	UK	M	Developer	< 1 (4 weeks)
P6	UK	M	Developer	6
P7	UK	M	Product designer	6
P8	UK	M	Product owner	11
P9	UK	F	Managing director	15+
P10	UK	M	Technical director	20+
P11	UK	M	UX Designer	3
P12	Germany	M	Product owner	5+
P13	UK	M	CTO	10+
P14	UK	M	Developer	3
P15	UK	M	Developer	5+
P16	UK	M	Product owner	10+
P17	UK	M	Product owner	11
P18	UK	M	UX Designer	8
P19	Bulgaria	M	Program manager	4
P20	Lithuania	M	Product owner	10+

the remaining 6 participants, and all except for one had experience in the indie app development. One of the participants had just started their app development career, who was also included in the study as we felt that he could express which areas of privacy-friendly app development would need improvement for people just starting out.

Procedure and Data Collection

We conducted 20 speed dating semi-structured interviews in the summer of 2021 using remote meeting software, such as Microsoft Teams or Zoom,

depending on the participants' preferences. Although this may not be the observational studies that we would intend in an ideal situation due to the disruption of the pandemic, we believe this closely resembled the app building situations as those were also carried in a computer-based context. All discussions were audio recorded with the participants' consent. Each session consisted of three parts. We started with a warm-up session in which we explained our research objectives and challenges. We asked about participants' experiences in designing apps for children, what they think is important to keep in mind, and what they think challenges are for developers in privacy-friendly design. Then, the researcher shared their screen to display the design workbook and invited the app developers to picture themselves using the design ideas during their app designing, building, debugging, or publishing situation.

With every concept, we gave participants some time to read the description and view the sketch and allowed them to ask any questions for clarification. After participants described their initial reactions, we followed up with a series of questions to explore their sentiments, value alignments, and why participants liked or disliked the features; for example, "How would you feel if you had to pay for the certificate?". We explained to the participants that they could be honest and critical in their feedback, even if they felt negatively about a design idea, without adverse consequences. We concluded each interview with a summary slide which had all of the concepts briefly listed. We asked participants which concepts they particularly liked, would like to see implemented in practice, and would be meaningful in their development practices.

Our study has been approved by our Institutional Review Board. Participants signed consent forms and were informed in advance about their rights in the study. For example, they were informed that all data would be anonymised and that they could withdraw from the study before a specified date. The full interview procedure is available in Appendix B.

5.3.4 Data Analysis

Our reported results are predominantly based on in-depth discussions with app developers during the semi-structured interviews. All recorded interviews underwent transcription and any personally identifiable information was anonymised. Our data analysis followed a thematic approach [404], enabling us to develop codes and themes related to developers' *challenges,*

perceptions, requirements and values.

In our thematic coding process we emphasised the consensus-building aspect of the analysis. The transcriptions were divided into two equal-sized sets, and two experienced HCI researchers, myself and a second researcher, independently analysed the first set of transcriptions. This initial analysis allowed us to generate an initial set of codes. Importantly, our coding process involved ongoing discussions between the two of us, resulting in a consensus on code development [356].

Following the independent analysis, we convened to consolidate and reconcile the codes derived from the initial analysis. This collaborative effort resulted in the creation of a shared codebook, which provided a common reference point to ensure the consistent categorisation of data across the entire dataset.

The remaining half of the transcriptions was coded by myself using the established common codebook. We reached a point of code saturation, wherein no new codes emerged from the data, after 13 transcripts. During the thematic coding process, a total of 93 unique codes were generated to capture the diverse range of themes and patterns within the data. After approximately 16 transcripts, we observed that no new themes or insights emerged, suggesting that data saturation had been attained [405]. A detailed list of all unique codes derived during the analysis, can be found Appendix B.3.

In parallel with the coding process, we created a mapping between the identified codes and the 12 design concepts under consideration. This mapping enabled us to gain a holistic overview of how each design concept was perceived by the study participants. It facilitated a nuanced understanding of the developers' perspectives and their evaluation of the design options.

In our analysis we did not specifically look out for differences between subgroups within our participants. While we found that participants indicated preferences for using certain design ideas within the capacity of their jobs, they often viewed and analysed these ideas from a viewpoint as independent from their official job roles as possible.

Interviews lasted between 38 and 75 minutes. The total duration of the recordings is 1043 minutes and the average session length is 52 minutes (SD=10.2).

Table 5.2: List of speculative design ideas which arose as part of the Research through Design ideation workshop

Design	Name
[D1]	Dos and Don'ts Checklist
[D2]	Courses: Making it official
[D3]	Requirements Matrix
[D4]	Wisdom of the Crowds
[D5]	Machine over Mind
[D6]	Universal Compliance Service
[D7]	Plug-and-Play Self-Control
[D8]	Parental Assistance
[D9]	Public Pledges & Awards
[D10]	Badge of Honour
[D11]	Patreon and Crowdfunding
[D12]	Unlimited Arcade

5.4 Interview Results

Here we report requirements and concerns that app developers reflected during their interaction with our design options. We start with an overview of participants reactions to our 12 design options, and then we describe the key themes which emerged from our analysis: (1) perceptions of guideline support; (2) requirements for development libraries; (3) concerns for compliance checking; (4) suggestions for alternative funding mechanisms; and (5) challenges for recognition of best practices. We have summarised the requirements and barriers formulated by our participants in Table 5.4.

5.4.1 Overview of Participants' Reactions

Table 5.3 provides an overview of participants' reactions to the different design concepts, listed as either Positive, Neutral, Negative, or Mixed (i.e., an idea having almost equally positive and negative reactions to it). Participants often explicitly expressed whether they liked or disliked an idea, or had mixed feelings about it. For example, P13 said the following about the *Requirements Matrix* [D3]: *"This is excellent. This talks to a lot of the things that are missing from the checklist"*. All participants had at least

Table 5.3: Overview of participants' reactions: lime indicates a positive perception, red indicates a negative perception, magenta indicates an idea being both positively and negatively received, and grey indicates a neutral reaction. The columns display the individual participants' reactions, and the rows refer to the design ideas.

Pts	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
[D1]																				
[D2]																				
[D3]																				
[D4]																				
[D5]																				
[D6]																				
[D7]																				
[D8]																				
[D9]																				
[D10]																				
[D11]																				
[D12]																				

Positive Negative Mixed Neutral

two positive reactions to the design ideas, and each idea had at least one participant who reacted positively to it.

In general, most participants reacted positively towards ideas which help make guidelines more accessible. They felt that current guidelines and regulations are complex to understand, and that a simple breakdown would help during the development cycle. Specifically, the *Dos and Don'ts Checklist* [D1] and the *Requirements Matrix* [D3] were received well, because they are non-intrusive, i.e. they do not have to be technically enforced and there is no cost associated with owning or consulting such a resource. Similarly, participants also liked approaches which help with marketing and increase exposure to customers, such as the *Public Pledges & Awards* [D9] or *Badge of Honour* [D10]. Such tools do not fundamentally affect apps and there is no deterring cost associated with using them.

Participants were *generally sceptical* about approaches which aimed to tackle structural problems. For example, through *Unlimited Arcade* [D12],

a subscription-based marketplace for privacy-friendly apps, we aimed to circumvent the extreme competition present in current marketplaces. However, participants felt that Google and Apple have a sufficiently strong monopoly that such approaches will fail to gain such traction. Similarly, we had expected that *Patreon and Crowdfunding* [D11] would be positively received, as it essentially provides an additional revenue stream. However, participants did not believe that parents would see the benefits of supporting apps on such a platform and that it would run into the similar issue that a few apps would procure most of the funding.

Participants were *mostly negative* about approaches which tried opening a communication channel with parents. One such example is the *Wisdom of the Crowds* [D4], a platform allowing parents to provide feedback. Participants felt that parents could not be trusted to provide expert feedback and that it may introduce a policing situation, which would add even more complexities overcoming market competition. Similarly, they felt that *Parental Assistance* [D8], which automatically generates guidance for parents about privacy risks in applications, would act as an extra deterrent towards potential customers, meaning developers would be punished for trying to do the right thing.

We did not find any noticeable differences between participant subgroups in their perceptions of how our proposed ideas can benefit the developer communities, however we noticed differences in their preferences for tools they would use in their own work. For example, we found that participants who had an executive or managerial role, indicated the *Requirements Matrix* [D3] to be useful for the type of work they do, while developers could see themselves using SDKs, such as *Plug-and-play self-control tools* [D7], to help speed up development. However, in their analysis of how these tools could benefit the wider development communities, they often took a viewpoint beyond their official job title, leading to varied and nuanced insights.

5.4.2 Perceptions of Guideline Support

Our first set of design ideas aimed at helping developers understand best privacy practices when designing apps for children. We focused on clarifying rules and requirements set forth by regulations (such as GDPR and COPPA), human rights organisations and public bodies (UNICEF and ICO), as well as marketplaces (Google Play and Apple App Store). We proposed three tools to address this: *Dos and Don'ts Checklist* [D1], *Courses: Making it*

Table 5.4: Requirements and barriers to adoption of tools and technologies to assist in privacy-friendly app development, as formulated by our study participants.

Needs and requirements	**Socio(-technical) barriers**
Guidance for privacy-friendly app development needs to be actionable, provide international support, conflict resolution, and have clear legal implications.	Guidance should be backed by trustworthy and credible organisations which allows developers to negotiate the importance of privacy-friendly app development.
SDKs should not add development overhead and should support users' experiences.	There is a need for users' awareness of the importance of privacy and the normalisation of privacy-friendly app development in the development community.
Compliance checking should happen during the development process, and should be constructive in providing actionable feedback. Compliance checking after development will undermine an app's competitive position.	Incorporating compliance checking means additional time, effort, and money spent in app development, which means that developers should already be committed to privacy-friendly app development.
Need for gradual changes in the current ecosystem, which do not strongly affect users' current habits (e.g., by having them navigate away from the mainstream marketplaces).	Need for recognition of privacy-friendly development practices by end users and the need for new and more wholesome measures of success by the marketplaces.

Official `[D2]`, and the *Requirements Matrix* `[D3]`. In general, participants reacted positively to the simplicity and non-intrusive nature of these ideas, but they would also like sufficient technical depth to help them translate high level principles to implementation, sufficient coverage to adapt to frequent regulatory changes, and support from credible organisations to encourage adoption.

Need for Actionable Guidelines with Clear Legal Implications

Participants confirmed findings from previous research that there is a general lack of understanding of what privacy-friendly and age-appropriate apps should look like, as well as a lack of support in addressing this gap. They found current guidelines too complex and largely inaccessible:

> *"I'm probably one of the few people in the world that read the entire bloody GDPR document, the whole stupid thing. I got to the end of it and it was, 'now what?' It's just so dense, nobody reads it."* — P10

They liked the idea of having a simplified checklist which breaks down technical rules and regulations by removing jargon and legalese. They found it important that it is accessible for a wide range of audiences involved in development, including novices and non-technical team members. The advantage of checklists is that it can provide a quick overview of what is important without having to make significant investments in reading and understanding large documents. Importantly, participants had positive experiences in working with checklists in closely related environments, such as quality testing in Xbox game development, which increased their confidence in having checklists for children's app development.

> *" So you know, doing Xbox game development, you have messages that you have to show in certain circumstances if you're auto saving. You absolutely have to show this icon. So having an absolute list of: 'you must follow these rules as a developer', that works absolutely fine. "* — P10

However, participants also indicated that in some cases oversimplifying best practices is not practical. Not all principles are equally straightforward, with some requiring more context and technical depth. For example, participants wanted more explanations about why certain rules have to be implemented and *"it would be useful in understanding where it would come from"* (P10). They wanted clarity about the origin of the principles, suggesting adding a reference or hyperlink pointing to the source document.

> *" I think saving time and giving the reference link to sort of them to go and read about it, or mock it, and it will be used. If it can be*

developed in a way that developers say, 'I don't know about this, actually let me just go and have a look at this and take me to the right place, the right link, as opposed to just the homepage', that I think would be quite useful." — P2

In addition, many participants expressed that it was key to minimise the friction and time between translating from principles to actual implementation, for example having exemplar implementations in the formats of mock-ups or wireframes would be tremendously helpful with uptakes.

"I think it'd be good to have an idea of how you would implement that, and how it might look. ... Designers particularly, when they're starting to look at this, have an idea of how it might be implemented and how we go about doing it." — P7

Lastly, several participants described that it's important to have clarity on whether requirements were: legally bound, nice-to-have, or enforced by marketplaces.

'The ICO and GDPR, as far as I am concerned, is legislation and the governing body that manages that legislation. There's another dimension to this, which is: (i) these are like legislative, nationally legislative, potentially globally or a European; (ii) these are recommended or leading bodies that make guidelines and recommendations, and (iii) these are marketplaces essentially. So I think there's another dimension in the categorisation of these." — P8

They would like to retain choice and autonomy on what to implement, as the development of some features may be beyond the developer's budget. Moreover, when developing for clients, the development cost of every feature must be justified, which is ultimately the client's decision.

Need for International Regulatory Support and Conflict resolution

Because apps are often launched into an international market, a large number of participants indicated that too often they had to abide by the rules and regulations of different countries and marketplaces. However, these rules are complex, ever changing, and contain a lot of legalese, and participants indicated that clarifications in this landscape are much needed.

> *"Unity has their own terms and conditions on how you use their analytics. A lot of people don't know this, but Unity up to a particular point had their analytics for you. They were turned on no matter what you did for a long time, even with COPPA and GDPR. So, you couldn't be technically COPPA and GDPR compliant using Unity."* — P13

In addition, several of these participants also mentioned that marketplace rules change frequently and can often be unpredictable. For example, one participant explained how his app was removed from the Chinese app marketplace without warning due to a change to the rules.

> *"They basically they just blocked it all of a sudden. We put an update through and then that app was just gone from China. It's just, you don't get a warning, you don't get an email, it's just not available. You know, no warning."* — P12

While this change might have been reflected in the documentation on the website, the participant was never notified of this. Any tool addressing legalities and marketplaces requirements could benefit from notifying developers of critical rule changes, including guidance on how to implement these changes into the app.

Lastly, some participants were worried that marketplace rules, best practices, and regulations might contradict or conflict with each other, in which case they would like guidance on how to resolve these conflicts.

> *"And it might be worth as well having where things might conflict. So maybe GDPR might have a regulation that conflicts with some things that Google require of apps. So that you can resolve that as best you can. "* — P14

Need for Trust and Credibility in Courses and Certifications

Participants admitted that there is a need for certification of developers' practices of designing for children. However, they were less convinced about a formal or traditional course, because they were worried that it might take too much time and that companies would not be willing to pay for it:

> *"The main reason why, if you don't normally get these sorts of certifications from global academic institutions like [university], you don't normally see this in an online world because it's a bit like a Wild West. There is no set rules and guidelines and certificates. There is a range of set of arbitrary skills that you can learn, unless you do something like Udemy or whatever. But as a business owner that wouldn't carry as much weight as such."* — P1

In addition, one of the concerns many participants had with adhering to privacy-friendly design principles was that they felt that 'formal education' does not translate well to the wild west of the online world, where limited rules and expectations of best practices exist. Several participants thus expressed that strong credibility associated with the course certification, backed by governing bodies, could be essential to offset these concerns and encourage updates by the community:

> *"I think when it comes to safety for children, the number one thing is making sure it's from a reliable source. So ICO would pull on that. But it's more about having something that's large enough of an industry name, that everyone knows. Something like GOV.uk. I think if people had something published, that was, 'this is how you do it', and 'this is almost like the law, this is the best practice', that's the best way to go forward."* — P11

5.4.3 Requirements for Privacy-Friendly Development Libraries

In order to make it easier to integrate privacy-friendly design features into apps, we proposed off-the-shelf libraries which developers can easily import and use: *Plug-and-Play* `[D7]`, a privacy control panel, and *Parental Assistance* `[D8]`, providing privacy information about the apps for the parents. We found that participants were largely deterred by the potential negative impact associated with integrating these tools in their app developments, for example that it may deter parents or clash with the native app branding, and therefore would prefer to wait out for a widespread adoption of these features to prevent feeling 'standing out'.

SDKs and Libraries Should be Easy to Integrate and Known to be Compliant

In general, participants liked the idea of having libraries and SDKs which make privacy-friendly design easier. They indicated that developers like to rely on libraries, as it reduces development time and costs, and eliminates the need to re-implement software. Importantly, such SDKs would be guaranteed to already be compliant with any privacy-friendly feature requirements, making it a convenient and easy way to become compliant.

> *"It seems to me that, probably the idea of the SDK makes a lot of sense, and to put as much of this into that, so that you can kind of market your app as being compliant with all of this stuff, it's had all of these things approved you know. It's kind of been through these various tests."* — P12

However, they also pointed out that it is essential that the library is easy to use and is lightweight. One of the advantages of relying on libraries, is that it defers responsibility to an expert third party which is knowledgeable in the area of privacy-friendly development.

> *"Being able to defer a responsibility to another party, we like being able to say something is no longer our responsibility. Especially if it's something that's really technical and if it's stuff that we don't want to have to concern ourselves too much with."* — P10

To this end, participants indicated that it would be valuable to have a centralised location where they can easily access libraries that meet certain compliance standards. This repository would allow them to quickly find and use libraries that have been vetted for compliance, rather than having to search for and assess the compliance of each library individually. Having a central repository of compliant libraries could be especially useful for organisations that have strict compliance requirements:

> *"I know Amazon, a lot of their stuff that they're offering now, the service provisions is literally incorporated as part of that. So, I think having a library which just manages a lot of that. I'm not sure how that would work practically. But definitely having access to libraries, you know, on GitHub or GitLab or wherever you want to kind of put it."* — P8

SDKs and Libraries Should Support Users' Experiences

Several participants expressed their concerns that the adoption of these libraries may affect users' experiences. They feared that users' experience to be supported by each app could be different, which may be difficult to generalise in a third-party library. Removing user-facing features by following the standards set in the development tools may adversely impact user experience, potentially be detrimental to user retention, sales, and other monetary aims. Instead, they suggested implementing libraries on a higher level of abstraction, for example as a skeleton framework where the underlying mechanics are functional, but the user experience can be tweaked.

> *"I think it'd be good to have an idea of how you would implement that, and how it might look. I wouldn't take it as far as showing, 'here's a finished thing', I'd maybe keep it as a wireframe to say, 'here's some boxes of how you might do that'. So I think it'd be good to kind of get that documentation around it. "* — P7

In addition, there was a perception that privacy-friendly features which are user facing may act as a deterrent, and parents may refrain from installing the app due to its highlighted negative privacy signals, resulting in developers being penalised for doing the right thing.

> *"Parents aren't thinking about it. So we're penalised for association, as the well-meaning company. And the company that hasn't got involved in parental communication about this issue, goes scot-free, because they haven't got the bandwidth to think about it."* — P16

The Need for Acceptance of Privacy-Friendly SDKs for Implementing Privacy-Friendly Features

While participants indicated their interests in the idea of libraries and SDKs, as they can significantly reduce the threshold for engaging in privacy-friendly design practices, participants also indicated the need for the normalisation of the use of privacy-friendly features in apps before they would consider adopting them themselves.

Firstly, participants felt that there is little awareness amongst parents about the importance of privacy and other child-friendly features in apps. For

example, they indicated that parents will not specifically seek out information presented apps aimed at them, and in many cases, parents are not involved in the installation and onboarding process.

> *"Oftentimes, the parents are not there right ... it'd be the child who opens the app for the first time, and they can't read you know, for my audience, they can't read. They are fantastic at finding out what to tap, so they will tap the screen and find a button that closes the privacy policy maybe."* — P17

As a result, they indicated that adding features aimed at parents would perhaps only discourage, confuse, or dissuade them from using the app, which means that costs associated with implementing such features ultimately outweigh its benefits. Similarly, participants were also concerned about how adding such features would situate them amongst competitors who did choose not to engage in such practices, thereby perhaps providing them with an additional competitive edge.

We therefore asked participants what changes could be made that could still incentivise developers to consider integrating such privacy-friendly features. Our participants then indicated that they would be more likely to use privacy-enhancing libraries and SDKs if it had been standardised or if other developers and apps were using them as well, as this would mean that end users would specifically seek out such behaviours in apps.

> "*It just becomes universal. 'This control panel is what you have on every app that is made for children'. Because if it becomes easy for the devs to do, and then it becomes widespread, then it creates a model of expectations.*" — P4

5.4.4 Concerns and Needs for Compliance Checking Mechanisms

To help developers comply with privacy-friendly design principles, we explored design ideas for compliance checking based on (1) engaging with parents (*Wisdom of the Crowds*) `[D4]`, (2) through an automated tool (*Machine over Mind*) `[D5]`, and (3) outsourcing to a third party (*Universal Compliance Service*) `[D6]`. We found that it is important for developers to receive constructive feedback from credible sources. In general, they would rather not rely on parents to be the gatekeepers of assessing privacy principles.

Feedback Needs to be Credible

In general, participants liked having a tool which independently assesses apps for their privacy and age-appropriateness. Participants indicated that it was difficult to be neutral about their own app, making it more desirable to defer it to an expert third party. However, participants were concerned that a tool like *Machine over Mind* [D5] would be *"nearly impossible to implement due to the variations and interpretations the system could make without the contextualization"* (P8), leading to *"unreliable results and feedback"* (P3). For example, as implementations differ per app, it is difficult to assess that consent is appropriately requested. This lack of trust in the feedback and outcomes deterred some participants from using it, arguing that it might produce false positives or return erroneous feedback which would require time and labour to rectify. They were worried that even if the tool is free to use, there is a missed opportunity and time cost associated with it.

> *"You know, you need to be compliant with accessibility, legislation. Which is different in the US as it is in the rest of Europe. And this is the thing that people don't get. Once you layer all these things on, you've spent a ton of your time designing for compliance, and very little of your time designing for the user. And most of these things invariably cause user attrition."* — P13

Instead, participants indicated that it is better to focus on quantitative measures, such as analysing third-party libraries and data trackers, and focus on a subset of features rather than focusing on everything related to privacy or child-safety.

Similarly, participants were not keen to involve parents to review and assess apps (*Wisdom of the Crowds*) [D4]. In general, they felt that parents are not the right judge to assess apps for their privacy, safety, and age-appropriateness. They thought parents would rather focus on reporting technical issues of the app, where managing these reviews can be a horrendous process.

> *"Again, having worked with parents, the level of subjectivity and personal opinion is so broad. You get some people that are hyper sensitive, and even having access to the child's first name and you get some people that are happy to have all their data and stuff shared with their child on Facebook when they're six years old. "* — P8

Instead, participants preferred it if a panel of experts was appointed to assess and review apps. This way, they would be more likely to receive feedback which directly relates back to established privacy standards, rather than other subject measures of assessment.

Feedback Needs to be Detailed and Constructive

We also asked participants whether automated compliance checking is redundant, since Google and Apple have their own review process in place. However, a large number of participants indicated that the feedback provided by these large platforms is not sufficiently detailed, often requiring a lot of 'detective work' to figure out what is wrong. Similarly, they would not want our tools to be framed as a static safety test which apps are required to pass. Instead, they want constructive and detailed feedback, including suggestions for changes, which are expected to be made. Participants indicated that if the tool resembles a safety test, they will try to convince or cheat the system rather than putting it to good use. For example, they would alter metadata or make superficial cosmetic changes which ultimately does not change the underlying functioning of the app.

> *"I would be trying to convince the machine that we've done it. Not even really caring whether or not we haven't. So, well we can get a checkbox on that by doing this. So, let's just.. You would end up playing the system in order to get the check boxes. So, I wouldn't care whether or not my parental controls worked."* — P10

Compliance Checking Needs to be Effortlessly Integrated with the Development Cycle

Participants liked the simplicity of uploading an app somewhere for assessment, because it is accessible and simple to use. They compared it to security or SEO checkers which they have had positive experiences with before. However, participants were worried that it could produce a lot of friction and add time in the development process. They stated that this could happen legitimately, for example as privacy-friendly app development might require fundamentally adding features or changing existing features, or due to errors and false positives which are prone to occur in such automated systems. Ultimately, if one were to use such methods, it would require them to have

to be committed to privacy-friendly app development, otherwise they simply choose not to bring this additional work upon them.

> *"If I really wanted to do an in-depth check, I would go to you as opposed to go to them [Google]. But the only downside with that is, you might throw up more alerts that would pass their machine, but it wouldn't pass here. So you'd be giving yourself more work to do at the end of the day. But if you were serious about what you wanted to do, you would be doing it regardless."* — P5

However, a number of participants were concerned that a test with a finished app product seemed to come at the wrong stage of the development cycle. If fundamental changes need to be made to an app, this would be costly and take a lot of time. It is unlikely that developers would engage with this. Instead they advocated for a Privacy-by-Design approach, proposing complementing these design ideas with the *Dos and Don'ts Checklist* [D1].

> *"That's kind of what I see the app stores doing at the moment. And they say, actually we're not allowing that, or we're retrospectively changing the rating on that because of our compliance. ... It's then a hoop I've got to jump through as a developer. If I have to jump through it as a developer, fine I will because I have to, and it would be annoying. As long as I had all the checklists and the other stuff before. I then need that checklist with 'what's required and why it's required' that I can follow, to make sure I'm compliant. So that when I fill the form in [marketplace submission], I've got a reasonable chance of knowing that it's going to be okay."* — P10

Compliance Checking Should Not Undermine an App's Commercial Potential

A strong sentiment from the participants was that they did not want compliance checking of apps to negatively impact their reputation or revenue. This was particularly true with *Wisdom of the Crowds* [D4], as they were worried that parents would suddenly become the gatekeepers of privacy-friendly apps. For example, participants felt that parents would only review apps if they have had a bad experience with it or that parents would focus too much on the negative aspects.

> *"I feel like parents are more likely to actively feel outraged about something as opposed to 'I'm just going to fill this out' right? So, I guess the thing I'm battling with is the motivation for a parent to sign up and do this."* — P7

Another common concern that participants had was that the mechanism of *Wisdom of the Crowds* [D4] could provide an opportunity for their competitors to employ unfair methods and gain a competitive edge. For example, one participant explained how competitors left bad reviews for other apps and bought positive reviews on various marketplaces for their own apps.

> *"I started getting these negative reviews and I realised it was from the same account. Okay yeah, put a new release now and then that same account would make a negative review again. [...] What that meant was that review then became the first one people saw on the application. [...] And then I saw this person had written negative reviews about 25 other education apps. There was one particular one they hadn't written a negative review of, one that they'd written a positive review about."* — P17

5.4.5 Concerns and Suggestions for Creating Privacy-Friendly Apps through Alternative Funding Mechanisms

To explore how we could support developers seeking for a balance between privacy-friendly apps and monetisation, we proposed designs to enable alternative funding schemes, including *Crowdfunding and Patreon* [D11] , and privacy-friendly app marketplaces, *Unlimited Arcade* [D12]. Our study found that participants often felt they were unlikely to succeed with these mechanisms. Instead, they proposed collaborative measures and gradual changes to leverage the current marketplaces.

Need for Gradual Changes in Introducing Alternative Marketplaces

One of the major concerns that participants had with alternative marketplaces is that it would directly compete with Google or Apple, because of which it is unlikely to succeed. In addition, these platforms are known to

have strict rules about their apps being uploaded to other marketplaces. Because of their monopoly, participants have had experience with alternative marketplaces not generating a lot of revenue. One participant explained how he uploaded his app to the Samsung marketplace. However, he earned too little money that the cost of keeping track of these app versions far outweighed its benefits.

> *"I don't remember whether we are still on Samsung Kids. Because the network keeps changing things; I just can't keep up with updating."* — P20

For alternative platforms to be successful, participants indicated that marketing is important and that they would only consider engaging with it if it is already sufficiently popular and successful.

Instead of competing with existing platforms, participants proposed leveraging their current market share and influence. For example, they suggested lobbying current platforms to buy into the scheme, or to add an ethical apps category. Alternatively, they suggested creating an app library, rather than a marketplace, which redirects users to the Google or Apple marketplace.

New Monetisation Methods Should Not Challenge Users' Existing Habits

One thing that participants liked about alternative platforms (such as unlimited arcade) is that it may raise users' awareness about the cost related to app development. Several participants indicated that there is a misconception of how much it costs to create apps. Providing more transparency on how much money developers need to raise will gave parents a better understanding on why certain revenue sources are necessary.

However, these participants were also concerned that parents are generally reluctant to pay for wholesome and privacy-friendly apps, as they are expecting everything to be free. Users' attachment with certain apps may lead to a market concentration around a few apps (not necessarily the best apps) in this alternative, ethical app market, while some apps will not receive funding at all.

> *"And yeah, I think as a developer I'd find that mildly frustrating, that I'm now jumping through the hoops of people where I'm like, you know, I already know that parents don't quite understand the value given to them by apps."* — P13

Furthermore, many participants had the practical concern that parents would need to navigate away from the Apple or Google marketplace to a different environment, which could be burdensome. Instead, they suggested adding alternative ways to support crowdfunding ethical apps in the existing systems, e.g. implementing an in-app tip jar, which could avoid a complete change of users' existing habits and facilitate the objective towards developing alternative operational models for the app market.

> *"I could also see something like an in-app sort of tip type thing, you know 'leave developer/agency a tip'. Because then, it's sort of like: 'I have used this app or my child has used this app, and it's done good'. So then they have the option to contribute for further development and maintenance."* — P6

Need for New Measures of Success

One of the problems participants identified with alternative marketplaces is how developers would be compensated. Currently, subscription-based platforms do this based on game play time and in-app purchases. However, nudging children to play games for longer or make purchases conflicts with children's best interests. Instead, participants indicated that there is a need for defining new measurements for success, based on more wholesome metrics, rather than game play time. Participants were not entirely sure what this would like or how this could be achieved, indicating that this could even differ per app genre.

> "*Because a lot of the time, when it comes to the measures of success for an app, they're all around engagement and how long people have spent in the app, and how much they've bought, or all of this. So the advocacy element, [...], to not be around those things, and have more wholesome measures for success around the app.*" — P18

5.4.6 Challenges for Rewarding Privacy-Friendly Apps

To further incentivise privacy-friendly and age-appropriate app design, we explored two rewards systems: *Public Pledges and Awards* `[D9]`, allowing developers to take a pledge (similar to a climate pledge), and a *Badge of*

Honour [D10], which rewards those upholding certain privacy standards. Developers found that these approaches can work if there were sufficient community awareness of the importance of privacy, similar to climate change or organic products in the food industry.

Need for Recognition and Adoption of Privacy-Friendly Development Practices

In general, participants reacted favourably to the design ideas of recognising good practices. A badge or award provides for positive marketing and exposure, allowing small companies to be potentially listed alongside big ones. Having a badge associated with your app, especially one awarded from a trusted or credible organisation, makes it easier to negotiate with clients and for clients to find you. Customers enjoy the benefit that they can immediately recognise privacy-friendly apps, which allows them to make better informed decisions.

> "*I would say any kind of way a company can have a recognised way of showing externally to their audience that they are ethical, is good. So, a badge of honour would work to show it's certified. As long as this badge showed that was from a trusted source, and it was relatively recognised by parents,*" (P11).

However, several participants did indicate that it was important that developers must actively apply or seek out these badges, and that they must be assessed by an independent third party to ensure that these badges remain valuable and impactful. We asked participants whether they would be willing to pay for such a badge or its assessment, but they were concerned that this would defeat its purpose by creating a 'pay to win' economy:

> *"The problem that [company name] had, is that all the other reviews sites were basically based around getting money out of the app developers."* — P17

On a more practical note, a number of participants also expressed their concerns that there are currently no negative consequences associated with apps without a badge. They compared this to the food hygiene rating practices and stated that no one will advertise a bad food hygiene rating; unless these badges are mandatory, privacy invasive companies will be scarcely incentivised to cooperate.

The Need to Raise Awareness Amongst the Right Stakeholders

One of the concerns that participants had is that it was not always clear who the target customers always are. Participants perceived a misalignment between the customer and the buyer; children are the pursuers of games and will ultimately decide what they want to buy, however, a badge or award is unlikely to sway their decision even though their parents might take different priorities in their choice-making:

> *"Kids are really driving a lot more sort of family purchasing decisions because it's technology and they're so okay with it. So you know, you're in a place, where the one, probably the person with the most knowledge is the kid. The person who needs to be protected the most is the kids, so it just creates this very interesting puzzle."* — P16

Several participants also agreed that raising awareness is not a trivial task and requires careful behaviour engineering. They made the analogy with the B Corp Certification movement (advocating for a positive impact on society) and envisioned people may slowly become more aware of the importance of privacy, suggesting that privacy-friendly apps could benefit from a similar campaign.

> *"I think, as a parent, if there's somewhere that I can go or some kind of rubber stamp that I can look for, like on Twitter, they have the blue ticks. I think it's Waitrose, you can filter by B-Corp project, so you can be like: 'I only want to buy from companies that are B-Corp, so I'm only going to buy from that."*

A few participants also proposed having different types of badges to indicate different levels or types of privacy compliance. For example, having a separate badge for data privacy or reduced game play time to support different user needs.

> *"Maybe there's different styles of badges to represent these different types of awards. Maybe they're not necessarily 'this one is the best', and 'this one is the worst', and there is some in between. Maybe they're just more like, different looking ones to represent what the parents might be looking for. But I think it's going to be, it's just going to be driven by what the users are going to be looking for and want."* — P12

5.5 Discussion

5.5.1 Summary and Key Findings

Using Research through Design (RtD), our study identified some critical requirements and needs from app developers regarding how they would like to be supported with designing privacy-friendly apps for children (RQ3.a). These latent requirements and needs provide important directions for designers and practitioners who want to develop support for the developers' community in an immediate and specific way (RQ3.b). However, when prompted about integrating these tools into their own app (practices), our participants were reluctant to make the final step of committing to using them. Participants formulated further, more nuanced, socio-technical barriers that they would like to see addressed before they were prepared to uptake privacy-friendly development practices (RQ3.c).

Participants found it important that guidelines and SDKs are backed by credible and trustworthy institutions, as a way to motivate and justify the importance of privacy-friendly apps to other stakeholders. They suggested ways to achieve this, such as certifications and privacy labels, which they felt could offset any additional development costs. They also focused on how integrating privacy-friendly features may affect the market acceptance of their apps, and felt that perceived costs associated with implementing privacy features must be compensated by equal market competitiveness. They were concerned that end users might not always understand the importance of privacy in apps, leading to lack of valuing privacy-friendly app features. They also indicated that systemic changes in current marketplaces and platforms are critical for moving to a mobile ecosystem where privacy-friendly apps become the norm, but acknowledged that it would require cooperation from major market leaders. They suggested that platforms could consider making gradual changes to increase users' awareness and value of more privacy-friendly apps for children and thus a gradual transformation from a single, data-driven app ecosystem.

Our participants perceived these barriers by considering the values and roles of multiple stakeholders, including parents, children, regulatory organisations or current and future platform providers. Through this, we identified a critical dimension for future development of support for app developments: *the importance of multi-stakeholder engagement*. From addressing developers' barriers for incentives, to developing trust of design guidelines to support

them navigating and bringing changes to the monopolising market space, all these future design explorations demand critical engagement beyond the developer community and with multiple stakeholders. This reflected that successful privacy-friendly app development must be situated amongst multiple paradigm shifts and behaviour engineering (see Fig 5.2). In the next sections, we look at the socio-technical requirements and barriers more in depth.

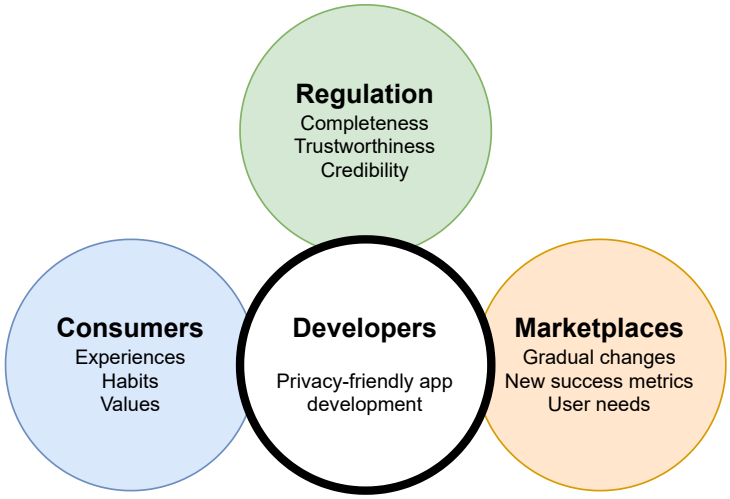


Figure 5.2: Supporting privacy-friendly app development is a multi-stakeholder process, which requires a holistic understanding of how users' incentives intertwine with practice changes and the credibility of all stakeholders involved.

5.5.2 Addressing the Need for Credibility and Normalisation of Privacy-Friendly App Development

In creating privacy-friendly apps for children, developers perceive a certain trade-off that needs to be made. They feel that the implementation of privacy-friendly features or adhering to certain guidelines comes at a cost. In some cases, these costs were explicit. For example, as was the case with our automated compliance testing suite, *Machine over Mind* [D5], making changes retroactively would take a lot of time and effort. In other cases, these costs were implicit or hidden, for example through friction encountered

during development, even when integrating or using existing SDKs. As a result, participants found it important that these costs associated with creating privacy-friendly apps are offset with certain benefits.

Firstly, they required that their efforts should be recognisable to consumers. They proposed that guidelines and tools should be backed by influential organisations as a way to communicate trustworthiness and credibility. There has been an increasing number of efforts to establish guidelines and tools aimed at developers. For example, UNICEF published the policy guidance on AI for children [406], detailing how AI systems should uphold children's rights and offer a set of practical implementation tools with it, such as a development canvas. UNICEF also offers a similar toolkit for privacy [92], which aims to clarify the GDPR and which contains a questionnaire-based checklist, covering the full spectrum of privacy considerations for children which developers must make. Similarly, the ICO in the UK also provides tools to help developers understand how children's data is mapped in their applications [354], as a way to help with implementing the Age-Appropriate Design Code and to be more intentional with their data processing. Despite these efforts, studies have shown that developers often find it difficult to keep track of new guideline developments and integrate them into a common compliance framework [270]. We have shown that developers have very specific requirements when it comes to guidelines, for example they need to be highly practical and offer conflict resolution between frameworks. This requirement has been echoed in studies done with software engineers in assessing Privacy Engineering Methods, stating that usefulness is the most important contributor in incorporating privacy-by-design principles [407]. However, our study also shows that these practical elements extend beyond the technical features, and that it is important to also consider commercial aspects in building guidance and tools, as developers are concerned with negotiating the importance of privacy with consumers. The lack of such considerations in current guidelines points to a need to involve developers and consumers as additional stakeholders in the design process of such guidelines [345, 374], as well as other domain-specific experts, such as those from cybersecurity or child development. This resonates with several existing approaches to developing specialised technical guidelines [368], which is supported through a rich body of HCI research regarding how software development can benefit integrating privacy principles in the development process [24, 408]. Participatory design of guidelines and tools would ensure that they are formatted according to developers' needs such that the time and effort to use them is

minimised.

Secondly, developers also sought for the normalisation of privacy-friendly design features in apps amongst competitors, indicating that they would be more likely to adopt such features if their competitors did so too. To accomplish this, they suggested that standardisation efforts be made to establish a set of common expectations amongst both competitors and consumers. To create standardisation requires backing from credible organisations which have the weight to force developers to comply. The IEEE Standards Association is an example body that has produced a large array of standards [409], bringing in stakeholders from various domains. Similarly, following the launch of the AADC in September 2021, the UK ICO has been rapidly developing compliance forces through a certification programme [410]. This way, a number of independent standard compliance certification bodies are able to carry out the enforcement and validation more efficiently. However, it is not entirely clear how these efforts are exactly aimed at developers. These certifications are more geared towards establishing legal compliance, while developers are looking to position such efforts in the marketplaces, where consumers can interface with them as well. This suggests that in developing standards too, that it may be beneficial to consider both consumers and developers as stakeholders. The normalisation of privacy can also be achieved through other means. For example, through efforts on a corporate level. Increasing work in HCI suggests that commitment towards privacy is often aligned with the company's vision [411], and that putting in place privacy champions in software teams can have a positive impact [24]. However, such efforts are limited to development companies and studios and would not include independent developers or small teams.

A focus on external stakeholders in adopting privacy-friendly features and tools in apps by developers does not mean that we should abandon supporting developers through such means. Rather, it calls for a holistic approach to put systems into place where privacy in apps benefit and impact all stakeholders. Participants pointed out that several of our design ideas could work well together, especially those that raised awareness amongst parents, children, and developers alike. We believe the HCI community has an important role to play in this, as the design of such systems call for multi-stakeholder multi-disciplinary approaches. Despite strong and rapid regulatory movements, we must recognise and encourage further considerations regarding the fundamental data-driven ecosystem under which developers are carrying out their innovations.

5.5.3 Users' Incentives, Behaviours and New Practices

Some of our design approaches, such as the *Badge of Honour* [D10], were motivated by existing research related to privacy nutrition labels [402, 412], and were specifically aimed at helping developers raise awareness amongst their end users about the improved privacy aspects of their apps. While existing research has shown how the effectiveness of privacy nutrition labels could be correlated with users' level of privacy awareness or tasks [402, 412], and when they were presented to the users [413, 198], our results showed that our participants were more concerned whether users were prepared to make any actual changes of their app purchase habits (i.e. incentive changes) and the credibility of such 'badges of honour'.

Participants compared our design proposals with existing movements in similar consumer industries which benefited from ethical initiatives, such as Fairtrade [414] and B-Corp [415]. The challenge with these approaches is that it has a multi-stakeholder audience, requiring all stakeholders to change their understanding and behaviours towards privacy. It would require parents to value the preservation of their children's privacy in apps over the actual financial cost. Currently, research into the behaviours of how parents choose apps for their children is still limited, but suggests that privacy is not yet a priority [22]. While parents might be willing to prioritise the safety of content driven features, such as advertisements, privacy tends to fall behind. Safety and privacy are often considered to be separate concerns or even mutually exclusive. However, if we wish to foster an environment where privacy-friendly apps become the norm, it is important for all stakeholders to be aware of the tangible consequences associated with a loss of privacy, such as loss of opportunities later in life and loss of autonomy [416]. This also means that discussions about the importance of privacy need to be normalised, for example by including it in school curricula or as conversations between parents and children [417].

To overcome the barriers for the recognition of new, privacy-friendly development practices, developers in our study indicated the importance of a two-step approach: (1) establishing a market standard for *a privacy-friendly app for children*, and (2) promoting the recognition of this standard by the end users (such as parents). In this way, their additional effort would lead to visible recognition amongst their competitors and users and ensure a possible competitive edge. We see a resemblance from this call for socio-technical changes to previous privacy research [402, 413] which have found that in-

creasing the transparency of personal data being collected by websites or smartphone devices for the users would not necessarily effectively impact users' privacy behaviours unless their awareness about this transparency and its implications were securely established. However, facilitating this user awareness and community change in the app ecosystem poses some unique challenges.

Instead of a 'privacy paradox' [418], research has observed a 'value paradox' of today's parents when supporting their children's online activities: they would commonly undermine the cost of a good app for their children and are rarely ready to pay for any apps; even though they normally place tremendous values on their children's education and interaction with other types of media [419]. This can be partially attributed to the freemium app ecosystem, which has dominated and influenced our consumer behaviour for a substantial period of time [420]. This can also be related to the lack of backing from credible organisations regarding the importance of such practices. Encouraging developers to rethink factors that are currently influencing their development decisions is key to supporting developers' to overcome the barrier of adoption. Facilitating a further understanding of the interplay of these factors is one crucial direction for future investigations of how users' awareness and community recognition can be effectively integrated to develop and boost the inner motivations of developers.

5.5.4 Overcoming Systemic and Structural Barriers

To answer RQ3.c, regarding how developers foresee overcoming systemic barriers put in place by marketplaces, we discuss how our findings align with recent developments and future trends. It is known that major industry stakeholders, such as Apple and Google, are poorly incentivised to limit data collection and analytics, as it forms a major source of their revenue [35]. Both Apple and Google do not react kindly to any initiatives trying to undermine their terms and conditions, as was demonstrated by Epic Games v. Apple court case [421]. Epic Games cut Apple out of their 30% commission on in-app purchases, leading Apple to block them from their marketplace. While a behemoth like Epic Games can afford to take Apple to court, most smaller studios will not have such capacities. Furthermore, in the past few years, Apple has taken an opposing stance to Google's data driven position in generating revenue. For example, from iOS 14 onward, apps will need to explicitly ask permission from users to allow third-party tracking services [355]

and Apple has also introduced privacy labels to inform users what type of data is being collected by apps [422]. These initiatives suggest that major industry players are already aware of growing concerns amongst consumers and regulators about the importance of privacy, and are trying to situate themselves such that they can move away from data driven monetisation methods. While this is easier for Apple to do, as they do not rely on advertising for their revenue as much as Google or Facebook, other marketplace providers will have to show similar support to facilitate a shift to the development of privacy-friendly apps.

While our participants welcome the vision of creating alternative marketplaces, they raised the concerns regarding the current measurement of app success, which is commonly based on gameplay time. Without a fundamental rethinking and promotion of alternative ways of evaluating apps' values and contributions, the community could hardly foresee a successful paradigm shift and associated practice changes. The major platforms have started introducing subscription based services, in which games can be accessed without in-app purchases and advertising [3, 54]. While these platforms are not transparent about their payment structure, interviews with app developers have revealed that royalties are directly still tied to gameplay time, incentivising app developers to build in addictive feedback loops and other features to maximise gameplay time [423]. Additionally, developers expressed concerns that these payment structures only benefit big development studios, leaving apps with a small user base earning very little.

Currently there are no platforms in existence where alternative payment structures are considered, especially since Google and Apple have a monopoly in this field. The rigid structures in place at the moment also speak to the need for a paradigm shift in our models for data governance. One example of this is the Web 3.0 concept [424], which is aimed to help facilitate decentralised data architectures and restore data autonomy back to users. For example, decentralised marketplaces allow buyers and sellers to exchange 'goods' without the need of central service providers, which in the mobile ecosystem would allow the community to eliminate Apple and Google. It would also give developers the autonomy to establish how they wish to monetise their services, rather than being forced to rely on in-app purchases and targeted advertising. However, introducing this paradigm shift in the app development ecosystem may require additional structures to overcome the dominance of the app market for promotions. Several of our participants mentioned that leading app markets can make a life-changing decision about

how they would like to rank their app or whether they would like to feature their apps on the marketplace. Leading markets have also been known for previously removing or banning certain apps providing privacy protections in a way that was against their best interest [425]. Emerging alternative app markets (such as F-Droid) would prove critical in the process of redesigning the data governance structure in the app ecosystem. Furthermore, this new data paradigm would also raise new research challenges regarding how to facilitate the creation and uptake of this new data governance paradigm, so that users can regain their data rights.

5.5.5 Limitations and Future Work

The methodology we used had several limitations. Firstly, we focused on the UK app market, rather than including the rest of Europe and the US. We chose the UK because of new regulatory initiatives introduced in late 2020 for organisations developing digital products and services aimed at children. However, given the international nature of app marketplaces, we encourage future studies to incorporate stakeholders from other geographic areas as well.

Secondly, we also focused on mobile apps for children, instead of considering all digital services for children which include an element of data protection, such as toys and websites. We have not specifically asked participants whether they perceived any difference for developing children of different ages. Our focus has been on the data protection and privacy aspects of children's apps instead of the more nuanced support for different developmental needs of children.

Thirdly, in our analysis of the interviews, we did not make a distinction between subgroups of participants (e.g., work experience or role). We acknowledge that there were several variations in job roles, however all participants have had experience in creating and publishing apps for children. In our study, they often used their app creators' lens to assess and evaluate our design ideas. However, they did indicate individual preferences of design ideas as they would benefit different roles in different ways.

Fourthly, we used a sample size of 20 developers, primarily from the UK, meaning that our results may not generalise to a wider international audience of developers, where regulatory requirements such as the GDPR, COPPA, and the AADC are less prioritised. In our case, as our focus was on the UK market, our in-depth interviews with a limited sample size provided rich data.

Future studies may consider using methods to reach larger audiences, such as surveys, and even venture beyond the UK/EU developer communities.

Lastly, our findings were closely derived from the 12 design ideas that we generated in the ideation workshop. While the ideas were sufficiently diverse, it would have been interesting to include developers (and other stakeholders) as co-speculators in the design process itself. However, the community for developing children's apps specifically is rather limited in the UK and the consequences of the COVID-19 pandemic made it difficult to gather such a unique set of stakeholders in a room together. However, for future studies, it would be interesting to co-design solutions directly with stakeholders, and even prototype some of the design ideas to evaluate how it would fare in practice.

5.6 Conclusion

There is an increasing demand from consumers and regulatory bodies for apps and services aimed at children to make data protection and privacy a core element of their design. However, mobile app developers are not sufficiently equipped to understand and integrate privacy preserving design features in their products due to conflicts of interest between marketplace providers and other stakeholders. In this study, we examined developers' requirements to enable them to address these challenges by eliciting reactions to 12 speculative design concepts we created. Our findings show that developers are in need of tools and actionable support to help them design privacy-friendly apps. However, they also formulated critical socio-technical barriers preventing adoption of these tools. Overcoming these barriers requires a substantial effort from the HCI design community, relying on multi-stakeholder multidisciplinary initiatives. We examined in depth how developers envision the future of privacy-friendly app development to look like, and how we can overcome some of the socio-technical barriers they formulated.

The findings in this chapter provide important directions for how we can concretely support children's app developers in better understanding the complexities of the mobile ecosystem. We take these findings forward into the next chapter, where we look to translate the requirements formulated in this chapter to develop and evaluate a support tool that disrupts their existing app development practices.

6

Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps

Contents

6.1 Introduction 175

6.2 Designing `DataAvalanche.io` 178

6.2.1 Design Consideration 179

6.2.2 Functionality 181

6.2.3 Components and Architecture 185

6.3 Implementation 186

6.3.1 Privacy-Friendly Alternatives 186

6.3.2 Legal Implication 188

6.3.3 Children Specific Configuration 189

6.3.4 Knowledge Graph 189

6.3.5 Back-End Server 190
6.3.6 Front-End 190
6.4 Evaluation 191
6.4.1 Participants and Recruitment 192
6.4.2 Interview Procedure 193
6.4.3 Surveys 195
6.4.4 Data Analysis 195
6.5 Results 196
6.5.1 Alternatives are Good but Not Always Applicable 196
6.5.2 Privacy Implications are Useful for Transparency . 198
6.5.3 Data Tracking is Not Surprising 199
6.5.4 Putting `DataAvalanche.io` to Use 201
6.5.5 Additional Requirements 202
6.5.6 Survey Results 205
6.6 Discussion 206
6.6.1 Summary and Key Findings 206
6.6.2 Affecting Developer Practices and Choosing Alternatives 208
6.6.3 Evaluating Privacy Implications Through Increased Transparency 208
6.6.4 Improving `DataAvalanche.io` 209
6.6.5 Limitations 211
6.7 Conclusion 211

6.1 Introduction

In the preceding three chapters, we performed a comprehensive examination of children's privacy within the mobile app ecosystem. We determined that a significant number of children's apps track data and fail to provide adequate support for children in comprehending and safeguarding their privacy rights. Through two studies involving children's app developers, we discovered that while developers aim to create apps that promote the best interests

of children, they encounter challenges that may prompt them to implement privacy-invasive practices. To address these issues, we conducted interviews with children's app developers and formulated a set of requirements for developing a tool to assist them in creating more privacy-sensitive apps. In this chapter, we will utilise these findings to develop a web-based tool for evaluating the potential impact of a disruptive solution on developers' practices and decision-making processes, with the aim of encouraging them to prioritise privacy as a fundamental aspect of their apps [1].

Previous research has demonstrated that tools can be developed to aid developers in automating the creation of privacy policies and effectively communicating privacy-related information to end-users [30, 426]. Additionally, research has investigated the utilisation of IDE plugins to clarify the privacy implications for developers [32, 31]. However, these studies do not specifically address the need for developers to have increased transparency and understanding of the data-related behaviours of third-party SDKs. In light of this, our intention is to develop a web-based tool that assists developers in comprehending the landscape of SDKs and selecting privacy-friendly alternatives.

To this end, we aim to answer the following research questions:

RQ4 Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?

- 4a How can we empower developers to make informed decisions about the privacy practices of different SDKs and libraries, and to choose alternatives that are more privacy-friendly?
- 4b How do tools and guidance for developers to protect the privacy of their users, including specific configurations and legal considerations, affect their choices in selecting third-party libraries?
- 4c How does providing transparency on the data sharing practices of different SDKs and libraries affect developers' practices in terms of understanding and evaluating privacy risks?

[1] This Chapter has been published as: Ekambaranathan, Anirudh, Jun Zhao, and George Chalhoub. "Navigating the Data Avalanche: Towards Supporting Developers in Developing Privacy-Friendly Children's Apps." *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 7.2 (2023): 1-24.

To answer these questions, we developed `DataAvalanche.io`, a web based tool for children's app developers. `DataAvalanche.io` allows users to analyse privacy practices of commonly used SDKs and proposed privacy-friendly alternatives. Our tool also visualises legal implications of using certain SDKs. We evaluated `DataAvalanche.io` with 12 children's app developers through a cognitive walkthrough process and a System's Usability Scale survey [427].

Our participants generally reacted positively to `DataAvalanche.io` They found it useful that privacy information about SDKs was collected and viewable in a central repository. Specifically, they found it helpful that we linked to relevant documentation and any specific privacy configurations that are important when designing for children. However, we also found that developers were hesitant to make changes when it came to choosing privacy-friendly alternatives to commonly used SDKs. They cited four reasons, related to usability and monetisation, that took precedence over privacy in their decision-making process. Developers appreciated the legal implications we provided, as they felt that this could help them inform end-users and select SDKs that are compliant with certain jurisdictions. In evaluating the privacy of apps through our data sharing graph, which we initially created in Chapter 3, they indicated to require more guidance in translating this knowledge to practical and technical requirements in their apps. Overall, our findings provide valuable insights into the privacy practices of developers, particularly in the context of children's apps. We have identified factors that could influence developers' decisions to prioritise privacy in their development process.

This chapter makes the following contributions:

- We designed and evaluated `DataAvalanche.io`, a tool for developers to evaluate the privacy of commonly used SDKs in children's app development. We identified four reasons why developers prioritise factors other than privacy when selecting third-party libraries and SDKs, providing a nuanced understanding of the decision-making process.

- Through our evaluation, we also have an increased understanding of how developers view and evaluate privacy information in apps. Developers are particularly drawn to and benefited from practical features which translated to technical requirements for their apps.

- We formulated concrete requirements for future tools to help developers consider privacy as a core element in the development practices.

We identified a range of additional requirements that participants suggested could be included in our tool to make it more useful and effective in helping them consider privacy in their development practices. These requirements provide a valuable starting point for the design of future tools and guidance to support developers in considering privacy in the app development process.

6.2 Designing `DataAvalanche.io`

In this chapter we aim to design and evaluate a tool to help developers in creating privacy-friendly apps for children. We name our tool `DataAvalanche.io`, after the *data avalanche* principle introduced in Chapter 3. To reiterate, we use the term data avalanche to describe the uncontrollable large scale data dissemination that happens once data leaves an end-user's device a reaches a third-party. This third party may in turn share it with fourth-party platforms and organisations. In this section, we describe how we designed `DataAvalanche.io` and how we motivated certain design choices based on findings from previous chapters as well as existing literature.

The findings from Chapters 4 and 5 show that there are three areas in which developers require help:

1. There is a need for better actionable and concrete **guidelines** to support developers in understanding how to develop privacy-friendly apps. This includes guidance on practical and concrete aspects as well, such as suggestions for business models and third-party libraries.

2. Developers indicated a need for increased transparency and guidance in the use of **third-party libraries** and their privacy practices.

3. There is a need for changes in current opportunities for **monetisation**.

In this research, we have chosen to focus on the second need because it is more feasible to translate these users' needs into specific technical needs (as shown by our RtD study in Chapter 5) and develop concrete technical tools to address these issues. The goal of our research is thus to examine whether by providing developers with more information on the privacy practices of different SDKs and libraries, as well as tools and guidance for evaluating and

choosing alternatives that are more privacy-friendly, we could affect developers' practice of making informed decisions about which SDKs and libraries to use in their apps.

We believe the other two requirements, although essential for facilitating the creation of privacy-friendly apps for developers, they would require more social-technical support that is beyond the scope of this thesis. The third point, which focuses on changes to monetisation opportunities, would require significant structural changes to how marketplaces operate. This may be beyond the scope of our current work, and requires the involvement of multiple stakeholders, such as marketplaces, developers, and regulatory bodies. The first point, which focuses on designing guidelines for privacy-friendly app development, would require a non-technical effort. While guidelines can be helpful for developers, they may not necessarily provide concrete and actionable solutions to the challenges that developers face. Additionally, the development of guidelines is not within the scope of this thesis either, as it may require expertise and insights from other fields such as law or psychology.

6.2.1 Design Consideration

One of the key challenges faced by developers when building privacy-friendly apps for children is navigating the privacy implications of third-party libraries and SDKs. To effectively address the needs of app developers, we have formulated three high level design goals for our tool (`D1 - D3`). These goals are based on the key areas in which developers require assistance, as identified through our analysis of the literature and findings from the previous chapter (see Chapter 5), as well as our research questions formulated in the introduction.

`D1` Support developers making informed choices of third-party libraries by providing more comprehensive privacy information about SDKs and libraries, and proposing privacy-friendly alternatives.

One of the key challenges faced by developers when building privacy-friendly apps for children is navigating the privacy implications of third-party libraries and SDKs. This is something that was already established earlier in Chapter 4 as well as in previous literature, where it has been observed that developers, for example, often choose prominent ad vendors without fully understanding the privacy implications of these choices [28, 10, 26].

Further in Chapter 5, we drew out more concrete requirements developers formulated to overcome this challenge. Specifically, we first identified that developers would like *SDKs and libraries to be easy to integrate and known to be compliant* (section 5.4.3). Specifically, they suggested a *centralised location where they can easily access libraries* that meet certain compliance standards (section 5.4.3). This served as a main motivation for developing `DataAvalanche.io`, where users can access a large number of commonly used SDKs. Secondly, developers found it important that tools do not undermine an app's commercial potential. We therefore also incorporated the need to suggest privacy-friendly alternatives to mainstream SDKs which developers can draw on. Finally, developers also indicated that it is important that tools should integrate with the development cycle (section 5.4.4). Therefore, we designed `DataAvalanche.io` in such a way that it can be used at the very beginning, without interfering with further development once it has started.

`D2` Support developers to protect the privacy of their users by providing them with specific configurations and legal considerations for using third-party libraries.

This is motivated by the specific requirements raised by the developers for the access to *actionable guidelines with clear legal implications* (see 5.4.2). Specifically, they articulated the need for clear accessible instructions for how apps for children should be designed. From our findings in Chapter 3, we know that certain libraries require specific configurations for apps aimed at children. Therefore, in our design we make this clear and accessible to developers. Secondly, developers also indicated the need for transparency on the legal implications and requirements of SDKs. We therefore aim to clarify this in our design through making privacy policies more accessible and making the GDPR implications more explicit. While we do not aim to provide a comprehensive guideline for developing children's apps, we wanted to relate this back to the behaviours of SDKs in an intuitive manner through helping developers visualise the countries SDKs share data with, in order to support them in complying with relevant laws and regulations.

`D3` Support developers in understanding the complex landscape of data sharing in the mobile app ecosystem by providing a knowledge graph about the data tracker network.

In Chapter 3 we made technical contributions in shedding light on some of the opaque data sharing practices, namely by uncovering part of the fourth-party tracking ecosystem. We draw on these results and translate them into technical features to fulfil the requirements set by developers in Chapter 5. Findings from chapter 5 show a need for understanding *the privacy implications* of libraries (see 5.4.2). We therefore wish to shed some light on the data sharing infrastructure of the mobile app ecosystem, in order to help developers explore and understand the data avalanche and the complex landscape of data sharing.

6.2.2 Functionality

D1: Empowering Developers to Make Informed Decisions about SDKs and Libraries

The main objective of `D1` is to provide developers with the tools and guidance they need to make informed decisions about the privacy practices of different SDKs and libraries. To achieve this, we aim to offer the following features and functionalities:

- **Search feature**: The search feature allows developers to easily find information on specific SDKs or libraries, or to search for alternatives to a specific SDK or library. This helps developers to access the information they need to make informed decisions about the privacy practices of different SDKs and libraries.

- **Basic information**: Basic information about the SDK, including its website, company, location, company size, and any social media links, helps developers to get a general understanding of the characteristics and size of the company they are dealing with. This is useful for contextualising the privacy practices of the SDK and for making informed decisions about which ones to use in their apps.

- **Privacy information**: Privacy information for the SDK, including a link to the privacy policy and the number of data sharing partners, helps developers to understand the privacy practices of the SDK. This is crucial for making informed decisions about which SDKs and libraries to use in their apps, as it allows developers to evaluate the privacy risks and benefits of different options.

- **Alternatives**: The tool provides a list of privacy-friendly alternatives to the SDK. By *privacy-friendly alternatives*, we refer to SDKs or libraries which have declared themselves as 'privacy-friendly alternatives', or those that are self-hosted or open-source. Our research has shown that this helps developers to reduce the extra development involved in considering a new development practices and make informed decisions about which ones to use in their apps. For example, if a developer is considering using a specific ad library but is concerned about its data sharing practices, they can use the alternatives feature to find alternative ad libraries that have more privacy-friendly practices.

Overall, the combination of these features and functionality is aimed to help developers to make informed decisions about the privacy practices of different SDKs and libraries, and to choose alternatives that are more privacy-friendly.

D2: Providing Developers with Tools and Guidance for Protecting Child Privacy

The main objective of `D2` is to provide developers with the tools and guidance they need to protect the privacy of their users, including specific configurations and legal considerations for using third-party libraries. To achieve this, the tool will offer the following features and functionality:

- **Child-specific configurations**: For some SDKs, the tool will provide a link to any child-specific configurations that may be required to protect the privacy of child users. This includes configurations that are required to comply with specific guidelines or regulations, such as the Children's Online Privacy Protection Act (COPPA) in the United States. By providing access to these configurations, the tool helps developers to easily implement the necessary safeguards to protect the privacy of child users. For example, if a developer is using an SDK that is subject to COPPA regulations, they can use the child-specific configurations feature to access the relevant settings and to ensure compliance with these regulations. This can help developers to avoid legal liabilities and to protect the privacy of their child users.

- **Legal implications**: The tool will provide information on the legal implications of using certain libraries, based on the geographic locations

where data is being shared. This includes information on relevant data protection laws and regulations, such as the GDPR in the European Union, and any specific requirements or restrictions for handling the personal data of children. This helps developers to understand the legal risks and requirements of using different SDKs and libraries, and to ensure compliance with relevant laws and regulations. For example, if a developer is using a library that shares data with a country that has strict data protection laws, they can use the legal implications feature to understand the specific requirements they need to follow in order to comply with these laws. This can help developers to avoid legal liabilities and to protect the privacy of their users.

- **Visualisation of data sharing**: The tool will visualise the countries that a specific SDK or library shares data with, using a map-based interface. This allows developers to see at a glance which countries their app's data is being shared with, and to understand the extent and scope of data sharing practices. This can be particularly useful for developers who are concerned about the privacy risks of using certain SDKs or libraries, as it allows them to easily see where their app's data is being shared and to make informed decisions about the privacy risks and benefits of different options. For example, if a developer is using a library that shares data with a country that has weaker data protection laws, they can use the visualisation feature to understand the specific risks and implications of this data sharing practice, and to consider alternative options that may be more privacy-friendly.

D3: Shedding Light on the Data Sharing Infrastructure of SDKs and Libraries

The main objective of `D3` is to shed light on the data sharing infrastructure of different SDKs and libraries, and to allow developers to explore and understand the risks and implications of these practices. To achieve this, the tool will offer the following features and functionality:

- **Data sharing partners table**: For a selected SDK or library, the tool will show all data sharing partners in a tabular format. This allows developers to see at a glance which companies their app's data is being shared with, and to understand the extent and scope of data sharing practices. For each of the data sharing partners, the table will

also show how many data sharing partners it has in turn. This helps developers to understand the complexity and depth of the data sharing ecosystem, and to make informed decisions about the privacy risks and benefits of different SDKs and libraries. By clicking on a specific data sharing partner, developers can also load the tool for that partner, allowing them to explore the data sharing practices of that company in more detail.

- **Data sharing partners graph**: For a selected SDK or library, the tool will show a graph depicting all the data sharing partners. This allows developers to visualise the relationships between different data sharing partners, and to see how data is being shared between different companies. By hovering over the nodes in the graph, developers can view which partner a node represents, and can click on it to load the graph of that SDK or library in turn. This enables developers to explore the data sharing ecosystem in more depth, and to understand the risks and implications of different data sharing practices. This feature helps developers to navigate the data avalanche and to make informed decisions about the privacy risks involved in using different SDKs and libraries.

The functionality provided for `D3` is aimed to help developers explore and understand the data sharing practices of different SDKs and libraries, and make informed decisions about the privacy risks and benefits of these options.

Functionality for Accessibility

In addition to the main functionality described above, we also include several features to help users navigate and use the tool more effectively. These features include:

- **Sample chips**: Below the search bar, the tool provides sample chips which users can click on to quickly access information about different SDKs and libraries. This helps users to get a broad overview of the different options available in the tool's database, and to explore different SDKs and libraries more easily.
- **About page**, which explains what the tool is, who it was developed by, and how it can be used. This helps users to understand the purpose and background of the tool, and to learn more about how it works.

- **FAQs**, which answer basic questions about how to use the tool and what it does. This helps users to get started with the tool more quickly, and to learn more about its features and functionality.

6.2.3 Components and Architecture

`DataAvalanche.io` is composed of three main components: a REST API, a front-end, and a knowledge graph.

Knowledge Graph

The core component of the tool is the knowledge graph, which contains the data sharing partners of the SDKs we analysed in Chapter 3. The knowledge graph is stored in the back-end and contains all the relevant information associated with the SDKs, including company and privacy information that we want to display to the user. The knowledge graph serves as the central repository of data for the tool, and enables developers to explore and understand the data sharing practices of different SDKs and libraries in the mobile app ecosystem.

The REST API

The tool's REST API provides developers with access to data from the knowledge graph through three endpoints. The `tracker` endpoint retrieves all available data for a selected SDK or library, including company and privacy information. The `search` endpoint provides autocomplete functionality for the search feature. The `graph` endpoint returns an SDK's data sharing partners and its partners in turn, enabling developers to explore the data sharing ecosystem to two degrees of freedom. The REST API enables developers to easily retrieve data from the knowledge graph and helps them navigate the complex landscape of data sharing in the mobile app ecosystem. In our case, we use it to implement a front-end to help developers view our knowledge graph data.

Front-End

The front-end of the tool is responsible for rendering the user interface and interacting with the user. It communicates with the back-end through the REST API and is responsible for handling user input and rendering the

visualisations and information retrieved from the back-end. The front-end of the tool is responsible for rendering the user interface and interacting with the user. It contains four main components: two visualisation modules for displaying a map of data sharing locations (*legal*) and for visualising the knowledge graph (*graphing*), an information retrieval module with a *search* function, and a component for viewing *metadata* of an SDK such as the company name, website, and size. This can be seen in Figure 6.3a). These components work together to provide users with the necessary tools to explore and understand the data sharing relationships between different SDKs and libraries.

Architecture

Figure 6.1 depicts the architecture of `DataAvalanche.io`. `DataAvalanche.io` has a client-server architecture, with the front-end serving as the client and the back-end serving as the server. The front-end is implemented using `Vue 3.0` [428] and `Vuetify` [429], which provide a framework for building user interfaces and a design system, respectively. These technologies were chosen for their ease of use, performance, and support for modern web standards. The back-end consists of a `WSGI` [430] web server running `Flask` [431], which is a lightweight Python web framework. The back-end is responsible for serving the `REST API`, which provides access to the knowledge graph stored in the server. The knowledge graph is stored in a `JSON` object, with each key-value pair representing an SDK and its metadata, including a list of data sharing partners. To ensure the security and reliability of the tool, an `NGINX` [432] reverse proxy is used to manage the incoming traffic to the back-end. This helps to protect the back-end from malicious attacks and ensures that the tool can handle high levels of traffic. We elaborate on the implementation details of this in the next section.

6.3 Implementation

6.3.1 Privacy-Friendly Alternatives

As part of our tool, we wanted to show privacy-friendly alternatives for commonly used SDKs in order to understand how this would impact developers and if they would consider switching. However, there currently does not exist a reliable database that offers such a mapping, and creating one is

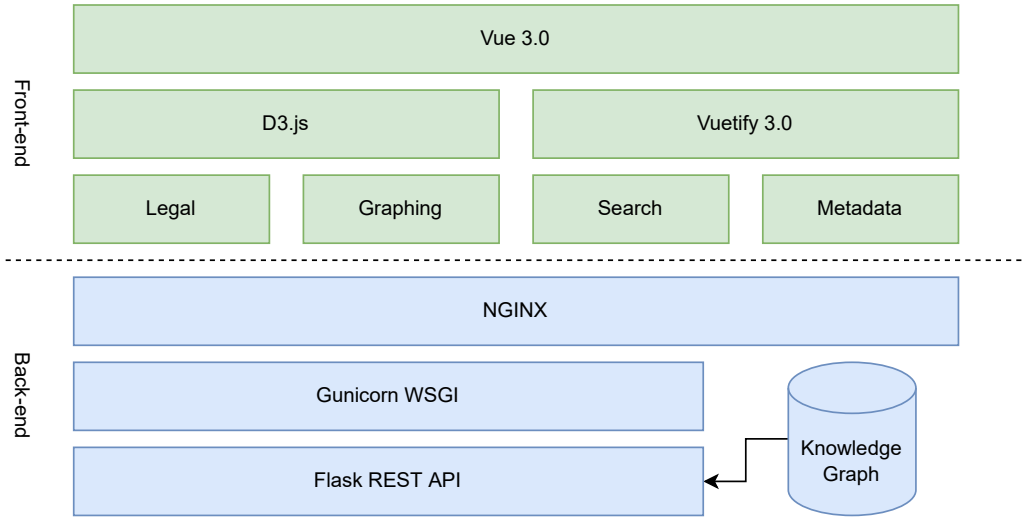


Figure 6.1: System architecture of `DataAvalanche.io`. The front-end is implemented using `Vue 3.0` and `Vuetify`, while making use of `D3.js` for visualisation. On the back-end we run an `NGINX` reverse proxy connecting to a `WSGI` web server. The REST API is written in `Flask`.

beyond the scope of this project. Instead, as the goal of our research is to explore whether providing such privacy alternative may affect app developers' development practices, we selected three libraries and manually identified alternatives, which we presented to our participants as part of our tool.

As developers in Chapter 5 indicated that they would not like tools to undermine an app's commercial potential, we selected three non-commercial SDKs related storage management and analytics for the purpose of our prototyping: Countly Analytics [433], Parse [434], and Piwik [435]. In deciding what constituted an SDK to be privacy-friendly, we read through the descriptions of SDKs which have situated them as 'privacy-friendly alternatives', or those that were self-hosted or open-source. We identified these by searching the web, making use of terms such as 'privacy-friendly alternatives to [SDK]', where we replaced '[SDK]', with SDKs such as Google Analytics and Firebase.

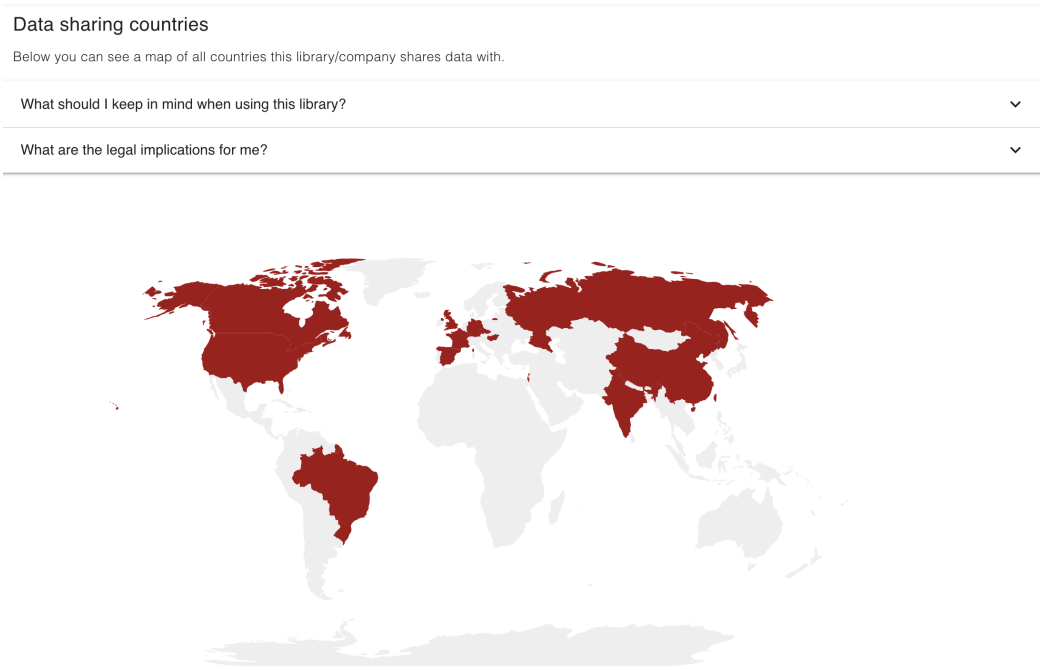


Figure 6.2: In `DataAvalanche.io` users can view to which countries SDKs are sharing their data with. We have provided static information about what GDPR implication would be.

6.3.2 Legal Implication

We wanted to provide transparency on the legal implications of using third-party libraries and SDKs; however, providing a comprehensive legal analysis of every SDK is beyond the scope of this study. Given our focus on the UK market, we instead focused on clarifying a specific GDPR-related privacy implication and providing easier access to privacy policies of all the SDKs wherever possible (see Figure 6.2). For the former, we read through the privacy policies of the SDKS and provided clarifications of GDPR requirements for those SDKs that claim to share data outside the EU jurisdiction. This information is aimed to help developers understand that such SDKs may share data with countries where end users may not be able to enforce their privacy rights and that they should be mindful of this when making decisions about which libraries and SDKs to use.

6.3.3 Children Specific Configuration

It has been shown in previous research that apps (including those for children) do not sufficiently obtain consent before tracking data and obtaining the advertising ID [19]. For children's apps this is partly attributed to the specific configurations which must be set for apps designed for be used by children. In Chapter 3 we manually read through the documentation of 71 SDKs to determine whether they required special configurations for use in children's apps. As an example, the documentation for the Adjust SDK[2] states that:

> "If your app targets users under the age of 13, and the install region is not the USA, you need to mark it as a Kids App. This prevents the SDK from reading device and advertising IDs (e.g. `gps_adid` and `android_id`). To do this, call the `setPlayStoreKidsAppEnabled` method with a `true` parameter".

For those that have special configurations, we included this information in the metadata section of our tool, along with a URL to the relevant documentation (see Figure 6.3a).

6.3.4 Knowledge Graph

As we have previously described in Chapter 3, we performed a comprehensive third-party tracker network analysis as an effort to map part of the fourth-party tracking ecosystem. We used Unity as a root node, and recursively identified its data sharing partners to investigate how each of these entities may further share users' data with fourth-parties. This led to the uncovering of a vast and complex knowledge graph (see section 3.4). To our knowledge, this is the first time that a fourth-party tracker network has been examined and presented to the public. We use this knowledge graph as a fundamental part of our tool.

In order to implement the knowledge graph, we stored the data in a `JSON` object. Each key-value pair in the object consists of the name of an SDK and its metadata. The metadata includes a list of the SDK's data sharing partners, as well as other information such as the company's name, website, location, and size. We chose this approach in order to keep the implementation lightweight and to facilitate rapid prototyping. While the knowledge

[2] `https://help.adjust.com/en/article/apps-for-children-android-sdk`

graph could potentially be imported into a NoSQL database such as MongoDB, or created using a graph database such as Neo4j [436], we ultimately decided against this in order to maintain simplicity and efficiency.

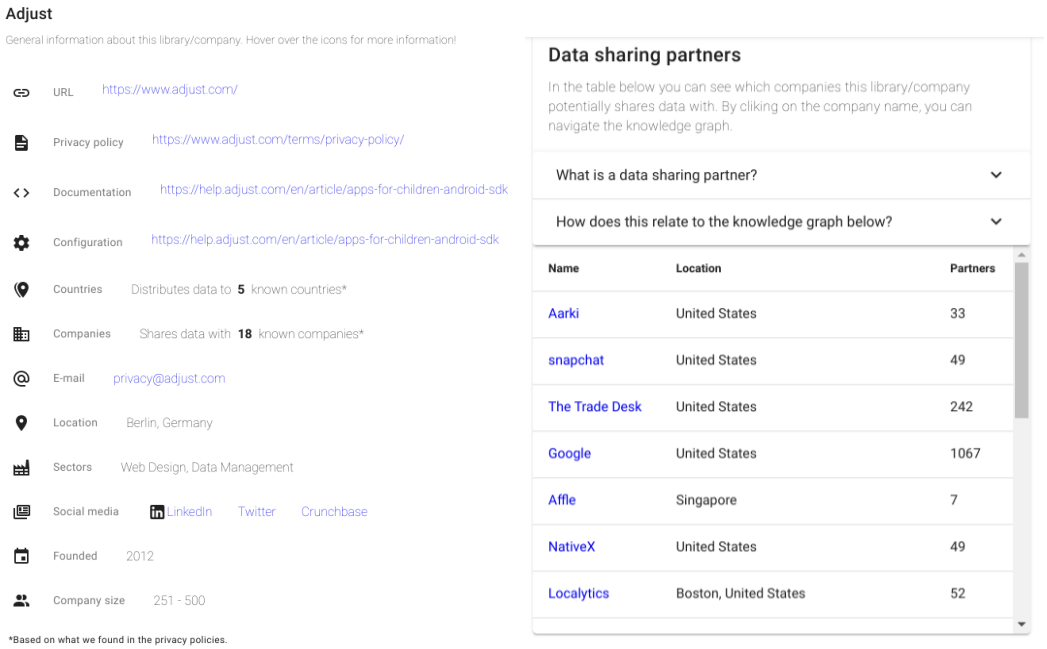
6.3.5 Back-End Server

On the back-end, we run an NGINX reverse proxy to handle incoming requests and redirect them to the appropriate server. This is important for improving the security and performance of the tool, as NGINX can handle a high volume of requests and traffic, and also provide additional layers of protection against common attacks such as DDoS. We also use a Gunicorn WSGI web server to host the tool, which provides a standard interface for connecting web servers and applications. This allows us to easily deploy and run the tool on a variety of platforms and environments. Finally, the REST API is written in Flask, a microweb framework for Python. Flask allows us to quickly and easily build the API, and provides a number of useful features such as request routing, template rendering, and error handling.

6.3.6 Front-End

The front-end of the tool is implemented using Vue 3.0, a progressive JavaScript framework for building user interfaces. We chose Vue for its simplicity, ease of use, and strong developer community. Alongside Vue, we also used Vuetify, a Material Design component library, to provide a consistent and visually appealing interface for the tool. For visualisation, we made use of D3.js [437], a powerful JavaScript library for manipulating and displaying data in a variety of formats. D3.js allows us to create interactive and dynamic visualisations of the knowledge graph, which is crucial for helping developers explore and understand the complex data sharing relationships between different SDKs and libraries, as outlined in D3.

For the knowledge, we decided to not show the full graph, as with nearly 3000 nodes and 15,000 edges it would become confusing to view and too heavy to load in the browser. Instead, we show the data sharing partners which are one and two degrees separated from the root node. In addition to the graph, we also show the data sharing partners in a tabular manner, so that users can scroll through it textually. This is shown in Figure 6.3b.



(a) (b)

Figure 6.3: In (a): Privacy documentation and information which developers might find useful. In this image, we have selected Adjust as an example. In (b): Table allowing users to view the data sharing partners of the selected third- or fourth-party organisation/library.

6.4 Evaluation

We evaluate our findings and tool with 12 children's app developers. None of the developers participated in the earlier studies of this thesis. The purpose of this is two-fold. First, by examining how developers choose third-party libraries and whether privacy is a consideration in this process, we can gain insight into the factors that influence these decisions. By using our tool as a probe, we can gather data on these processes and better understand the decision-making practices of developers in relation to privacy. Second, by evaluating the usefulness of our tool for developers in understanding the privacy practices of commonly used SDKs, we can assess the impact of the tool on developers' decision-making processes and determine whether it helps them make more informed decisions about selecting third-party libraries and informing end users. This aligns with our research question about the ef-

fectiveness of the tool in assisting developers in making informed decisions about the privacy practices of different SDKs and libraries.

To evaluate our tool, we first conducted semi-structured interviews, followed by surveys. During the interviews we made use of a cognitive walkthrough [347, 348] to systematically allow users to explore the tool. The interviews allowed us to delve deeper into developers' experiences and perceptions of the tool, as well as gather more in-depth information about their privacy practices and decision-making processes. For the survey, we utilised the Systems Usability Scale [427] to gather data on the overall usability and user satisfaction of the tool.

6.4.1 Participants and Recruitment

In recruiting participants, we were looking for developers who have experience developing mobile applications for children. We initially reached out to participants from our previous study, as they would have made good candidates to evaluate our tool. However, due to circumstances, they were not available to participate. We therefore started a new recruitment campaign.

Similar to the previous studies, we made use of various methods to recruit our participants. Firstly, we used popular search engines, such as Google and DuckDuckGo, and made use of keywords such as "Kids App Developers" and "Game Studio" to find participants. Secondly, we also made use of our network to circulate our study. Often, we had an initial email exchange or preliminary video call to discuss the details of the study, during which participants were informed about the consent procedure and their data rights. We recruited 12 children's app developers who were compensated with £15 Amazon gift voucher each. Our study protocol was reviewed and approved by an Institutional Review Board.

In total, we had twelve participants who were located in various countries. Children's app developers were incredibly difficult to recruit, which is why we had a limited sample size. We found that while the market for children's apps is big, there are not many children's app developers. We finally stopped recruitment after we had 12 participants, which research indicates is necessary to achieve data saturation and for stable themes to emerge [357]

While not all participants were located in the UK, they still had experience developing apps for the EU market. All participants were male and had direct experience with developing apps. Demographic information about the participants can be seen in Table 6.1.

Table 6.1: Table containing descriptive characteristics of the study participants. While all participants produced apps for the UK market, some were located in a different country.

Participant	Country	Role	Years of Exp.
P1	India	Lead Android developer	10+
P2	Brazil	Mobile game developer	5-10
P3	Armenia	App developer	2-5
P4	US	App developer	5-10
P5	Armenia	Web and Mobile developer	2-5
P6	Canada	App developer	0-2
P7	US	App developer	10+
P8	Israel	Mobile game developer	2-5
P9	Germany	App developer	5-10
P10	US	App developer	2-5
P11	Canada	App developer	5-10
P12	Bulgaria	App developer	2-5

6.4.2 Interview Procedure

We conducted 12 semi-structured interviews in the summer of 2022 using remote meeting software, such as Microsoft Teams, Google Meet, or Zoom, depending on the participants' preferences. All interviews were audio recorded with the participants' consent. We started each interview with a general introduction, during which we introduced ourselves, the research goals and objectives, and once again informed participants about the procedure.

Each interview consisted of three parts. The first part was about the developer's experiences in designing apps and the privacy considerations they had to make. We also shared screenshots of some of the app features from our earlier findings in which children were asked to comply with complex privacy policies (Figure 3.2a). We asked developers whether children should be empowered and supported to make privacy decisions. We kept this part brief as we had discussed some of it in our previous experiments. However, as as we had not worked with these participants before, we used this as an opportunity to inform the participants about our research and the line of thinking we were interested in.

In the second part we shared the public URL `DataAvalanche.io` with

our participants, asked them to open the URL and share their screen with us. In this part, we were interested in using the tool as a probe to uncover what participants thought about the privacy behaviours of commonly used SDKs.

Furthermore, to ensure consistency in the way that participants use our tool, make use of a cognitive walkthrough process [347, 348], which is commonly used to assess the usability of systems. During a cognitive walkthrough, one or more evaluators work through a series of tasks using the system and ask a set of questions from the users' perspective. In our case, the participants executed the following set of tasks and answered our associated questions:

1. First, participants opened `DataAvalanche.io` and shared their screens with us.

2. We allowed participants to glance over the tool and explore a bit on their own while voicing their initial thoughts and expressions.

3. For the interview, we had pre-selected two SDKs, Adjust and Unity Ads, which were available as chips below the search box. We told participants to select one of the two SDKs to explore more in depth section by section.

4. Participants next scrolled to the *metadata* section of `DataAvalanche.io`, where they could see important privacy and SDK information.

5. Participants scrolled to the privacy-friendly alternatives, where we asked them about when and how they would consider switching to SDKs.

6. Participants then scrolled to the *legal* section, where they could see a map of the countries the SDK shares data to and with. We asked participants if they were surprised by this behaviours and what their thoughts were. We also asked them if they would find this useful and how they would imagine using this in their development practices.

7. Participants then scrolled to the data sharing partners, which showed the knowledge graph in tabular and graph format. Similarly, we asked participants what they thought of the privacy behaviours of the SDK and whether this is what they expected. We also asked how they imagine using these features of the tool in their own development practices.

8. Finally, users scrolled to the bottom where they had the opportunity to read FAQs.

After these tasks were completed, while participants were still sharing their screen, we asked them about the usability of the tool itself. We asked which features they liked and disliked, which features they would like to see added, and how they would see themselves using this in practice.

At the end of the interview, we asked participants if they had any additional comments or questions. After the interview, we sent the participants the exit survey.

The interview guide for this is available in Appendix C.

6.4.3 Surveys

For the exit survey, we made use of the Systems Usability Scale (SUS) [427] to gauge the perceived usability of the tool from the perspective of developers. The SUS is a widely recognised and standardised evaluation tool that measures the usability of a product or system. It consists of 10 statements that users are asked to rate on a 5-point Likert scale, with higher scores indicating a higher level of perceived usability.

We also asked two open-ended questions at the end of the survey to solicit additional feedback from participants. The first question asked if there were any additional features that participants would like to see in the tool, and the second question asked for any additional comments. These open-ended questions provided us with valuable insight into participants' thoughts and ideas, and helped us to identify areas for improvement in the tool.

6.4.4 Data Analysis

The collected audio recordings of the interviews were transcribed and anonymised. To derive insights into developers' *challenges, perceptions, requirements, and values*, we made use of a thematic analysis approach [404].

Our thematic coding process was characterised by a collaborative consensus-building approach to ensure the rigour of the analysis [356]. The anonymised interview transcripts were divided into two equal-sized sets to facilitate a systematic analysis. An experienced HCI researcher and I independently analysed the first set of transcripts. This initial analysis generated an initial set

of codes. Importantly, we engaged in ongoing discussions to ensure consensus in code development, resulting in a shared understanding of the coding framework [356]. Following this, I completed the coding of the remaining half of the transcripts using the established common codebook, as well as the open-ended survey questions.

Code and data saturation was achieved after approximately coding 8 interviews, after which no new issues were identified and the codebook started to stabilise. At this point, we observed that no new themes or insights were emerging, and existing themes were being consistently reinforced [405]. In total, 31 unique codes were generated. The number of codes derived in this chapter is fewer than those in the previous chapters, as the cognitive walkthrough encompassed a much narrower range of topics than the former semi-structured interviews. The complete set of codes derived during this analysis, can be found in Appendix C.2.

Interviews lasted between 38 and 75 minutes, with the average interview being 46 minutes (SD=11).

6.5 Results

Here we report the results of the evaluation of `DataAvalanche.io`. We first start by describing the results from our interviews. Through our analysis we uncovered four high level themes:

We end this section with a description of SUS survey results.

6.5.1 Alternatives are Good but Not Always Applicable

`DataAvalanche.io` offers developers to view privacy practices of third-party libraries and also provides privacy friendly alternatives. We asked developers how they choose third party libraries, what privacy considerations are made here, and when they would consider alternatives.

In evaluating the usefulness of our tool for developers to consider privacy-friendly alternatives, such as open-source SDKs or those known to do less data tracking, we found that participants largely welcomed the option:

> "*I think the privacy-friendly alternative section is probably a really key feature because it suggests to me that if I'm using a library to*

do notifications, I can probably find something else and preferably, ones that are open source and that I can use in my application instead of this. " — P4

However, this sentiment was not shared by all participants, and in most cases, privacy was not a major decision factor when choosing SDKs. In fact, "*privacy concerns really just take a backseat, it is not the first thing that we think about*" (P11). Developers formulated four reasons why they would choose a prominent SDK over a privacy-friendly alternative.

Financial Incentives

Firstly, participants acknowledged that apps need to earn money, and that advertising is often the most lucrative way to do this. However, they also acknowledged that some advertising networks generate more profits than others, and therefore, there may not always be a strong incentive to choose a privacy-friendly network over a more lucrative one:

"*The problem was, to show an interesting ad to a user you're supposed to know them really well. Only two of the companies that could ever - I could think of right now - to know anyone in the planet more than anyone else is Facebook and Google. Others don't have that much privilege rights.* " — P1

Learning Curve and Time Investment

Secondly, participants indicated that they have already invested a significant amount of time in learning and becoming proficient with a particular SDK and its related features. Changing to a new SDK would negatively affect their productivity, workflow, and their ability to deliver the service they are offering. The challenge of learning a completely new tool, even if it is the best on the market, can be a significant obstacle.

"Whenever you use a new tool, especially analytics-wise, you have a big learning curve. You could create one of the best privacy-friendly analytics tools, but the problem is my eight years - or someone else's five years - learning curve could be on Google Analytics."

Feature Offering and Quality

Thirdly, some participants prioritised the features and quality of certain SDKs, indicating that this is one of the more important reasons for choosing an SDK, as the "*functionality of the actual third-party library is going to be the dominant factor in making a choice*" (P7). Others were a bit more direct and stated that "*in terms of choosing a platform, I'd say the faster and the better well-known, that's the priority*" (P2).

Additionally, participants indicated that some SDKs come built in with integration with many other tools and features, as is the case of Firebase, which hooks into many other Google products:

> "*Firebase has pretty much everything, so if you want a Google sign-up or a Facebook sign-up, or any of the third-party application signups, you can do it through Google.* " — P6

Education

Lastly, some participants indicated that certain SDKs are more accessible due to their popularity and the availability of educational resources online. This makes them more attractive to beginner developers or developers with a limited budget for acquiring technical skills.

> "*The thing is, with Firebase, why I'm using Firebase, because it's mainly popular. Every course that I watch and stuff like that in the Udemy, everyone uses Firebase. That's how I learned, and I really liked it. Afterwards, every time that I need stuff like that, I use Firebase.*" — P11

We finally asked participants what would prompt them to consider alternatives. They took a practical stance and stated that ultimately, the product offering is set by customer demand. If customers demand more privacy-centric products, then that is what they will provide: "*If there is a good enough demand, developers will have no other option to offer it*" (P1).

6.5.2 Privacy Implications are Useful for Transparency

Participants particularly liked the *legal implications* provided by our tool. They found them useful to address the *transparency* challenge they often

face. Participants reflected that when they choose libraries, often they could not exactly identify what data is being collected by these third-party libraries and what is being done with it. While they often had suspicions, they could not exactly put their finger on it: "*For example, when it comes to Firebase the data that we were storing, is it being used by Google or is it not? I'm not sure about it, but when it comes to Google Analytics I might have some doubts that they are using it. Crashlytics I don't think so. Yes, I've had some concerns about the data in Firebase, but I'm not really sure*" (P2).

They ascribe part of this problem to the complexity of privacy policies and terms and conditions, stating that they are not accessible and written in a way that the general public cannot understand it: "*Part of the problem is if you read through the disclosure that's written by lawyers, it has to be written very conservative from a legal standpoint, so it's not transparent. Nobody else but another lawyer could read it and make sense of it. You are asking if that achieves transparency, and no, it does not. It's legally is mumbo jumbo* " (P7). However, at the same time, participants expressed their frustration that do admit that third-party vendors often try to have everything 'technically' disclosed, and thereby have themselves legally protected. They referred to such practices as being invisibly transparent: "*companies do take information and they are pretty transparent, but I say they are invisibly transparent* " (P6).

Interestingly, many participants also mentioned that the *legal implications* discussions provided by `DataAvalanche.io` would also help them amend their privacy policies or appropriately inform end users: "*freelancers would be able to share it with clients if there are concerns about data privacy. If the clients live in a country where there are strict regulations when it comes to data sharing. This could be very useful,* " (P3). Furthermore, oftentimes developers need to list all third-party services integrated into their apps in the privacy policy, alongside notable privacy practices, which `DataAvalanche.io` makes substantially easier to do.

6.5.3 Data Tracking is Not Surprising

After showing participants the data sharing graphs, we asked them more concretely about their expectations surrounding data collection and sharing. While we expected our knowledge graph and data sharing maps to induce a shock factor, due to the pervasiveness and vastness of data sharing, we found that in general most participants were not very surprised. Most had

a strong belief that third-party SDKs collect and share much more data than is necessary: "*They probably know from each computer's IP what each person is browsing, and when you connect it to Google using Google Analytics. They would have access to whatever niche that your website is. They would basically gather all this data from the user using the IP, and they probably would connect it,*" (P3).

Some participants indicated that they were not entirely sure how to use the knowledge graph and how they could integrate it in their own development practices. Additionally, they were not sure what the privacy implications of the number of data sharing partners implied, suggesting that companies which have been around longer, would naturally have more sharing partners:

> "*I think because I don't really understand what you'd be doing with this data, I can't really comment on how useful the knowledge graph is or the data that's feeding that knowledge graph. I don't know what that supposed to do for me. The fact that Xander has 100 times more partners than somebody else, so what? They've been around longer, they're a bigger company probably means that they're the better product.*" — P7

Participants were not specifically surprised that companies were collecting and sharing as much data as possible. They accepted that "*they have a fiduciary responsibility to pursue revenue, it's what they're supposed to do, they're a company* " (P7). They believe that third-party vendors collect, sell and share data with other companies for purposes of advertising and targeted analytics: "*Oh, they're sharing it. They're getting money for it off the back end. They're sharing it with marketing companies or whatnot* " (P4). One participant went as far as to doubt the legality of such practices, but resigned to this being the reality of the current state of privacy: "*I don't know if it's illegal ... we don't have privacy in the modern internet*" (P5). They accepted that data tracking is an inherent part of life nowadays, even if users take measures to protect themselves: "*people might have pushed the Do Not Track button, but at the end of the day Facebook is still going to look at other parameters for your device and associate that*" (P11).

However, participants made some suggestions about how the data tracking information can be made more practically useful for them. Some participants suggested that the data sharing attributes can be crucial for them to

filter SDKs, in addition to links to open-source alternatives, and information on past data breaches from companies: " *I would love to see some kind of filter where I could say, okay, I would love only to share within Europe to have this to get me alternatives for example,* " (P9).

Some other participants suggested that this data tracking analysis capability can be helpful to analyse existing apps, and then automatically generate a privacy report, describing which third-party libraries are included, and more depth on what type of data specifically is being shared.

6.5.4 Putting `DataAvalanche.io` to Use

As part of the interviews we also asked participants how they would put `DataAvalanche.io` to use and what advantages it could offer in their development practices. While we envision very specific use cases for the tool, we realised that participants might be able to formulate creative use cases, drawing on their own experiences, which might be more relevant to the type of work they are doing.

Participants formulated three areas in which they foresee `DataAvalanche.io` being used in. Firstly, participants identified several ways in which our tool could be used to benefit children and end users of apps. For example, they suggested that it could be used to generate privacy policies and present privacy information to end users in an improved way. They also mentioned the possibility of using it for requesting consent in apps.

> "*If we create an application, we can let the users know that, let's say, Firebase share their data around the world. This way, we can [obtain] consent from the users.*" — P5

Secondly, participants also indicated that `DataAvalanche.io` can be personally used for their own development. They found it particularly useful that that all information is accessible through a central repository: "*It is good to have a place where you can find easily all these third-party tools and their documentation easily to access*" (P2). They also liked that certain privacy information was presented visually, as "*we understand visuals and it helps to take it home for the developer*" (P4). As a result, they found that this makes it easier to make decisions in choosing libraries. One developer gave an example of this:

> "*As you can see, there is so much difference between Amplify and Google Firebase. If we we're creating a bigger application it's better to use something like this [pointing to an SDK] so that they don't share too many data.*" — P5

Thirdly, participants indicated that privacy is becoming increasingly important in today's industry. Many investors and startups prioritise privacy, and developers often need to demonstrate strong privacy practices to obtain funding. One of the examples they suggested was tech-for-good companies, "*developers who have the best interest of the users, [as] they would use this application*" (P6). The increased demand for privacy also means that privacy-friendly SDKs which are now offered as alternatives will become more and more mainstream, and there is a need for a platform for them to communicate their availability.

> "*Privacy is a big thing now. It's becoming bigger and bigger nowadays. People are spooked about it, especially with the stuff with crypto going on. I think this is very important to have. It'll help you give a better description in your own privacy policies when you do write them. Especially when you get funding and everything, they're going to want to know all this stuff.*" — P4

6.5.5 Additional Requirements

Based on the requirements gathered from the developer interviews, it is clear that there are several key themes that participants consider when choosing SDKs for their apps. These include the need for navigation and filtering, to help them find the SDKs that meet their specific needs, the importance of having access to clear documentation and educational resources, the need to consider privacy implications, and the commercial considerations such as revenue and market trends.

In terms of navigation and filtering, participants mentioned the importance of being able to categorise and sort SDKs based on various criteria, such as popularity, features, or compliance standards. They also highlighted the need to be able to filter SDKs by countries and the ability to mark favourites and bookmarks for future reference.

Documentation and education were also identified as key considerations. Participants emphasised the importance of having access to clear and concise

documentation for SDKs, as well as educational resources such as tutorials and summaries of privacy policies. They also suggested the idea of embedding documentation directly into the tool and the possibility of community contributions to the tool.

Privacy was another important factor for participants, who highlighted the need to see more details about data sharing practices and who is benefiting from the data. They also mentioned the need to be alerted about privacy breaches and to be able to compare apps in terms of their privacy practices.

Finally, participants pointed out the commercial considerations they often have when selecting SDKs, such as the need to consider the revenue potential of their apps and the impact that certain SDKs might have on their market trends. They suggested the idea of being able to see trends and having the option of adding user data to a map.

While these new requirements were not implemented, these requirements demonstrate the complexity and varied considerations that developers have when it comes to selecting third-party libraries and SDKs for their apps. A full overview of all 17 requirements can be seen in Table 6.2.

Table 6.2: Additional requirements formulated by our participants to improve `DataAvalanche.io`.

Feature	**Explanation**
Ads	Add information about popular ad networks and their privacy practices to help developers make informed decisions about which ad networks to use.
Categorize SDKs	Organize SDKs by their function to help developers easily find the tools they need.
Sort by popularity	Rank SDKs by their popularity among developers to see which ones are most commonly used and trusted.
Embed documentation	Include relevant documentation and code snippets directly in the tool to make it easier for developers to find and use the information they need.
Tutorials	Provide instructional materials or tutorials to help developers understand how to use the tool and make informed decisions about which SDKs to use.
Privacy breaches	Display any past privacy breaches or issues that a particular SDK has had to help developers understand the risks associated with using certain tools.

App upload	Allow developers to upload their app and receive a privacy check or comparison to identify potential privacy issues and make improvements.
SDK comparisons	Compare the privacy practices and features of different SDKs to help developers make more informed decisions.
Mark favorites and bookmarks	Allow developers to mark their favourite or frequently used SDKs, or bookmark ones they want to keep track of, to quickly access the tools they need.
More data sharing details	Provide more detailed information about the types of data that each SDK shares to help developers understand the potential privacy implications.
Who is benefiting from the data	Use data or visualisations to show which companies are benefiting most from the use of certain SDKs to help developers make more informed decisions about the trade-offs they are making.
Filter SDKs by countries	Allow developers to filter SDKs by the countries that they share data with to help them select tools that align with their privacy goals and comply with regulations such as the GDPR.
Trending	Display the most popular or frequently used keywords or categories to help developers quickly find the tools they need and stay up-to-date on industry trends.
Summary privacy policy	Use natural language processing to summarize the privacy policies of SDKs to help developers more easily understand the key points and make informed decisions about which tools to use.
Community contributions	Allow developers to suggest open source libraries or provide recommendations for privacy-friendly alternatives, and include links to the libraries' GitHub pages, to help developers discover new tools and contribute to the community.

Add user data to map	Use a map to show where users of an app are located, and provide information about the percentage of users in each country, to help developers better understand the potential privacy implications of using certain SDKs and make informed decisions.
Ratings	Add ratings or a trust score to third party libraries, based on metrics such as user reviews or third party evaluations, to help developers make informed decisions about which tools to use in their projects.

6.5.6 Survey Results

The survey consisted of two parts, the SUS questions to assess the usability of `DataAvalanche.io`, and two open-ended questions prompting for additional requirements and comments.

The answers to the SUS questions showed that participants generally had positive reactions to the usability of `DataAvalanche.io`. For example, they largely agree that *the system was easy to use, the functions were well integrated, and people would learn to use this system quickly.* However, there were some statements that received mixed responses, including the frequency of use and the ease of learning. While some participants agreed that they would use the tool frequently and that it was easy to learn, others demonstrated different opinions on *the consistency of the system* or *whether the system was cumbersome to use.* Figure 6.4 provides a full overview of the SUS results.

In response to the survey's open-ended questions, participants proposed several requirements to improve `DataAvalanche.io`. Largely, these requirements reflected the requirements formulated in the interviews. The suggestions encompassed features such as a comparison functionality to evaluate third-party tools, a "favorites" option for saving preferred stacks, user-generated content for sharing opinions on specific libraries, and side-by-side comparisons. Additionally, participants emphasised the importance of providing clear explanations of map data, incorporating ratings or trust scores for library assessments, and summarising key aspects of privacy policies. They also expressed interest in open-source library listings. Some partic-

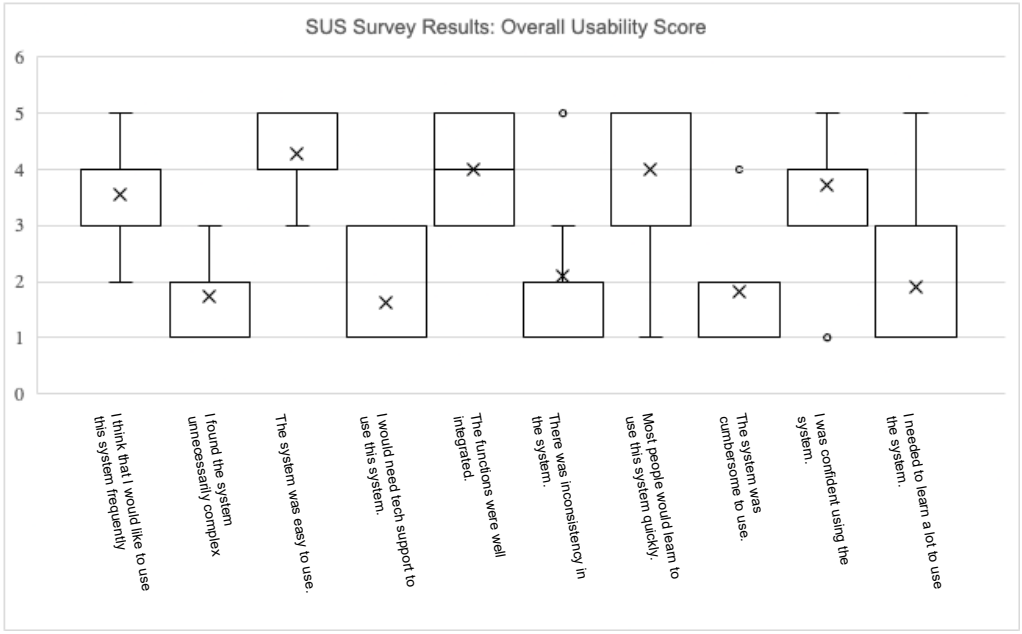


Figure 6.4: The results of our SUS survey.

ipants recommended adding more colour and detailed infographics to the tool. One participant noted, "*more features need to be added to the website and also a tutorial video needs to be included*" (P10) reflecting the desire for user-friendly enhancements.

6.6 Discussion

6.6.1 Summary and Key Findings

In this study we designed `DataAvalanche.io`, a web-based tool which helps provide transparency on privacy practices of commonly used SDKs for developers to make more informed privacy choices in their app development practices. We motivated the design of tool based on previous literature and findings from the former chapters. Specifically, we focused on the need to provide transparency about third-party libraries, which we identified in Chapter 4, and drew on requirements participants formulated in Chapter 5 to inform

the design. Our evaluation of `DataAvalanche.io` with children's app developers provided us with an important understanding of the factors that influence their decisions when selecting third-party libraries, as well as their needs and preferences for privacy guidance and tools.

Firstly, this study allowed us to gain an understanding of the trade-offs developers make when considering privacy in their apps. We were able to closely monitor their decision-making thoughts and identify four main reasons why developers prioritise certain factors over privacy when choosing third-party SDKs: the need for monetisation, the learning curve associated with a new SDK, availability of educational resources, and quality of the SDK and the feature offering. Previous research has identified the importance of using third-party libraries in software development [27, 438], but our study sheds new light on the specific considerations developers have in mind when making these choices.

Secondly, our evaluation also revealed that developers had positive reactions to the visual and legal aspects of the tool. They appreciated the clear and concise presentation of information, as well as the ability to easily understand and compare the privacy practices of different SDKs. The legal features, such as the ability to view which countries SDKs shared data with and the legal implications of this, were highly valued by our participants.

Thirdly, our study found that participants had difficulties understanding the privacy implications of third-party libraries sharing data and had difficulty figuring out how to use the knowledge graph effectively.This suggests that perhaps this information is too abstract and not actionable enough, and requires being presented in a more practical way to be useful.

Finally, participants identified several additional requirements for our tool that would help them make more informed decisions about the privacy practices of different SDKs and libraries. These requirements build upon the features of our prototype, and include features such as categorising SDKs by their functionality, ranking SDKs by popularity, displaying documentation and code examples directly in the tool, and providing tutorials or information about the differences between SDKs. Overall, these requirements demonstrate the complexity and varied considerations that developers have when it comes to selecting third-party libraries and SDKs for their apps.

6.6.2 Affecting Developer Practices and Choosing Alternatives

One of the features of `DataAvalanche.io` was to propose alternative, privacy-friendly third-party SDKs. Our intention was to help developers avoid using prominent SDKs provided by organisations known for their data collection and advertising practices, such as Google and Facebook. Previous research has shown that developers find third-party libraries and SDKs essential to their development practices because they can simplify development and generate revenue [27, 438, 154]. However, our evaluation of the tool revealed additional reasons why developers might not choose a privacy-friendly alternative, suggesting that inducing change is not as straightforward as simply providing information about the landscape of third-party SDKs.

This suggests that it may be challenging for privacy-friendly SDKs to compete with more well-established options that offer a wider range of features and support. To be successful, privacy-friendly SDKs may need to not only offer similar functionality, but also provide clear and actionable guidance for developers on how to use them to protect the privacy of their users. Participants also indicated that much of the drive for privacy in apps is dictated by market demand, suggesting once again the importance of a multi-stakeholder approach to improving privacy in apps (we saw this in Chapter 5 as well).

In order to effectively improve privacy in apps, there needs to be a focus not only on the technical aspects of privacy-enhancing tools and guidance, but also on the economic and social factors that influence developers' decisions. This suggests that the HCI community has a role in working with other stakeholders, such as policymakers, user advocates, and industry partners, to create a supportive environment that encourages developers to prioritise privacy in their apps. This may involve creating financial incentives for privacy-friendly practices, raising awareness about the importance of privacy among users and developers, and developing standards and guidelines for app development that prioritise privacy.

6.6.3 Evaluating Privacy Implications Through Increased Transparency

Participants reacted favourably to the legal visualisations and implications which we presented in our tool. Previous research already indicated that

there is a need for increased awareness and transparency around legal matters of app development [270], but our research confirmed that developers welcome practical tools which address this. Our feature for conveying legal implications is still largely a prototype, as GDPR requirements are statically displayed to the user. We can envision that this feature is expanded to dynamically change based on the data sharing countries, or based on when a user hovers their mouse over a country. However, for this to be realised, we require a comprehensive analysis of data protection regulations of different countries and jurisdictions. Such an analysis was beyond the scope of this thesis, but we do recommend this as an important direction for future research.

One of the novel insights we shared with our participants is the knowledge graph which portrays the fourth-party tracking ecosystem. As far we are aware, such as graph currently does not exist. However, our evaluation of this with developers showed that they were not entirely sure how to interpret it and how they could use it in practice. Several participants reacted in shocked manner to finding out how much data is being shared. However, participants also wanted to know how they could use it in practice. We realise that participant require features which are practical and which can immediately be applied in their own work. One potential solution for addressing this issue is to provide more concrete examples of how the knowledge graph can be used in practice, such as case studies or scenarios that demonstrate the benefits of using privacy-friendly SDKs and avoiding certain third-party libraries. Additionally, the HCI community can play a role in developing more user-friendly and intuitive ways of presenting this information, such as interactive visualisations or tools that allow developers to more easily explore and understand the implications of different data sharing practices.

6.6.4 Improving `DataAvalanche.io`

In our evaluations with children's app developers, participants identified several additional requirements for our tool to better support their decision-making process in choosing third-party libraries. These requirements included features such as categorising and filtering SDKs based on different criteria, providing clear and concise documentation, displaying data sharing practices and the companies benefiting from the data, and displaying trends and user data on a map.

We interpret these additional requirements as a positive sign that the

prototype of DataAvalanche.io which we presented to participants can be turned into a useful product to help with matters of privacy in apps. We find that some of the requirements which participants formulated can easily be implemented, such as improving the design and usability. One such requirement which was requested by multiple participants was the ability to compare multiple SDKs side by side. In implementing such a comparison feature, we can make use of what we know about the decision process from developers, for example by clarifying the amount of educational material, the necessary learning curve, and the overall feature offering.

However, participants also formulated several requirements which in turn would require further research. Firstly, participants indicated that they would like to upload apps for a full analysis. Past research has shown how static analysis of apps can reveal the trackers and third-party libraries present in apps. We can draw on this to complement DataAvalanche.io with a tracker analysis apps currently in development.

Secondly, participants indicated that they would like to have privacy policies summarised, so that they can immediately learn what the privacy practices and implications are of using a certain SDK. There is a large body of research being done in the automated analysis of privacy policy through the use of NLP techniques. We can draw on some of these methods, and implement such techniques in our tool to provide a more comprehensive analysis of privacy practices of SDKs.

Thirdly, participants also proposed community contributions through ratings and trust scores. Privacy labels have recently become more popular, as both Apple and Google have started using variants of them. Apple forces developers to disclose all personal information collected in apps [422], and Google now has an initiative where developers can choose to disclose which data is collected and whether it is shared with third parties [352]. However, these tools are aimed end users, rather than developers. A similar initiative for developers to rate the privacy-friendliness of SDKs, alongside their usefulness, could persuade developers to adopt more privacy-friendly alternatives.

The fact that participants formulated such concrete requirements is highly beneficial for the HCI community, as efforts now can be made to support them through designing tools that address these needs. These requirements provide insight into the specific challenges that developers face when it comes to protecting the privacy of their users, and can help inform the design of tools that can better support them in this task.

Finally, some improvements that might make DataAvalanche.io more

accessible to the wider community include more closely integrating known open source resources for privacy tools for developers [439] to make our knowledge base and privacy analyses more comprehensive. Additionally, we could consider open sourcing our tool in the future to allow for contributions from the development community.

6.6.5 Limitations

We would like to address two limitatins which we encountered in this study. Firstly, due to difficulties in recruiting, we had a limited sample size. While 12 participants generally are sufficient for data saturation to reach [357], we also acknowledge that the app development process is complex, different types of apps require different specialisations and SDKs. In addition, the app development process can involve many stakeholders, including UX designers, database engineers, and coders. We also limited ourselves to children's app developers, by considering SDKs and legal implications specific for children. However, some of the efforts also apply to all apps in general. Some possible ways to address these limitations in future studies could include recruiting a more diverse sample of developers, such as those who work on different types of apps or those who have different levels of experience and expertise. This could help to ensure that the results are more representative of the broader app development community and provide a more comprehensive understanding of the challenges and needs related to privacy in app development.

Secondly, in developing `DataAvalanche.io`, several of the parts were still in the phase of being high-fidelity prototypes. For example, the legal implications and privacy-friendly alternatives were not entirely fleshed out, as we used those parts to probe participants' responses. This means that the results of our study may not fully reflect the potential usability and effectiveness of a fully developed version of the tool. In future work, we will aim to further refine and test the tool in order to better understand its impact on developers' decisions about third-party libraries and SDKs.

6.7 Conclusion

In this study, we drew upon all the findings of the previous chapters to design and evaluate `DataAvalanche.io`, a web-based tool for developers to shed light on the privacy practices of commonly used SDKs for children's

app developers. Through this tool, we were aiming to help developers better understand the privacy and legal implications of using certain SDKs, and encouraging them to consider privacy-friendly alternatives instead. The findings of this study chapter provide us with an important understanding of developers can be supported in designing privacy-friendly apps for children.

`DataAvalanche.io` was inspired by the problems formulated by study participants in Chapter 4 and 5. In Chapter 4, participants made it clear that they would like to have increased transparency on the privacy practices of third-party libraries and SDKs. In Chapter 5, participants formulated further requirements for how supporting tooling should look like. We used these requirements to inform the design of `DataAvalanche.io`, which is now publicly available.

We evaluated `DataAvalanche.io` with 12 children's app developers to understand how it helped them understand privacy practices of commonly used SDKs and whether they would consider privacy-friendly alternatives. Firstly, we found that developers prioritise certain factors over privacy when choosing third-party SDKs and identified five main reasons for this. This chapter provides insight into the trade-offs developers make when considering privacy in app development. Secondly, we found that developers had positive reactions to the visual and legal features of the tool, including the clear presentation of information and the ability to compare privacy practices of different SDKs. They also found the legal features, such as the ability to view which countries data was shared with and the legal implications of this, quite valuable. Thirdly, we found that participants had difficulty understanding the privacy implications of third-party libraries sharing data and using the knowledge graph effectively. This suggests that the information may be too abstract and not actionable enough, and may need to be presented in a more practical way to be useful. Finally, our participants formulated a range of additional requirements which they would like to see implemented in our tool.

The findings of this chapter show how we can help developers understand the privacy implications of commonly used SDKs through developing supporting tooling. These findings provide important directions for future research in the HCI community. Firstly, our study highlights the importance of considering privacy as a core element in the development practices of children's app developers. This is particularly relevant given the increasing demand for privacy in the digital age and the need for tools that can help developers make informed decisions about the privacy practices of different

SDKs and libraries. Secondly, our study also highlights the need for tools that provide clear and actionable guidance for developers on how to use privacy-friendly alternatives to protect the privacy of their users. Finally, our study suggests that efforts should be made to provide more practical and actionable information for developers, as they struggled to understand the abstract and complex nature of the data sharing practices of third-party libraries.

7 Conclusion

Contents

7.1 Introduction 215

7.2 Review of Research Goals and Findings 216

7.2.1 RQ1: *What privacy features are available in children's apps and can children's apps be considered to be privacy-friendly?* 217

7.2.2 RQ2: *What are the key considerations and current practices of app developers when designing apps for children?* 219

7.2.3 RQ3: *How do app developers want to be supported in designing privacy-friendly apps for children?* . . 220

7.2.4 RQ4: *Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?* . . . 222

7.2.5 RQ: *What are the key considerations and challenges for developers when designing privacy-friendly children's apps and how can we better support them in this process?* 223

7.3 Contributions 224
7.3.1 A Research Driven Methodology to Evaluating Privacy in Apps 225
7.3.2 An Understanding of What Privacy Looks Like in Children's Apps 225
7.3.3 An Understanding of Why Privacy in Children's Apps is an Uphill Battle 226
7.3.4 Requirements to Support Developers to Improve Privacy in Children's Apps 226
7.3.5 `DataAvalanche.io`: the Development and Evaluation of a tool to Support Developers to Improve Privacy in Children's Apps 227
7.4 Directions for Future Research 227
7.4.1 Development of Multi-Stakeholder Approaches for Building Privacy-Friendly Apps 228
7.4.2 Exploring Socio-Technical Support for Developers 228
7.4.3 Exploring Alternative and Ethical Marketplaces and Platforms 229
7.5 Concluding Remarks 229

7.1 Introduction

Children are increasingly gaining access to and capitalising on the opportunities presented to them in the digital world. Through the use of mobile devices, they have access to a multitude of apps available on popular marketplaces, such as the Google Play Store [4] and the Apple App Store [3]. Whilst such apps offer many potential positive experiences, such as education and entertainment, they may also be associated with privacy risks that have tangible consequences, such as the loss of autonomy, political influences, and targeted advertising.

As computer science researchers, it is our responsibility to ensure that children can take full advantage of the positive aspects of the digital world, whilst also being shielded from potential harms. In this thesis, we sought to explore this problem through the lens of children's app developers. As the

developers have an integral role in the way apps are designed, we set out to determine how we can support and encourage them to make privacy an essential component of their development processes. To achieve this, four research questions were formulated and answered in this thesis:

RQ1 What privacy features are present in children's apps and to what extent can these apps be considered privacy-friendly in the UK market?

RQ2 What are the key considerations and current practices of app developers when designing apps for children?

RQ3 How do app developers want to be supported in designing privacy-friendly apps for children?

RQ4 Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?

We answered the research questions posed in this thesis through four chapters using a mixed-methods approach. Our analysis of the current privacy landscape of children's apps in enabled us to gain an understanding of the privacy concerns present in these apps, which provided a basis for our subsequent work with children's app developers to address these concerns. The culmination of this work was the design and evaluation of `DataAvalanche.io`, a web-based tool to help developers understand and navigate the complex privacy behaviours and practices of commonly used SDKs in children's app development.

In this final chapter, we will review the research questions, discuss the key findings and contributions, and provide directions for future research.

7.2 Review of Research Goals and Findings

This thesis started with a literature review and background section, through which we motivated our research questions. Each of our four research questions is answered in a separate chapter: RQ1 in Chapter 3; RQ2 in Chapter 4; RQ3 in Chapter 5; and RQ4 in Chapter 6. Below, we review these research questions and highlight our key findings.

7.2.1 RQ1: *What privacy features are available in children's apps and can children's apps be considered to be privacy-friendly?*

We started this thesis with an examination of the current privacy landscape for children's apps in Chapter 3. We sought to perform a privacy analysis of children's apps. However, to inform our analysis, we began with a conceptualisation of what such an analysis should look like through a systematic literature review of 48 papers. This review helped us understand how the research community conceptualises privacy in apps and what features they use to evaluate privacy. Through the review, we identified several shortcomings in the current literature on privacy analyses. Firstly, we found that privacy analyses are concentrated around using a few features, mostly privacy policies and permissions. We then review these features through the lens of the AADC (see 3.2) to better understand which areas of privacy could benefit from increased attention. We found that many studies focus on technical features, rather than user facing features aimed at understanding how well children are equipped to understand and exercise their privacy rights. Secondly, we also found that most studies do not focus on children's apps, but either rather broadly sample apps from the marketplaces or focus on genre specific apps (e.g., COVID or mHealth).

We used these findings to establish a more holistic method for analysing privacy in children's apps, consisting of a user-facing dimension and a technical dimension. We applied this method on a dataset of 137 'expert-approved' children's apps. Through this analysis we found that children's apps frequently lack privacy features that support children, while extensively making use of trackers. To further explore the consequences of losing control of privacy in such a manner, we investigated how data by third-parties is shared with further entities. In this process, we mapped the *fourth-party* tracking ecosystem through the creation of a knowledge graph. Similar to our literature review, we contextualised our findings against the AADC (see 3.4), to examine how our findings aligned with regulatory expectations and identify specific areas where these children's apps may be in breach of AADC standards. Through this analysis, we were able to provide concrete examples of how and where children's apps fail to meet the standards set by the AADC in terms of protecting children's privacy and data protection.

The two dimensional analysis of children's apps we performed show that

one the hand children's apps are collecting and sharing data, to the detriment of children's privacy, while simultaneously not supporting them to negotiate their privacy rights in apps. Importantly, through mapping part of the fourth-party ecosystem, we show that apps might inadvertently distribute data into a vast network of data sharing partners, where data is uncontrollably further distributed. We refer to this principle as a *data avalanche*. Our analysis of this shows that there are structural and systemic privacy issues in an ecosystem controlled by a vast network of actors. One of the issues is that the lack of transparency in this makes it difficult to investigate or understand what is exactly is going on and who is control of what data. Once data leaves an end user's device and is fed into this fourth-party ecosystem, it is safe to assume it will be nearly impossible track and exercise any control of this data, especially considering it may be transferred to countries where consumers do not have strong privacy rights.

The data tracker analysis was only one dimension of our privacy evaluation method. We also had a critical look at user facing privacy features in apps. Amongst the many issues, we importantly found that apps do not provide sufficient privacy support for users to negotiate the extent of data tracking. Apps often made privacy terms complex and consent non-negotiable, leading to the formation of a one-way relationship between apps and children, where children give up their data in return for very little benefit. Moreover, we found that many apps limit children from accessing privacy settings and information through age-assurance mechanisms.

As a result, we asked ourselves what the root is of this problem and what is causing this. However, as with any complex systems such as this, it is hard to pinpoint at a single stakeholder or phenomenon causing this. We considered two important stakeholders for this. Marketplaces, such as Google and Apple, need to negotiate this delicate balance between protecting end users while providing developers with a platform to create and offer apps. However, their true role in this is questionable. It has long sine been known that companies such as Google have a vested interest in the advertising industry [188], which in turn thrives on targeted analytics. While we have seen an increase in consumer protection initiatives from them [352], it remains yet to be seen what impact such measures have on the privacy of children.

On the other hand, we also considered developers who create and design apps for children. In many ways, they too are clients of the marketplaces, similar to how end users are. However, they are also tasked with ensuring that the apps they develop make privacy a key consideration in their design

[42], which in recent years has placed on them a special responsibility. The findings from Chapter 3 show that this is something that has not been upheld well in children's apps, and combined with an out-of-control tracking ecosystem, this creates a dangerous and threatening environment for children's privacy. In turn, this leads us to question the role developers in this: are they responsible? And what can we do to encourage them to make changes in the development practices to prioritise privacy? We consider these questions in depth in RQ2.

7.2.2 RQ2: *What are the key considerations and current practices of app developers when designing apps for children?*

To explore children's app developers' perceptions and barriers to privacy-friendly app development we conducted 134 surveys and 20 interviews.

Our findings show that developers care about children's privacy and their best interests. They feel a moral responsibility to ensure that children's privacy is protected in apps and employ a range of strategies to realise this in apps. For example, they try not to collect more data than necessary and if they do collect data they ensure it is all anonymised. Despite this, they also indicated to face several challenges which prevented them from always acting in children's best interests. Firstly, they mentioned that some form of data collection through third-party libraries is unavoidable. Collecting data for analytics is essential to improve and provide basic functionality for the app. However, choosing third-party libraries to do this, they often went for prominent and well known vendors, such as Google and Facebook. Secondly, they felt that there was a lack of guidelines to support them in designing apps for children. They felt that current guidelines, such as the GDPR, are too technical and not aimed at developers. And finally, developers struggled with issues related to monetisation. They indicated that potential privacy-friendly ways of monetising apps, such as making apps premium or offering in-app purchases, are not sustainable as they do not generate sufficient revenue. In addition, at times they competed with malicious actors in the marketplaces, which would clone apps and offer them for free, or face end users which demanded free apps by leaving negative reviews. As a result, developers felt forced to make use of methods such as targeted advertising monetise their apps. They described this as a feeling of making a trade-off between

protecting children's privacy and sustaining their business.

If we look more closely at the discrepancy between developers' intentions to incorporate privacy-friendly design principles and their practices, we gain further insights about potential solutions to overcoming these issues. The complexity of the mobile ecosystem suggests that overcoming privacy issues needs a multi-faceted and multi-stakeholder approach. It requires a paradigm shift which changes the way we think about developing and designing technologies. However, this is something that we probably cannot achieve solely through affecting development practices. Through our interviews, we have learnt that developers find themselves to also be subject to the larger plans of marketplaces. Therefore, any paradigm shift would require the cooperation of major stakeholders, including marketplaces, and an increased awareness amongst consumers about the importance of privacy. We have discussed a few of the difficulties in realising such changes, such as economic incentives. However, even in the face of such changes, developers continue to play a key role in this, and we need to more carefully formulate what exactly we can expect from them. Through the study in Chapter 4, it has become clear that developers need support to understand and navigate the complexities of the data infrastructure of the mobile ecosystem as much as end users do. This leads us to investigate more closely what this support should look like and how this support can be offered in a way that positively affects children's privacy at the same time.

7.2.3 RQ3: *How do app developers want to be supported in designing privacy-friendly apps for children?*

Having established challenges developers face in designing privacy-friendly apps, in Chapter 5 we sought to draw out concrete requirements for developing tools to support them. In this study, we made use of a *Research through Design* (RtD) [387] method to evaluate a series of design ideas, aimed at supporting developers in privacy-friendly app development, to identify requirements which developers have for supporting tools and technologies. RtD is a method which generally involves the development of design that shows a product which interacts with people in a way that was not possible before. In our case, RtD is a specifically useful, as we need to find new ways to make changes to structural and systemic problems in the app marketplaces.

Through an ideation workshop with other HCI researchers, we came up with 12 speculative design ideas, which in turn we evaluated with 20 children's app developers. The design ideas we proposed aimed to tackle the challenges we identified in Chapter 4. Through semi-structured interviews, we presented each of the ideas and elicited the participants responses. We asked them whether they liked the ideas, what they liked about it, and whether they would consider using a practical implementation of the concept.

Participants in this study formulated both technical and socio-technical requirements for overcoming barriers to integrating privacy-friendly features in their apps. The technical requirements were mostly functional in nature, relating for example to how guidelines and SDKs should look like. These requirements can be translated into concrete tools and support, for example through offering checklists for the AADC or the GDPR. However, in addition to these requirements, participants also formulated a range of socio-technical requirements which involved the blank of other stakeholders.

Firstly, participants found it important that guidelines and SDKs are backed by credible and trustworthy institutions, as a way to motivate and rationalise the importance of privacy-friendly apps towards other stakeholders. They formulated several ways to achieve this, such as certifications and privacy labels. They found that this increased negotiation and marketing position which such solutions could provide, would offset any additional development costs. Secondly, when evaluating our design ideas, participants' main focus had been on how integrating privacy-friendly features may affect the market acceptance of their apps. Their consensus was that the perceived costs associated with implementing privacy features must be compensated by equal market competence. Our participants were concerned that end users might not always have a sufficient understanding of the importance of privacy in apps, leading to their lack of valuing privacy-friendly app features. Lastly, our participants indicated that systemic changes in current marketplaces and platforms are critical to moving to a mobile ecosystem where privacy-friendly apps become the norm. However, they acknowledged that this is incredibly difficult and would require cooperation from major market leaders. Instead, they expressed the importance of platforms to consider bringing in *gradual* changes, which could facilitate an increase of users' awareness and value of more privacy-friendly apps for children and thus a gradual transformation from a single, data-driven app ecosystem.

While this chapter produced a comprehensive set of requirements for supporting developers, from their perspective, we also have to acknowledge that

some of these requirements do not have a sole technological solution. Instead, as we saw in Chapter 4, they require a paradigm shift in the way apps are monetised and accepted in the developer communities and by end users. However, in addition to these, we are also presented with requirements for how they wish to be technically supported to improve privacy for children. For example, in Chapter 4 we already saw a need for increased transparency in the landscape of third-party libraries. In Chapter 5 and in answering RQ3, we were presented with requirements for how developers would want this need to be supported. As the tools they request do not exist yet, we also do not know how they would affect developers' practices. This is what we investigated in the final chapter.

7.2.4 RQ4: *Could better support for developers in navigating the privacy implications of third-party libraries affect their practices and decision-making in building privacy-friendly apps for children?*

After having established requirements from children's app developers as to how they would like to be supported in designing privacy-friendly apps for children, in Chapter 6 we used these requirements to build and evaluate `DataAvalanche.io` so that we could assess whether a better technical support may affect app develoeprs' practice of building privacy-friendly-apps for children.

`DataAvalanche.io` consists of three main components that are aimed to help developers to navigate commonly used SDKs for children's app developers. To begin with, users can search and explore SDKs along with their relevant privacy information, such as a link to the privacy policy and documentation page for children's configurations. This section also offers privacy-friendly alternatives to commonly used SDKs. Secondly, users can examine the legal implications regarding where the data sharing countries of an SDK is visualised through a map. Lastly, users can navigate and interactively explore the data sharing partners of SDKs. We evaluated `DataAvalanche.io` with 12 children's app developers.

Through our evaluation we found that developers reacted differently to different parts of the tool. Firstly, they found it useful that we created a central repository containing commonly used SDKs along with their privacy information. While, they appreciated the privacy-friendly alternatives we

offered, they also formulated several higher priority considerations they need to make before changing their current practices. These include the need for monetisation, the learning curve associated with a new SDK, availability of educational resources, quality of the SDK, and the feature offering. This shows that developers consider more aspects than simply the 'prominence' of SDKs when making a decision to use them [270, 440]. Secondly, we found that participants particularly liked the legal implications which we presented to them, showing that there is a strong need to demystify and clarify the legal requirements set out by regulatory bodies when designing apps for children. Thirdly, participants indicated that they were not entirely sure how to interpret or use the data tracking graph which we provided. Some participants were slightly shocked at the degree to which data is being shared, but in general we found that participants were looking for practical guidance and use cases. The ability to explore the tracking ecosystem did not directly translate to something actionable in their development practices. We thus also asked them for any ideas of how this could be turned into something that would be more useful. Participants suggested highly practical ideas, such as using it to clarify privacy policies or to inform end users when obtaining consent.

In addition to these findings, participants also formulated additional requirements which they would be keen to see integrated in future iterations of the tool. These include the need for navigation and filtering, to help them find the SDKs that meet their specific needs, the importance of having access to clear documentation and educational resources, the need to consider privacy implications, and the commercial considerations such as revenue and market trends. These requirements indicate that participants find `DataAvalanche.io` a promising initiative, which may help them in the future once the feature offering is expanded.

7.2.5 RQ: *What are the key considerations and challenges for developers when designing privacy-friendly children's apps and how can we better support them in this process?*

Finally, it leads us to examine our overarching research question which we set out at the beginning of the thesis. We must remember that the goal of our research is not to *enforce* a practice for the app developers. Instead, we sought to find out ways to support developers navigating the complexities of

the mobile ecosystem and become more considerate of the privacy implications of their app development practices. In the first half of the thesis, we identified several challenges developers struggle with in making privacy a key consideration in their development practices. Through our Research through Design approach, we uncovered several solutions to how these challenges can be overcome. Importantly, participants formulated a range of socio-technical challenges which extend beyond what can solely be done for developers. For example, developers proposed the need for increased awareness and normalisation of privacy-friendly development within the developer community itself, as well as an appreciation for privacy by end-users and parents. Therefore, if we wish to imagine a world where privacy-friendly apps are the norm, it would require a paradigm shift, through a multi-faceted multi-stakeholder set of changes.

At the same time, we also realise that there are concrete efforts we can make to support developers individually to overcome challenges preventing them from adopting privacy-friendly principles in their design processes. In Chapter 6, we took the first steps towards making this happend. Through the development of a web-based tool, `DataAvalanche.io`, we successfully managed to demystify what third-party libraries and SDKs are doing and how they are behaving. We have learnt that developers benefit from the value offered by `DataAvalanche.io`. More importantly, we also increasingly better understand what features developers need and would like to see further implemented to shed light on an otherwise opaque and complex landscape.

As the need and demand for increased privacy is becoming vastly widespread, it is more important than ever that developers have the resources to cater to this paradigm shift. The road to better privacy in children's apps is long and change always takes time. But this thesis has made important steps in providing insight into what a future where privacy-friendly apps are the norm will look like.

7.3 Contributions

Having discussed the key findings and their implications, we formulate the key contributions this thesis has made. While we formulate these contributions in the individual chapters, we can now take a more holistic perspective, to see how this thesis has contributed to our understanding of the privacy landscape of mobile apps for children and the role of developers therein.

7.3.1 A Research Driven Methodology to Evaluating Privacy in Apps

Before performing our own privacy analysis of apps, we sought to establish what a comprehensive research driven methodology would look like for evaluating privacy in apps (Chapter 3). While data protection frameworks formulate on a high level what is expected from developers [42, 91], they do not provide methods to evaluate this in apps (and other digital products). Similarly, past research has focused on a small subset of privacy features in apps, such as tracking [319, 324, 331], permissions [21, 332, 334], or privacy policies [328, 329], we sought to perform a more holistic analysis incorporating multiple types of features in apps. By analysing past privacy assessment methods against the AADC, we were able to identify areas of privacy which have not received much attention (i.e., user facing features). Through this, we established a more holistic method for evaluating privacy in apps consisting of a user-facing and a technical dimension. The method we proposed is both timely and much needed, as regulatory bodies and consumers are becoming increasingly aware of the importance of privacy, leading to requirements about how digital services should be designed and shaped [42]. We are thus in need for robust methods for evaluating privacy in apps, which can address such regulatory requirements, for example as those put forth by the AADC. We are thereby hoping that the framework we developed through this study can be used in future research to position the privacy analysis of apps against a more rigorous and comprehensive set of standards.

7.3.2 An Understanding of What Privacy Looks Like in Children's Apps

In the past decade, many studies have been performed to investigate how apps uphold privacy standards. However, as we established in Chapter 3, through our literature review, at the time of writing, few studies look specifically at children's apps. This is especially problematic, as we see a rise in the consumption of digital media by children [2], paired with a market for apps targeted specifically at them [4]. Our analysis of 'expert-approved' children's apps provides a snapshot of how privacy standards are integrated in children's app (more specifically it shows the lack thereof). While past studies have looked at features for children in apps, for example parental control features [345], few studies have looked at privacy features in children's apps

specifically. We find that this is especially timely and important given the current debate and attention on children's privacy. Marketplaces are increasingly positioning themselves as being privacy-friendly, in favour of consumers [4, 422]. However, we are also aware that such marketplaces may not always have the consumers' best interest in mind. It is therefore crucial that we employ robust methodologies for verifying claims pertaining to privacy, in order to ensure that platforms and marketplaces are adhering to the standards they claim to uphold. Thus, in conjunction with our research-driven privacy assessment methodology, the privacy landscape we examined provides compelling evidence for the need of research investigations regarding the design of privacy-friendly apps and how to support developers creating them.

7.3.3 An Understanding of Why Privacy in Children's Apps is an Uphill Battle

While there is an increasing demand to improve privacy in apps, in Chapter 4 we have shown that this process in itself is not straightforward. The environment for developing and publishing apps, as created by marketplaces, is optimised towards rewarding those apps which make use of practices such as targeted advertising and in-app purchases. This makes it difficult for developers to face growing pressures to incorporate data protection and privacy into their apps, showing that they too are subject to the larger strategies of marketplaces. Specifically, we have identified two structural and systemic problems in the current ecosystem. Firstly, the trade-off that developers face between prioritising children's privacy and monetisation. Secondly, the intricate and complicated data sharing infrastructure underlying and funding much of the marketplaces. These systemic issues point not only to the need to support developers, but a general shift in the way to go about designing and distributing apps.

7.3.4 Requirements to Support Developers to Improve Privacy in Children's Apps

Much of the research in the HCI community involving app developers has been limited to understanding their perceptions and behaviours, explain why certain privacy-unfriendly design practices are common [10, 28]. In light of these findings, the common recommendation is that developers can benefit

from usable tools to identify privacy issues in apps [26, 270]. However, our understanding of what exactly developers to need to face some of the systemic and structural barriers imposed on them by monopolistic data controllers and marketplaces was still limited. In Chapter 5, we took the first steps towards addressing this, by working with developers to draw out requirements to support them in navigating these barriers and designing privacy-friendly apps for children. We have provided a starting point for future work that could support developers in this task.

7.3.5 `DataAvalanche.io`: the Development and Evaluation of a tool to Support Developers to Improve Privacy in Children's Apps

We know from research that developers struggle with understanding the legal language and implications surrounding software development [368, 27]. This is something that we have explored in detail in this thesis. The developers we interviewed formulated a range of technical and socio-technical challenges to privacy-friendly app development. We acknowledge that it is not possible to address all these challenges as once, and much is left open for future research. However, in this thesis, we aimed at providing a solution to the specific challenge of navigating the complex landscape of third-party libraries. In Chapter 6, we developed and evaluated `DataAvalanche.io`, a web-based tool which provides transparency on the privacy practices of commonly used third-party SDKs. Through this, we made a first step into addressing the challenges for developers and making privacy-friendly app development a bit more viable. Moreover, we also learnt what exactly developers need, and what their decision-making process looks like when evaluating privacy-friendly design principles. The requirements formulated by participants and the findings from our evaluation provide crucial directions for future research.

7.4 Directions for Future Research

Throughout the thesis, we have indicated research we might want to conduct in the future. Here we broadly summarise some of these research directions.

7.4.1 Development of Multi-Stakeholder Approaches for Building Privacy-Friendly Apps

Children's privacy in mobile apps is a multi-stakeholder problem. A broad array of actors are involved in the development, distribution, and use of mobile apps for children, including app developers, marketplaces, advertisers, parents, and children. Each of these actors have their own motivations, constraints, and incentives, which can influence the design and implementation of privacy measures in apps.

In this thesis we have primarily focus on app developers, seeking to understand their role in this multi-stakeholder problem and to identify ways to support them in designing privacy-friendly apps for children. We have already highlighted the importance of considering additional stakeholders to normalise privacy in children's apps. For example, in proposing supportive tooling in Chapter 5, several ideas would benefit from the input of parents and children.

7.4.2 Exploring Socio-Technical Support for Developers

In our research, we focused on demystifying the privacy practices of third-party SDKs and libraries for children's apps, as this was a concern raised by app developers in our interviews. However, developers also identified other challenges they face, such as the need for guidelines, compliance checking tools, and increased awareness among end users. These requirements address different aspects of the problem and may require input from additional stakeholders.

Future work could benefit from further evaluating these requirements and exploring how they could be integrated into a comprehensive framework to support app developers in designing privacy-friendly apps for children. This could involve, for example, conducting additional research with developers and other stakeholders to identify best practices and guidelines, developing tools to help developers assess compliance with privacy regulations, and working to increase awareness among end users about the importance of privacy in children's apps.

7.4.3 Exploring Alternative and Ethical Marketplaces and Platforms

Finally, in our work, we mostly focused on the Android operating system. We did this as Android currently has a majority market share and we make use of Android devices in our lab for experiments. We already say in Chapter 3 that a focus on iOS is missing. For future work, the research community could benefit from an increased understanding of privacy in iOS apps, and whether developers make different considerations.

There are several notable differences between Google and Apple when it comes to privacy. Apple has taken several strict measures in favour of consumer privacy, such as the mandatory privacy labels on the app marketplaces and the consent framework for third-party tracking [355]. Given these differences, it is worthwhile to investigate how this impacts developers and whether the mindset towards developing apps for children on iOS is significantly different.

7.5 Concluding Remarks

It is inevitable that the use of mobile technologies by children will continue to grow in the coming years, with it becoming increasingly common for young children to have access to tablets in school for educational purposes. While these technologies offer numerous benefits, they also come with risks and harms that must be addressed. It is our responsibility to ensure that children can take advantage of the positive experiences mobile digital devices provide while also protecting them from potential dangers.

In this thesis, we systematically examined the privacy landscape of mobile apps for children and collaborated with children's app developers to understand their challenges in prioritising privacy in their development practices and to identify requirements and challenges for overcoming these challenges. To assess whether a practical support may indeed affect their privacy development practices, we then incorporated some of these requirements into a publicly available tool to assist developers in navigating the complexities of the mobile ecosystem's data infrastructure.

In this thesis, we made use of a range of qualitative and quantitative research methodologies to closely collaborate with important stakeholders who play a crucial role in contributing to the privacy of the mobile ecosystem.

Through our research we have made important first steps towards creating a mobile ecosystem where privacy-friendly apps are the norm and identified a series of informed future research directions.

While there is still much work to be done, we believe that our contributions provide a valuable starting point for future efforts to support app developers in designing privacy-friendly apps for children and to create a safer and more privacy-protective online environment for children. We hope that our work will inspire others to join us in this important mission, and that our vision for an ecosystem in which ethical apps are the norm and children can use mobile technologies safely and securely will eventually become a reality.

A

Supplementary Material Chapter 4

A.1 Interview Guide

Below are the questions we used for our semi-structured interviews in Chapter 4. We started each interview with a brief description of our research questions and objectives. Prior to the interviews, participants would have already received an information sheet and consent form. Participants would able to verbally give consent to the interviews prior to starting.

We ended each interview asking the participants whether they had any questions or comments for us. We then informed them about what the following steps would be for us.

1. What is the reason that you decided to develop a children's safety app/parental control app?
   (a) Why do you think children are not safe online?
2. In your opinion, what does online privacy mean for children?
3. What are the primary risks for children when they are online?
   (a) How does your app address these risks?

4. What is the role of parents in children's safety online?
5. Should the app encourage discussions between the parent and child?
6. Do you think that a safety app will improve trust between parents and their children, or drive a wedge between them?
7. Do you think that parents should be able to technologically intervene using their own devices, when children are using their smartphone or tablet?
    (a) How important is it for children to remain autonomous and what effect does parent monitoring have on this?
    (b) Should parents be able to read the text messages of their children?
8. Should they be allowed to track the location of their children?
    (a) Is it important for children to enjoy or accept the app?
    (b) If so, what is being done to appeal to them?
9. Is commercial success of the app important, and why (not)?
10. What features of your app do you anticipate will make your app a success in the market?
11. Many apps contain advertisements using third party trackers, is it acceptable for safety apps to have them as well, as they are primarily targeted at children?

A.2 Survey Questions

Developer Practices surrounding Security and Privacy of Family Oriented Apps

Introduction

We would like to invite you to take part in a study. Please read the information on this page carefully and email the researchers (see below) before proceeding should you have any additional questions.

Study title: Developer Practices surrounding Security and Privacy of Family Oriented Apps

General Information

We appreciate your interest in participating in this questionnaire/ online survey. You have been invited to participate as **you or your company has developed apps targeted at families**. Please read through these terms before agreeing to participate by ticking the 'Next' button below.

We (The University of Oxford) are investigating the views and development practices of developers towards family-oriented apps. We hope that our findings will help in understanding why developers make certain security and privacy design choices.

If you take part, you will be invited to answer some multi-option questions and a few questions requiring short textual inputs, regarding the app you have developed.

The survey is expected to last **~15 minutes**. No background knowledge is required. Your responses will be stored for analysis by the researchers. Your answers will be completely **anonymous**, and we will use all reasonable endeavours to keep them confidential.

Please note that your participation is **voluntary**. You may **withdraw at any point** during the questionnaire for any reason, before submitting your answers, by closing the browser.

How will your data be used?

All the data collected in the study will be captured, transferred and stored on a secured server hosted by the Department of Computer Science, in compliance with the University of Oxford Policy on the Management of research data and records. All steps will be taken to ensure that no personally identifiable information will be collected or retained. Data will be stored securely for a minimum period of ten years after project publication and then destroyed. Data will only be transferred across the research team through password-protected university systems or the handover of a non-networked encrypted hard drive.

This study is part of a research project led by Anirudh Ekambaranathan and is supervised by Dr Jun Zhao (Department of Computer Science, University of Oxford).

This project has been reviewed by and received ethics clearance through, the University of Oxford Central University Research Ethics Committee, reference number: CS_C1A_19_021.

What if there is a problem?

If you have a concern about any aspect of this project, please speak to the project supervisor:

Dr. Jun Zhao. (jun.zhao@cs.ox.ac.uk)

Dr. Zhao who will do her best to answer your query. Your concern should be acknowledged within 10 working days and you will be given an indication of how she intends to deal with it.

If you remain unhappy or wish to make a formal complaint, please contact the chair of the Research Ethics Committee at the University of Oxford (using the contact details below) who will seek to resolve the matter in a reasonably expeditious manner:

Chair,
University of Oxford, Computer Science Departmental Research Ethics Committee.
Department of Computer Science, University of Oxford
Parks Road, Oxford
OX1 3QD

Please note that you may only participate in this survey if you are 18 years of age or over.
✱ *Required*

- [ ] I certify that I am 18 years of age or over.

If you have read the information above and agree to participate with the understanding that the data (including any personal data) you submit will be processed accordingly, please check the relevant box below to get started. ✱ *Required*

- [ ] Yes, I agree to take part.

Open Questions

You are invited to participate in the survey because we have identified you as an app developer for families or children. To complete the rest of the survey, we would like you to briefly describe (in one or two sentences) one of such apps that you have recently developed. You don't have to name the app if you don't want to.

Have you applied any design principles (such as user-led designs or participatory designs) to the development of the app? And if so, can you please briefly describe what design principles have been applied, and how?

Focus and Value of the App

Who are the primary users of the app you have most recently developed?

- ○ Parents
- ○ Children
- ○ Other

If you selected Other, please specify:

Who are the secondary users of the app?

- ○ We identify no secondary users
- ○ Parents
- ○ Children
- ○ Other

If you selected Other, please specify:

If the app is expected to be used by children, what age group do you expect the children to be?

- ☐ 0 – 5
- ☐ 6 – 9
- ☐ 10 – 12

- [ ] 13 – 15
- [ ] 16 – 17
- [ ] Other

Which of the following best describes the motivation for you to develop this app:

- ○ Nothing on the market was good enough or fulfilled our criteria for such a family oriented app
- ○ I feel this is a very important application
- ○ I feel there is a huge commercial potential in this area
- ○ We have a similar product for users of other age groups
- ○ I was assigned by my company to develop the app
- ○ No particular reason
- ○ Other

If you selected Other, please specify:

What do you expect the most important benefits your app will bring to the primary users?

Please select no more than 3 answer(s).

- [ ] They will learn something new
- [ ] They will improve their existing skills
- [ ] They will be entertained
- [ ] They will have a good time with their friends or families

- [ ] They will learn something they cannot achieve in other environments
- [ ] They will keep in touch with their friends or families
- [ ] Other

If you selected Other, please specify:

What kind of improvements have you seen your app already bring over similar existing apps?

Security and Privacy of App Development

Which of the following do you think are the primary risks for children when they are online? Select up to 3 options.

Please select between 1 and 3 answers.

- ☐ Cyberbullying
- ☐ Virus
- ☐ Grooming
- ☐ Addiction
- ☐ Sexting
- ☐ Inappropriate content, images or games
- ☐ Impact on their general wellbeing
- ☐ Impact on their mental health
- ☐ Other

If you selected Other, please specify:

Please indicate how much you agree with each of the following statements.

Parents of young children should have complete control over the smartphone or tablet usage of their children, in order to safeguard them.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

Parents of young children need to monitor all smartphone and tablet usage of their children (such as which apps they use or where they have been), no matter whether they have had their children's awareness or consent.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

It is acceptable for apps to show advertisements containing third-party trackers.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

It is acceptable for apps to show advertisements from third-party trackers, even if the app does not verify whether it is children who may see these adverts.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

It is acceptable for the app developers to sell data of adult users to third parties in order to sustain their business.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

It is acceptable for the app developers to sell data of users, including children's data, to third parties in order to sustain their business.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

Development practices

During the design of your app, which of the following parties have been involved:

Please select at least 1 answer(s).

- [ ] Parents
- [ ] Children
- [ ] Educators
- [ ] Scientists
- [ ] Investors
- [ ] Other

If you selected Other, please specify:

Which of the following plays the most important role in informing the design of your app?

Please select at least 1 answer(s).

- [ ] Market research
- [ ] Media
- [ ] Latest research
- [ ] My managerial team
- [ ] Investors
- [ ] My intuition
- [ ] Other

If you selected Other, please specify:

During your app development, do you make use of any third-party libraries? (For example, Firebase, Ionic, Retrofit etc.)

- Yes
- No

Development practices: third party APIs

Do you make use of any of the following third-party APIs?

- [ ] Google Analytics
- [ ] Google APIs
- [ ] DoubleClick
- [ ] Amazon
- [ ] Microsoft
- [ ] Facebook
- [ ] Twitter
- [ ] Mopub
- [ ] Crashlytics
- [ ] Yahoo
- [ ] Flurry
- [ ] Verizon
- [ ] Verizon
- [ ] Unity Tech
- [ ] Chartboost
- [ ] AppLovin
- [ ] Cloudflare
- [ ] Opera
- [ ] Other

If you selected Other, please specify:

What are your primary reasons for you to make use of third-party libraries? (Select up to three options)

- [ ] Convenience
- [ ] Cloud computing support
- [ ] Provide targeted adverts for my users
- [ ] Make my users data accessible to third parties
- [ ] Reuse existing software modules
- [ ] Other

If you selected Other, please specify:

Does your company have any existing practice regarding choosing third-party libraries?

- ○ It has to be approved by my team manager or above
- ○ We have a list to choose from
- ○ I can choose whatever I want
- ○ We discuss amongst colleagues
- ○ Other

If you selected Other, please specify:

Do you test libraries for security or privacy related issues?

- Yes
- No

How do you assess whether a third-party library is safe to use?

Business Strategies of Your App

What are the primary sources of income for the app? (Select 2 options at most)

Please select no more than 2 answer(s).

- [ ] We are supported by advertisements
- [ ] Pay per download
- [ ] In app purchases
- [ ] Subscriptions
- [ ] Affiliate or CPI programmes
- [ ] We are supported by other lines of products
- [ ] We are a non-profit
- [ ] We are running at a loss
- [ ] Other

If you selected Other, please specify:

Which of the following best describes the business model of the company?

- ○ We are a start-up funded by investors
- ○ We develop software for clients
- ○ We rely on the revenue our software generates
- ○ Other

If you selected Other, please specify:

If you selected Other, please specify:

Commercial success of the app was an important factor in the development of our app.

Please don't select more than 1 answer(s) per row.

	0	1	2	3	4	5	
Strongly disagree	☐	☐	☐	☐	☐	☐	Strongly agree

The Information Commissioner's Office in the UK is an information authority that uploads information rights in the public interests that reports directly to the Parliament. They are developing a new set of codes to protect children's best interests online.

Have you experienced any conflicting views between you and your company when it came to features affecting children's data and privacy? If so, could you please briefly explain what happened?

Are you aware of any conflicts in your app between protecting children's best interests and the commercial revenue of your app?

- ☐ No
- ☐ We use adverts to sustain our app, which in turn tracks the behaviour of our users
- ☐ We collect data of children and users which we use sell after anonymising

- [ ] Other

If you selected Other, please specify:

Have you ever had to make a personal trade-off between the best interest of children and the commercial success of the app? If so, could you briefly explain?

Do you personally apply any strategies to minimise the negative impacts to children's online data privacy?

- [ ] No
- [ ] I make use of libraries which have tested as secure
- [ ] I do not collect unnecessary data of users
- [ ] I make use of known age appropriate design principles
- [ ] I do not use nudge techniques to lead or encourage children to provide unnecessary personal data
- [ ] I make sure settings are 'high privacy' by default
- [ ] Other

If you selected Other, please specify:



Demographic information

What is your age?

- 18 - 22
- 23 - 29
- 30 - 39
- 40 - 49
- 50 - 59
- 60 - 64
- 65+

What is your gender?

- Male
- Female
- I identify as non-binary
- I prefer not to say

What is your native language?

- English
- Other

If you selected Other, please specify:

What is your current employment status?

- Full time paid employment
- Part time paid employment
- Self-employed
- Student
- Retired
- Other
- I prefer not to say

How long have you been working in the current organisation?

- Less than 1 year
- 1-3 years
- 3-5 years
- 5-8 years
- 8-10 years
- Over 10 years

How long have you been developing apps for children or families?

- Less than 1 year
- 1-3 years
- 3-5 years
- 5-8 years
- 8-10 years
- Over 10 years

How many family or children's apps have you developed in the last 2 years?

- Less than 3
- 3-5
- Over 5

Which of the following described your highest achieved level of education?

- High School
- A-Levels
- Bachelor's Degree
- Master's Degree
- Doctoral Degree
- I prefer not to say
- Other

If you selected Other, please specify:

What is your country of origin?

Do you have children, if so, how many?

- No

- 1
- 2
- 3
- 4 or more
- I prefer not to say

Closing questions

In light of these survey questions, would you change your existing development practices? Explain briefly your reasons.

Have you had to consider questions you did not consider while developing the app?

Final page

Thank you very much for participating in our survey!

If you have any further questions or comments please contact the researchers below:

Dr. Jun Zhao (jun.zhao@cs.ox.ac.uk)

Anirudh Ekambaranathan (anirudh.ekam@cs.ox.ac.uk)

Key for selection options

41 - What is your country of origin?

AD - Andorra
AE - United Arab Emirates
AF - Afghanistan
AG - Antigua and Barbuda
AI - Anguilla
AL - Albania
AM - Armenia
AO - Angola
AQ - Antarctica
AR - Argentina
AS - American Samoa
AT - Austria
AU - Australia
AW - Aruba
AZ - Azerbaijan
BA - Bosnia and Herzegovina
BB - Barbados
BD - Bangladesh
BE - Belgium
BF - Burkina Faso
BG - Bulgaria
BH - Bahrain
BI - Burundi
BJ - Benin
BL - Saint Barthelemy

BM - Bermuda
BN - Brunei
BO - Bolivia
BR - Brazil
BS - Bahamas, The
BT - Bhutan
BV - Bouvet Island
BW - Botswana
BY - Belarus
BZ - Belize
CA - Canada
CC - Cocos (Keeling) Islands
CD - Congo, Democratic Republic of the
CF - Central African Republic
CG - Congo, Republic of the
CH - Switzerland
CI - Cote d'Ivoire
CK - Cook Islands
CL - Chile
CM - Cameroon
CN - China
CO - Colombia
CR - Costa Rica
CU - Cuba
CV - Cape Verde
CW - Curacao
CX - Christmas Island
CY - Cyprus
CZ - Czech Republic
DE - Germany
DJ - Djibouti
DK - Denmark
DM - Dominica
DO - Dominican Republic
DZ - Algeria
EC - Ecuador
EE - Estonia
EG - Egypt
EH - Western Sahara
ER - Eritrea

ES - Spain
ET - Ethiopia
FI - Finland
FJ - Fiji
FK - Falkland Islands (Islas Malvinas)
FM - Micronesia, Federated States of
FO - Faroe Islands
FR - France
FX - France, Metropolitan
GA - Gabon
GB - United Kingdom
GD - Grenada
GE - Georgia
GF - French Guiana
GG - Guernsey
GH - Ghana
GI - Gibraltar
GL - Greenland
GM - Gambia, The
GN - Guinea
GP - Guadeloupe
GQ - Equatorial Guinea
GR - Greece
GS - South Georgia and the Islands
GT - Guatemala
GU - Guam
GW - Guinea-Bissau
GY - Guyana
HK - Hong Kong
HM - Heard Island and McDonald Islands
HN - Honduras
HR - Croatia
HT - Haiti
HU - Hungary
ID - Indonesia
IE - Ireland
IL - Israel
IM - Isle of Man
IN - India
IO - British Indian Ocean Territory

IQ - Iraq
IR - Iran
IS - Iceland
IT - Italy
JE - Jersey
JM - Jamaica
JO - Jordan
JP - Japan
KE - Kenya
KG - Kyrgyzstan
KH - Cambodia
KI - Kiribati
KM - Comoros
KN - Saint Kitts and Nevis
KP - Korea, North
KR - Korea, South
KW - Kuwait
KY - Cayman Islands
KZ - Kazakhstan
LA - Laos
LB - Lebanon
LC - Saint Lucia
LI - Liechtenstein
LK - Sri Lanka
LR - Liberia
LS - Lesotho
LT - Lithuania
LU - Luxembourg
LV - Latvia
LY - Libya
MA - Morocco
MC - Monaco
MD - Moldova
ME - Montenegro
MF - Saint Martin
MG - Madagascar
MH - Marshall Islands
MK - Macedonia
ML - Mali
MM - Burma

MN - Mongolia
MO - Macau
MP - Northern Mariana Islands
MQ - Martinique
MR - Mauritania
MS - Montserrat
MT - Malta
MU - Mauritius
MV - Maldives
MW - Malawi
MX - Mexico
MY - Malaysia
MZ - Mozambique
NA - Namibia
NC - New Caledonia
NE - Niger
NF - Norfolk Island
NG - Nigeria
NI - Nicaragua
NL - Netherlands
NO - Norway
NP - Nepal
NR - Nauru
NU - Niue
NZ - New Zealand
OM - Oman
PA - Panama
PE - Peru
PF - French Polynesia
PG - Papua New Guinea
PH - Philippines
PK - Pakistan
PL - Poland
PM - Saint Pierre and Miquelon
PN - Pitcairn Islands
PR - Puerto Rico
PS - Gaza Strip
PS - West Bank
PT - Portugal
PW - Palau

PY - Paraguay
QA - Qatar
RE - Reunion
RO - Romania
RS - Serbia
RU - Russia
RW - Rwanda
SA - Saudi Arabia
SB - Solomon Islands
SC - Seychelles
SD - Sudan
SE - Sweden
SG - Singapore
SH - Saint Helena, Ascension, and Tristan da Cunha
SI - Slovenia
SJ - Svalbard
SK - Slovakia
SL - Sierra Leone
SM - San Marino
SN - Senegal
SO - Somalia
SR - Suriname
SS - South Sudan
ST - Sao Tome and Principe
SV - El Salvador
SX - Sint Maarten
SY - Syria
SZ - Swaziland
TC - Turks and Caicos Islands
TD - Chad
TF - French Southern and Antarctic Lands
TG - Togo
TH - Thailand
TJ - Tajikistan
TK - Tokelau
TL - Timor-Leste
TM - Turkmenistan
TN - Tunisia
TO - Tonga
TR - Turkey

TT - Trinidad and Tobago
TV - Tuvalu
TW - Taiwan
TZ - Tanzania
UA - Ukraine
UG - Uganda
UM - United States Minor Outlying Islands
US - United States
UY - Uruguay
UZ - Uzbekistan
VA - Holy See (Vatican City)
VC - Saint Vincent and the Grenadines
VE - Venezuela
VG - British Virgin Islands
VI - Virgin Islands
VN - Vietnam
VU - Vanuatu
WF - Wallis and Futuna
WS - Samoa
XK - Kosovo
YE - Yemen
YT - Mayotte
ZA - South Africa
ZM - Zambia
ZW - Zimbabwe

A.3 Interview Codes and Themes

Table A.1: Codes Organised by Themes

Theme	Code
Developers' Perceived Responsibilities and Motivations	Better experience and less addiction
	Children shouldn't spend on apps
	Educational app
	High quality content more important than gaming techniques
	Moral obligation
	Respect children's privacy
	Targeted ads are bad
	Users' needs are paramount
Perceptions of Data Collection Practices	Ads have implication on personal privacy
	Apple guidelines are sound
	Apple is better than Android for data privacy
	Children's data not useful
	Confusion about what should be right for children
	Data collection can be a liability
	Developers are responsible for children
	Good practice needs to be shared with the team in order to be appropriately followed
	Google guidelines are sound
	Google libraries are industry standard
	Its okay to target parents instead of children
	Lack of transparency in data infrastructure
	Lack of transparency in third party libs
	Large companies will get away anyway
	Market acceptance has to be built upon data
	Market leaders are trustworthy
	There is a tradeoff between commercial success and best interest

Continued on next page

Table continued from previous page

Theme	Code
	Guidelines not good enough
	Appropriate ads are not bad
	Big companies need to take responsibility
	Cannot trust third-party libs
	Children will anyway use apps
	Collecting anonymized data is not bad
	Parents are uneducated
	Perceptions of risks for children
Reliance on Third-Party Libraries	Choice of third-party audit based on reputation not knowledge
	Use of third-party libraries
	Use third-party audit companies
	No third-party tracking
	No use or need for data collection
	No data sharing practices
	In-house security standards
	GDPR triggered more rigorous internal practice
	Developer doesn't need data
	Audit own apps
	Audit external providers to ensure no PI collection
	App does not collect data
	App collects anonymized data
The Need to Earn Money	Apps don't earn a lot of money
	Competition makes monetization difficult
	Demand from users for free apps
	Lack of good monetization options
	Pressure to design according to client's needs
	Pressure to monetize
	Ads
	Alternative business models
	App is outsourced or designer-led
	Free app
	Freemium model
	Paid app only

Continued on next page

Table continued from previous page

Theme	Code
	Subscription-based monetization
	Use of in-app purchases
	Regulation is ineffective
	App has to abide by play store rules
	Awareness of regulations
	Following regulations is tedious
	Little awareness of regulations
	Regulation for children is important
	Unequal regulation across jurisdictions

B

Supplementary Material Chapter 5

B.1 Interview Guide

Below are the questions we used for our semi-structured interviews in Chapter 5. We started each interview with a brief description of our research questions and objectives. Prior to the interviews, participants would have already received an information sheet and consent form. Participants would able to verbally give consent to the interviews prior to starting.

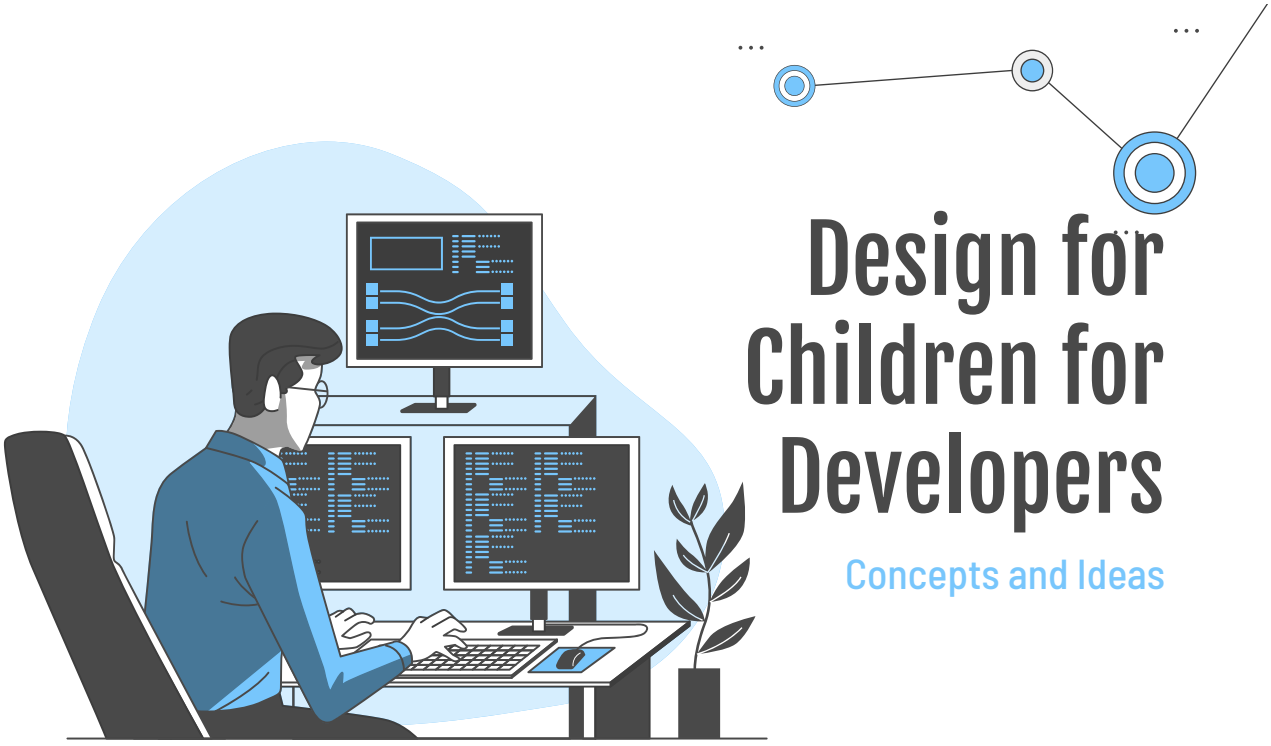
During this interview we shared our screen with participants, presenting them our design ideas. Before we shared our screen, we asked several general questions learn a bit more about our participants:

1. Can you tell me a bit about your background and experiences in developing apps for children?
2. What are your views on privacy in children's apps?
   (a) Is this something you have to consider in your daily work practices?
3. How would you go about encouraging or helping developers to make privacy more salient in their apps?

After sharing our screens, we showed participants our design ideas one by one. During each of these ideas, we asked participants what they liked or disliked and idea, and whether they would consider using it themselves.

We ended each interview asking the participants whether they had any questions or comments for us. We then informed them about what the following steps would be for us.

B.2 Design Workbook



Design for Children for Developers

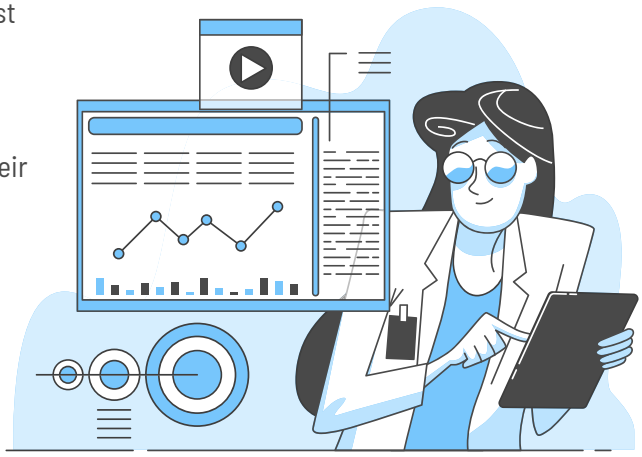
Concepts and Ideas

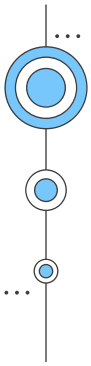
Table of Contents

01 **Understanding**
Tools to help understand best practices.

02 **Helping**
Tools to aid developers in their practices.

03 **Incentivising**
Tools and systems to incentivise developers to comply.



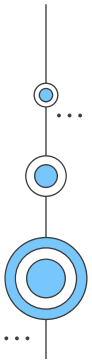




01
Understanding

Tools to help understand best
practices in designing for children.







Dos and Don'ts checklist

Infographic or checklist showing what should and should not be done in apps/services; allows developers to keep track during the design process; on paper or digitally.

Hypothetical examples

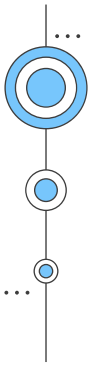
	Do's	Don'ts
Privacy policies	Show the privacy policy at startup.	Do not make the privacy policy technical.
Screen time	Allow users to set limits to their screen time.	Do not reward users for increased gameplay.
...	...	...
Transparency	Explain clearly how their data is used and by whom.	Do not add data trackers from third parties.

02

Courses: make it official

Traditional course, e.g. such as those offered on Udemy or Coursera, with an official certification from [redacted]; specialised in designing for children; 20 - 40 hours.





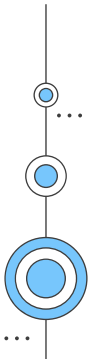


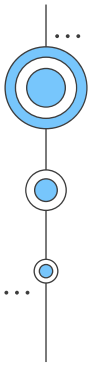
Requirements matrix

Requirements according to different marketplaces, guidelines, regulations, and institutes; overview and non-interactive.

	ICO	Google	GDPR	COPPA
Personalised ads	✗	✗	✗	✗
Must include parental controls	✗	✓	✗	✓
Opt-out data collection	✓	✗	✓	✗
Push notifications	✓	✓	✗	✗







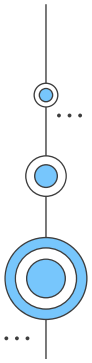


02

Helping

Tools to aid developers in their practices.

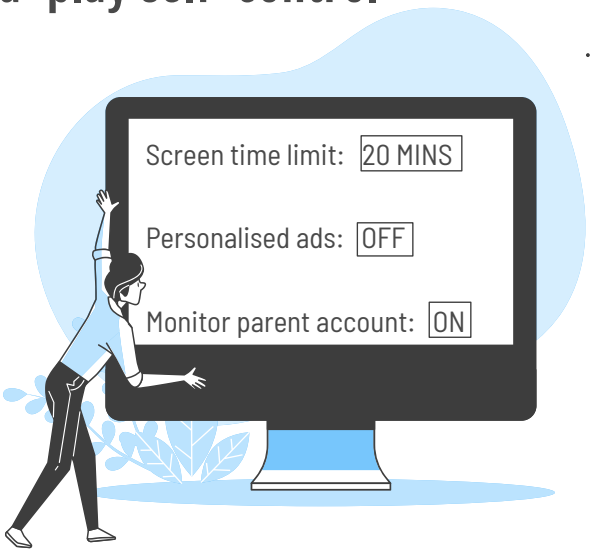




04

Plug-and-play self-control

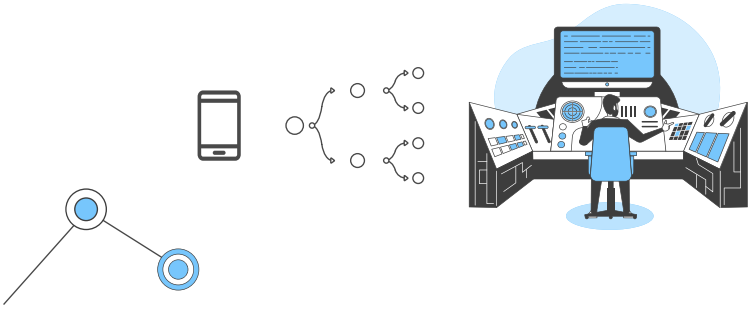
Library which can be imported and used in a plug-and-play fashion allowing parents and children to decide how to interact with the app.



05

Machine over mind

Webpage where your app or website can be uploaded, which automatically checks if your app meets certain data protection and transparency standards.

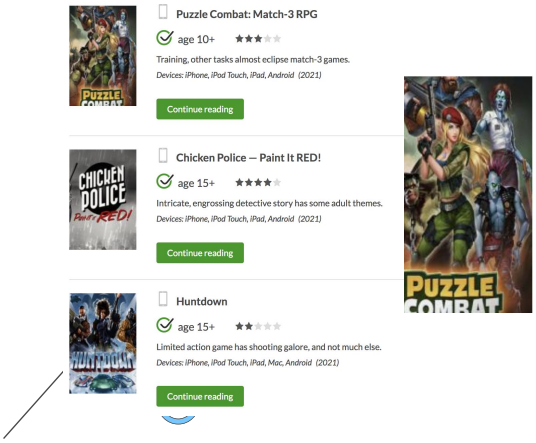


	Result
Personalisation	⊗
Parental controls	⊗
Opt-out collection	✓
Push notifications	✓

06

Wisdom of the crowds

Social network of parents who review apps according to age-appropriate compliance templates; allows for negotiation and interaction (surveys, interviews).



Common Sense says

age 10+

Training, other tasks almost eclipse match-3 games.

iPhone, iPod Touch, iPad, Android | Strategy Games

Save | Rate app

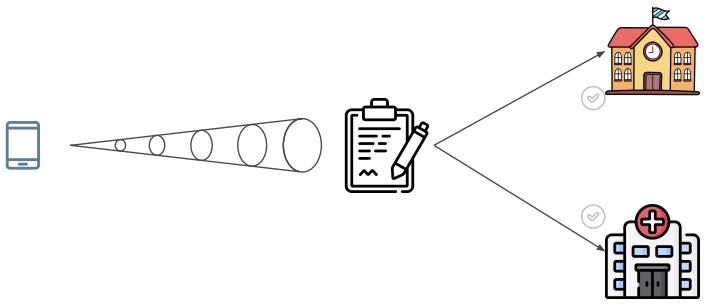
Launch survey

24 reviews	Result
Personalisation	98%
Parental controls	21%
Opt-out collection	56%
Push notifications	78%

07

Universal compliance service

Agency or platform which takes care of all compliance needs, e.g. when form-filling is required by governments, hospitals, schools, to prove that services are age-appropriate.



08

Parental assistance

Fill out features of your app, this tool automatically generates guidelines, warnings, and resources for parents, as to how they should interact with your app.

Attributes

What should parents know about your app?



Generation

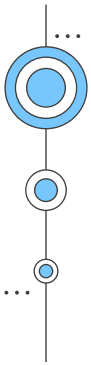
Computer generates a guidance leaflet



Attach

Page can be attached to app or mailed to parents





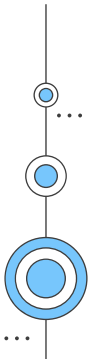


03

Incentivising

Tools and systems to incentivise developers to create age-appropriate services.





09

Public pledges and awards

Ask companies to take public pledges that they will develop technology for good according to certain standards. They will then be awarded (by us) for upholding these.

Fire Game Design
"Our games allow children to exercise self-control."

Blizzard
"We will not use persuasive techniques and nudges."

Awesome dev studios
"Our services are 100% privacy friendly."

10

Patreon and crowdfunding for ethical apps

verified

Soul food

Mental health app for kids

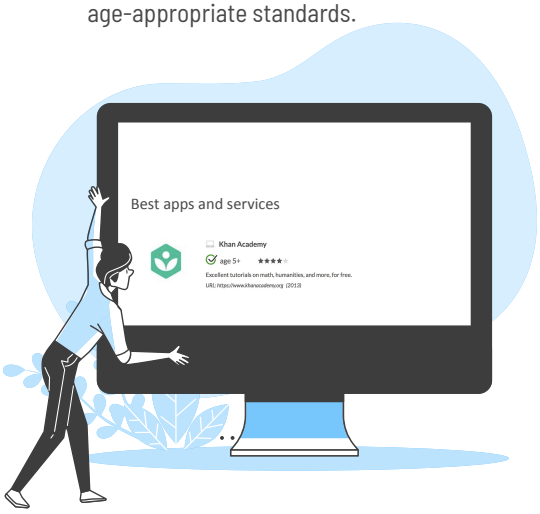
$1324 / $10000 received

Ethical marketplace where parents and children can financially support creators which uphold ethical standards.

12

Badge of Honour

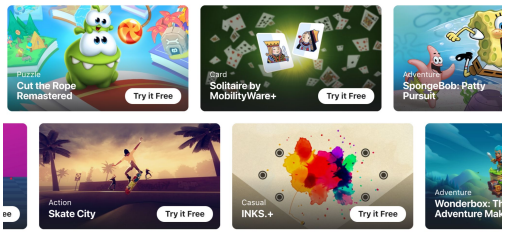
Receive a Badge of Honour if your app upholds certain age-appropriate standards.

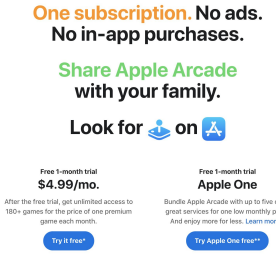


13

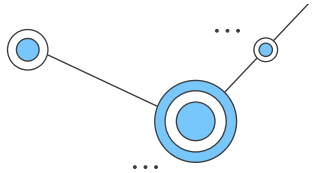
Unlimited Arcade

Upload your app to a Netflix/Spotify type platform, where users pay a monthly subscription, in return for no ads and no personal data collection/sharing.

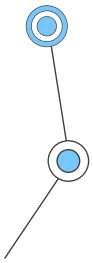




Overview



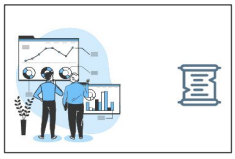
1. Do's and Don'ts checklist
2. Courses: Make it Official
3. Requirements Matrix
4. Plug-and-play self-control tools (parental and kids)
5. Machine over mind: automated data protection and child-friendliness compliance analysis
6. Wisdom of the crowds: Volunteer network for reviewing and participatory design
7. Universal compliance service: one form to rule them all.
8. Parental assistance: generate guidelines for parents
9. Public pledges and awards
10. Patreon and crowdfunding for ethical apps
11. Badge of honour: Badge for ethical apps.
12. Unlimited Arcade: Netflix/Spotify type marketplace.



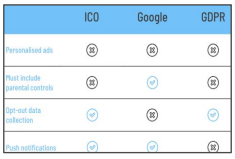
Do's and Don'ts: self-checking principles



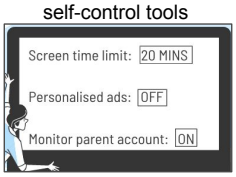
Official training courses: self-learning & cert



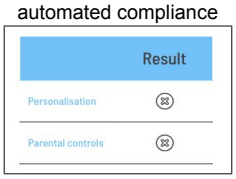
Requirements Matrix: legal compliance



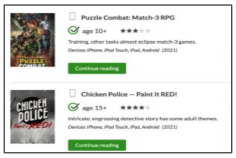
Plug-and-play self-control tools



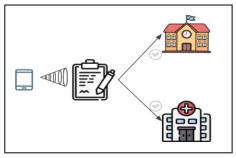
Machine over mind: automated compliance



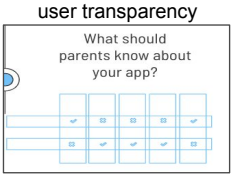
Wisdom of the crowds: user compliance support



Universal compliance service



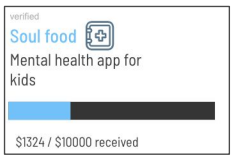
Parental assistance: user transparency



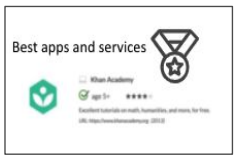
Public pledges & awards



Crowdfunding: alternative funding



Badge of honour: reputation recognition



Unlimited Arcade: alternative marketplace



B.3 Interview Codes and Themes

Table B.1: Codes Organised by Themes

Theme	Code
Perceptions of Guideline Support	Unaware of best practices
Requirements for Development Libraries	Adoption of standardized libraries
	Age appropriateness
	Alignment between marketplaces and regulation
	App monopolies
	Challenges: Apps don't earn a lot of money
	Challenges: Bribing certificates
	Challenges: Change comes from big players
	Challenges: Companies will follow the path of least resistance
	Challenges: Competition is unethical
	Challenges: Competitive marketplace
	Challenges: Complex marketplace practices
	Challenges: Don't replicate libraries
	Challenges: Ethical business models
	Challenges: Guidelines are complex
	Challenges: International market, different regulations
	Challenges: Small companies lack expertise
	Challenges: Small companies vs big companies
	Challenges: Trade-off ethics and monetization
	Challenges: Who decides what is ethical?
Concerns for Compliance Checking	Compliance is a cost
	Compliance is not a priority
	Compliance is penalized
	Compliance regulation can deter people
	Concerns for Compliance Checking: Compliance is a cost

Continued on next page

Table continued from previous page

Theme	Code
	Concerns for Compliance Checking: Compliance is not a priority Concerns for Compliance Checking: Compliance is penalized Concerns for Compliance Checking: Compliance regulation can deter people Concerns for Compliance Checking: Constantly changing regulations Concerns for Compliance Checking: Different types of apps have different requirements Development practices: Choice of third-party audit based on reputation not knowledge Development practices: Use of third party libraries Development practices: Use third-party audit companies Development practices: No third-party tracking Development practices: No use or need for data collection Development practices: No data sharing practices Development practices: In-house security standards Development practices: GDPR triggered more rigorous internal practice Development practices: Developer doesn't need data Development practices: Audit own apps Development practices: Audit external providers to ensure no PI collection Development practices: App does not collect data Development practices: App collects anonymized data
Suggestions for Alternative Funding Mechanisms	Suggestions for Alternative Funding Mechanisms: Crowdfunding Suggestions for Alternative Funding Mechanisms: Decentralize power Suggestions for Alternative Funding Mechanisms: Deferring responsibility

Continued on next page

Table continued from previous page

Theme	Code
	Suggestions for Alternative Funding Mechanisms: Ethics certification
	Suggestions for Alternative Funding Mechanisms: Examples of good and bad practices
	Suggestions for Alternative Funding Mechanisms: Expert feedback
	Suggestions for Alternative Funding Mechanisms: Explanation behind the rules
	Suggestions for Alternative Funding Mechanisms: Exposure of best practices
	Suggestions for Alternative Funding Mechanisms: Exposure to users
	Suggestions for Alternative Funding Mechanisms: Feedback from target audience
	Suggestions for Alternative Funding Mechanisms: Free materials
	Suggestions for Alternative Funding Mechanisms: Giving something back to parents
	Suggestions for Alternative Funding Mechanisms: Guidelines before development starts
	Suggestions for Alternative Funding Mechanisms: Helping parents understand
	Suggestions for Alternative Funding Mechanisms: Implementation details of best practices
	Suggestions for Alternative Funding Mechanisms: Libraries to speed up development
	Suggestions for Alternative Funding Mechanisms: Marketing and business
	Suggestions for Alternative Funding Mechanisms: Negotiation power
	Suggestions for Alternative Funding Mechanisms: New measures of success
	Suggestions for Alternative Funding Mechanisms: Outsourcing compliance

Continued on next page

Table continued from previous page

Theme	Code
	Suggestions for Alternative Funding Mechanisms: Quick and fast Suggestions for Alternative Funding Mechanisms: Quiz type compliance checking Suggestions for Alternative Funding Mechanisms: Rewarding ethical design Suggestions for Alternative Funding Mechanisms: Simple explanation for parents Suggestions for Alternative Funding Mechanisms: Standardized libraries Suggestions for Alternative Funding Mechanisms: Unlimited Arcade Suggestions for Alternative Funding Mechanisms: Video/visual content over reading
Challenges for Recognition of Best Practices	Challenges: Parents don't want to pay for ethical apps Challenges: Reliance on marketplace Challenges: Ethical development Challenges: Legislation makes people leave the kids industry Challenges: Compliance is a cost Challenges: Compliance is not a priority Challenges: Compliance is penalized Challenges: Compliance regulation can deter people Challenges: Constantly changing regulations Challenges: Different types of apps have different requirements Challenges: International market, different regulations Challenges: Trade-off ethics and monetization Challenges: Who decides what is ethical? Courses: Practical knowledge is important Development practices: Acting as an expert/consultant

Continued on next page

Table continued from previous page

Theme	Code
	Development practices: Common sense Development practices: Data compliance experts separate Development practices: Market research Development practices: Need for analytics Perceptions: Create public awareness of ethical apps Perceptions: Crowdfunding is difficult Perceptions: Developers are responsible Perceptions: Distrust of technology Perceptions: Don't replicate libraries Perceptions: Ethical apps give peace of mind Perceptions: Parents are a bad judge Perceptions: Parents want a safe environment for their kids Perceptions: Parents won't give feedback Perceptions: Parents won't go out of their way to read guidance Perceptions: Perceptions of risks for children Values: Better experience and less addiction Values: Children shouldn't spend on apps Values: Educational app Values: High-quality content more important than gaming techniques Values: Moral obligation Values: Respect children's privacy Values: Targeted ads are bad Values: Users' needs are paramount

C

Supplementary Material Chapter 6

C.1 Interview Guide

Below are the questions we used for our semi-structured interviews in Chapter 6. We started each interview with a brief description of our research questions and objectives. Prior to the interviews, participants would have already received an information sheet and consent form. Participants would able to verbally give consent to the interviews prior to starting.

This interview largely consisted of three parts. Firstly, we asked several general questions about privacy and app development. During this stage, we also shared screenshots from Chapter 3 showing privacy features in apps.

1. Could you tell a bit about yourself? And what experiences have you had with app development?

2. Have you made use of third-party libraries in your development, such as Google Analytics, Firebase, Adjust, Swrve, etc?

3. What made you decide to use these libraries, and how did you pick them?

4. Have you thought about privacy considerations of these libraries, or this something that often is not a primary concern/consideration during development?

5. Do you think that these libraries may collect more information than is needed to fulfil their functionality? Why is this the case and do you think this is problematic? What about specifically for apps aimed at vulnerable user populations?

6. Do you find that third party libraries are transparent in their data collection and sharing practices?

7. How do you generally request consent in apps and what are your experiences with this?

8. Do you feel that end users (and children specifically) are sufficiently empowered to exercise their privacy rights in apps?

9. Why do you think that this is a commonly overlooked area in app development?

10. How do you think it can be improved?

In the second step, we performed a cognitive walkthrough, allowing the participants to browse to `DataAvalanche.io` and share their screen. We then guided them through the tool and asked questions to elicit their impressions.

1. I'll give you a chance to just look at it and play around with it a bit.

2. What do you think this tool is used for?

3. We can select one tracker as an example: Unity Ads.

   (a) (Have you worked with this library before?)

4. What kind of privacy and data sharing practices do you expect from this library?

5. Feel free to browse through the tool.

6. Looking at the map, what are your first impressions? Do you feel that there might be privacy concerns?

7. How would you like to have these concerns addressed?
    (a) For example, more clarity on how to inform end users?
    (b) How to properly configure this in the app to secure privacy?
    (c) Communication in privacy policy?
    (d) Alternatives?
    (e) Or not at all?
8. How do you think developers who have the best interest of end users in mind, would use this tool?

Finally, we asked them whether they had further requirements and needs which they would like to see implemented in the tool.

1. Going section by section, what do you think can be improved?
2. Which critical features are missing from this?
3. Which features seem redundant?
4. What crazy feature, that may even be impossible to implement, would you like to see in this tool?

C.2 Interview Codes and Themes

Table C.1: Codes Organised by Themes

Theme	**Codes**
Alternatives are Good but Not Always Applicable	Discovery of SDKs is useful Visual elements are good Choosing libraries
Privacy Implications are Useful for Transparency	Privacy and children

Continued on next page

Table continued from previous page

Theme	Codes
	Need for Transparency Data collection practices Legal implications are useful
Data Tracking is Not Surprising	Perceptions of data Tracking Improvements in KG
Putting the Tool to Use	Collation of data in place Need for monetisation Tool is easy to use and access Demand for privacy makes this tool necessary Privacy management
Additional Requirements	Additional Requirements Ads Categorize SDKs Sort by popularity Embed documentation Tutorials Privacy breaches App upload SDK comparisons Mark favorites and bookmarks More data sharing details Who is benefiting from the data Filter SDKs by countries Trending Summary privacy policy Community contributions Add user data to map Ratings

Bibliography

[1] F. Haugen, "Statement of frances haugen," *United States Senate Committee on Commerce, Science and Transportation*, 2021.

[2] G. Britain, *Children and parents: Media use and attitudes report 2022*. Ofcom, 2022.

[3] "Apple arcade." `https://www.apple.com/apple-arcade/`.

[4] G. Play, "Expert approved apps," 2022. `https://play.google.com/intl/en-GB_ALL/console/about/programs/teacherapproved`.

[5]

[6] "Transcript of mark zuckerberg's senate hearing," Dec 2021. `https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/`.

[7] R. Binns, U. Lyngs, M. Van Kleek, J. Zhao, T. Libert, and N. Shadbolt, "Third party tracking in the mobile ecosystem," in *Proceedings of the 10th ACM Conference on Web Science*, pp. 23–31, ACM, 2018.

[8] T. Book, A. Pridgen, and D. S. Wallach, "Longitudinal analysis of android ad library permissions," *arXiv preprint arXiv:1303.0857*, 2013.

[9] J. Lin, "Understanding and capturing people's mobile app privacy preferences," tech. rep., CARNEGIE-MELLON UNIV PITTSBURGH PA SCHOOL OF COMPUTER SCIENCE, 2013.

[10] A. H. Mhaidli, Y. Zou, and F. Schaub, "" we can't live without them!" app developers' adoption of ad networks and their considerations of consumer risks," in *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[11] D. Lupton and B. Williamson, "The datafied child: The dataveillance of children and implications for their rights," *New Media & Society*, vol. 19, no. 5, pp. 780–794, 2017.

[12] N. Kobie, "Surveillance state: Fingerprinting pupils raises safety and privacy concerns," *The Guardian*, 2016.

[13] S. Livingstone, M. Stoilova, and R. Nandagiri, "Children's data and privacy online: growing up in a digital age: an evidence review," 2019.

[14] V. Rideout, "The common sense census: Media use by kids age zero to eight," *San Francisco, CA: Common Sense Media*, pp. 263–283, 2017.

[15] S. Livingstone, J. Davidson, J. Bryce, S. Batool, C. Haughton, and A. Nandi, "Children's online activities, risks and safety: a literature review by the ukccis evidence group," 2017.

[16] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[17] "Age appropriate design: a code of practice for online services," Sep 2020. `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`.

[18] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill, "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," 2018.

[19] K. Kollnig, P. Dewitte, M. V. Kleek, G. Wang, D. Omeiza, H. Webb, and N. Shadbolt, "A fait accompli? an empirical study into the absence of consent to third-party tracking in android apps,"

[20] L. Parker, V. Halter, T. Karliychuk, and Q. Grundy, "How private is your mental health app data? an empirical study of mental health app privacy policies and practices," *International Journal of Law and Psychiatry*, vol. 64, 2019.

[21] K. C. Chang, R. N. Zaeem, and K. S. Barber, "A framework for estimating privacy risk scores of mobile apps," vol. 12472 LNCS, 2020.

[22] F. L. Broekman, J. T. Piotrowski, H. W. Beentjes, and P. M. Valkenburg, "A parental perspective on apps for young children," *Computers in Human Behavior*, vol. 63, pp. 142–151, 2016.

[23] J. Zhao, U. Lyngs, and N. Shadbolt, "What privacy concerns do parents have about children's mobile apps, and how can they stay sharp?," *arXiv preprint arXiv:1809.10841*, 2018.

[24] M. Tahaei, A. Frik, and K. Vaniea, "Privacy champions in software teams: Understanding their motivations, strategies, and challenges," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, 2021.

[25] K. Bednar, S. Spiekermann, and M. Langheinrich, "Engineering privacy by design: Are engineers ready to live up to the challenge?," *The Information Society*, vol. 35, no. 3, pp. 122–142, 2019.

[26] N. Alomar and S. Egelman, "Developers say the darnedest things: Privacy compliance processes followed by developers of child-directed apps," *Proceedings on Privacy Enhancing Technologies*, vol. 4, p. 2022, 2022.

[27] R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. Cranor, "The privacy and security behaviors of smartphone app developers," 2014.

[28] M. Tahaei and K. Vaniea, ""developers are responsible": What ad networks tell developers about privacy," in *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–11, 2021.

[29] I. Hadar, T. Hasson, O. Ayalon, E. Toch, M. Birnhack, S. Sherman, and A. Balissa, "Privacy by designers: software developers' privacy mindset," *Empirical Software Engineering*, vol. 23, no. 1, pp. 259–289, 2018.

[30] S. Zimmeck, R. Goldstein, and D. Baraka, "Privacyflash pro: Automating privacy policy generation for mobile apps.," in *NDSS*, 2021.

[31] T. Li, E. B. Neundorfer, Y. Agarwal, and J. I. Hong, "Honeysuckle: Annotation-guided code generation of in-app privacy notices," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 5, no. 3, 2021.

[32] T. Li, Y. Agarwal, and J. I. Hong, "Coconut: An ide plugin for developing privacy-friendly apps," *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 2, no. 4, pp. 1–35, 2018.

[33] A. Kononova, W. Kim, E. Joo, and K. Lynch, "Click, click, ad: the proportion of relevant (vs. irrelevant) ads matters when advertising within paginated online content," *International Journal of Advertising*, vol. 39, no. 7, pp. 1031–1058, 2020.

[34] I. Leontiadis, C. Efstratiou, M. Picone, and C. Mascolo, "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*, p. 2, ACM, 2012.

[35] A. Acquisti, C. Taylor, and L. Wagman, "The economics of privacy," *Journal of Economic Literature*, vol. 54, no. 2, pp. 442–92, 2016.

[36] I. A. Bureau, "Iab internet advertising revenue report: 2015 full year results," 2015.

[37] I. Jorstad, D. Van Thanh, and S. Dustdar, "The personalization of mobile services," in *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005.*, vol. 4, pp. 59–65, IEEE, 2005.

[38] S. Livingstone, A. Blum-Ross, and D. Zhang, "What do parents think, and do, about their children's online privacy?," 2018.

[39] L. Pangrazio and N. Selwyn, "'my data, my bad...' young people's personal data understandings and (counter) practices," in *Proceedings of the 8th International Conference on Social Media & Society*, pp. 1–5, 2017.

[40] R. S. Barbour, "Checklists for improving rigour in qualitative research: a case of the tail wagging the dog?," *Bmj*, vol. 322, no. 7294, pp. 1115–1117, 2001.

[41] P. J. Stappers and E. Giaccardi, "Research through design," in *The encyclopedia of human-computer interaction*, pp. 1–94, The Interaction Design Foundation, 2017.

[42] ICO, "Age appropriate design: a code of practice for online services," 2021. `https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/`.

[43] Ofcom., "Children and parents: Media use and attitudes," 2018.

[44] G. Britain, *Children and parents: Media use and attitudes report*. Ofcom, 2013.

[45] H. K. Kabali, M. M. Irigoyen, R. Nunez-Davis, J. G. Budacki, S. H. Mohanty, K. P. Leister, and R. L. Bonner, "Exposure and use of mobile media devices by young children," *Pediatrics*, vol. 136, no. 6, pp. 1044–1050, 2015.

[46] Childwise, "The monitor preschool report.," 2017.

[47] P. McDonough, "Tv viewing among kids at an eight-year high," *The Nielsen Company*, vol. 26, 2009.

[48] C. S. Media, "Zero to eight: Children's media use in america 2013," 2013.

[49] A. Hiniker, H. Suh, S. Cao, and J. A. Kientz, "Screen time tantrums: how families manage screen media experiences for toddlers and preschoolers," in *Proceedings of the 2016 CHI conference on human factors in computing systems*, pp. 648–660, 2016.

[50] V. Rideout, "Learning at home: Families' educational media use in america.," in *Joan Ganz Cooney Center at Sesame Workshop*, ERIC, 2014.

[51] B. Auxier, M. Anderson, A. Perrin, and E. Turner, "Children's engagement with digital devices, screen time," 2020.

[52] B. Sari, Z. K. Takacs, and A. G. Bus, "What are we downloading for our children? best-selling children's apps in four european countries," *Journal of Early Childhood Literacy*, vol. 19, no. 4, pp. 515–532, 2019.

[53] S.-H. Jeong, H. Kim, J.-Y. Yum, and Y. Hwang, "What type of content are smartphone users addicted to?: Sns vs. games," *Computers in human behavior*, vol. 54, pp. 10–17, 2016.

[54] `https://play.google.com/about/play-pass/`.

[55] H. K. Rono, A. Bastawrous, D. Macleod, E. Wanjala, G. L. Di Tanna, H. A. Weiss, and M. J. Burton, "Smartphone-based screening for visual impairment in kenyan school children: a cluster randomised controlled trial," *The Lancet Global Health*, vol. 6, no. 8, pp. e924–e932, 2018.

[56] H. Henriksson, C. Alexandrou, P. Henriksson, M. Henström, M. Bendtsen, K. Thomas, U. Müssener, P. Nilsen, and M. Löf, "Ministop 2.0: a smartphone app integrated in primary child health care to promote healthy diet and physical activity behaviours and prevent obesity in preschool-aged children: protocol for a hybrid design effectiveness-implementation study," *BMC Public Health*, vol. 20, no. 1, pp. 1–11, 2020.

[57] L. Duan, X. Shao, Y. Wang, Y. Huang, J. Miao, X. Yang, and G. Zhu, "An investigation of mental health status of children and adolescents in china during the outbreak of covid-19," *Journal of affective disorders*, vol. 275, pp. 112–118, 2020.

[58] S. Fletcher-Watson, H. Pain, S. Hammond, A. Humphry, and H. McConachie, "Designing for young children with autism spectrum disorder: A case study of an ipad app," *International Journal of Child-Computer Interaction*, vol. 7, pp. 1–14, 2016.

[59] P. Leijdekkers, V. Gay, and F. Wong, "Capturemyemotion: A mobile app to improve emotion learning for autistic children using sensors," in *Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems*, pp. 381–384, IEEE, 2013.

[60] S. Schuck, N. Emmerson, H. Ziv, P. Collins, S. Arastoo, M. Warschauer, F. Crinella, and K. Lakes, "Designing an ipad app to monitor and im-

prove classroom behavior for children with adhd: iselfcontrol feasibility and pilot studies," *PloS one*, vol. 11, no. 10, p. e0164229, 2016.

[61] N. Kucirkova, D. Messer, V. Critten, and J. Harwood, "Story-making on the ipad when children have complex needs: Two case studies," *Communication Disorders Quarterly*, vol. 36, no. 1, pp. 44–54, 2014.

[62] R. A. Dore, M. Shirilla, E. Hopkins, M. Collins, M. Scott, J. Schatz, J. Lawson-Adams, T. Valladares, L. Foster, H. Puttre, *et al.*, "Education in the app store: using a mobile game to support us preschoolers' vocabulary learning," *Journal of Children and Media*, vol. 13, no. 4, pp. 452–471, 2019.

[63] K. Clayton and A. Murphy, "Smartphone apps in education: Students create videos to teach smartphone use as tool for learning.," *Journal of Media Literacy Education*, vol. 8, no. 2, pp. 99–109, 2016.

[64] S. Papadakis, "Apps to promote computational thinking concepts and coding skills in children of preschool and pre-primary school age," in *Mobile Learning Applications in Early Childhood Education*, pp. 101–121, IGI Global, 2020.

[65] J. D. Elhai, R. D. Dvorak, J. C. Levine, and B. J. Hall, "Problematic smartphone use: A conceptual overview and systematic review of relations with anxiety and depression psychopathology," *Journal of affective disorders*, vol. 207, pp. 251–259, 2017.

[66] H. Lee, M. J. Seo, and T. Y. Choi, "The effect of home-based daily journal writing in korean adolescents with smartphone addiction," *Journal of Korean medical science*, vol. 31, no. 5, pp. 764–769, 2016.

[67] B. Kidron, A. Evans, J. Afia, J. R. Adler, H. Bowden-Jones, L. Hackett, A. Juj, A. K. Przybylski, A. Rudkin, and Y. Scot, "Disrupted childhood: the cost of persuasive design," 2018.

[68] E. E. Rasmussen, A. Shafer, M. J. Colwell, S. White, N. Punyanunt-Carter, R. L. Densley, and H. Wright, "Relation between active mediation, exposure to daniel tiger's neighborhood, and us preschoolers' social and emotional development," *Journal of Children and Media*, vol. 10, no. 4, pp. 443–461, 2016.

[69] S. M. Fisch, R. T. Truglio, and C. F. Cole, "The impact of sesame street on preschool children: A review and synthesis of 30 years' research," *Media Psychology*, vol. 1, no. 2, pp. 165–190, 1999.

[70] G. Salomon, "Effects of encouraging israeli mothers to co-observe" sesame street" with their five-year-olds," *Child Development*, pp. 1146–1151, 1977.

[71] Y. L. R. Chassiakos, J. Radesky, D. Christakis, M. A. Moreno, C. Cross, *et al.*, "Children and adolescents and digital media," *Pediatrics*, vol. 138, no. 5, p. e20162593, 2016.

[72] D. A. Gentile, S. Coyne, and D. A. Walsh, "Media violence, physical aggression, and relational aggression in school age children: a short-term longitudinal study," *Aggressive behavior*, vol. 37, no. 2, pp. 193–206, 2011.

[73] B. J. Wilson, "Media and children's aggression, fear, and altruism," *The future of children*, pp. 87–118, 2008.

[74] D. A. Christakis, F. J. Zimmerman, D. L. DiGiuseppe, and C. A. McCarty, "Early television exposure and subsequent attentional problems in children," *Pediatrics*, vol. 113, no. 4, pp. 708–713, 2004.

[75] F. J. Zimmerman and D. A. Christakis, "Associations between content types of early media exposure and subsequent attentional problems," *Pediatrics*, vol. 120, no. 5, pp. 986–992, 2007.

[76] R. Jago, T. Baranowski, J. C. Baranowski, D. Thompson, and K. Greaves, "Bmi from 3–6 y of age is predicted by tv viewing and physical activity, not diet," *International journal of obesity*, vol. 29, no. 6, pp. 557–564, 2005.

[77] M. M. Garrison, K. Liekweg, and D. A. Christakis, "Media use and child sleep: the impact of content, timing, and environment," *Pediatrics*, vol. 128, no. 1, pp. 29–35, 2011.

[78] A. Sigman, "Time for a view on screen time," *Archives of disease in childhood*, vol. 97, no. 11, pp. 935–942, 2012.

[79] M. Guha, "Handbook of child psychology and developmental science," *Reference Reviews*, 2016.

[80] J. Falbe, K. K. Davison, R. L. Franckle, C. Ganter, S. L. Gortmaker, L. Smith, T. Land, and E. M. Taveras, "Sleep duration, restfulness, and screens in the sleep environment," *Pediatrics*, vol. 135, no. 2, pp. e367–e375, 2015.

[81] D. J. Solove, "Understanding privacy," 2008.

[82] S. Warren and L. Brandeis, "The right to privacy," in *Killing the Messenger*, pp. 1–21, Columbia University Press, 1989.

[83] A. E. Waldman, "Privacy as trust: Sharing personal information in a networked world," *U. Miami L. Rev.*, vol. 69, p. 559, 2014.

[84] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[85] J. King, "Taken out of context: An empirical analysis of westin's privacy scale," in *Workshop on Privacy Personas and Segmentation*, p. 2014, 2014.

[86] I. Altman, "A conceptual analysis," *Environment and behavior*, vol. 8, no. 1, pp. 7–29, 1976.

[87] I. Altman, "The environment and social behavior: privacy, personal space, territory, and crowding.," 1975.

[88] S. T. Margulis, "Three theories of privacy: An overview," *Privacy online*, pp. 9–17, 2011.

[89] S. Van der Hof, "I agree, or do i: a rights-based analysis of the law on children's consent in the digital world," *Wis. Int'l LJ*, vol. 34, p. 409, 2016.

[90] "What is gdpr, the eu's new data protection law?," May 2022. `https://gdpr.eu/what-is-gdpr/`.

[91] "Unicef industry toolkits." `https://www.unicef.org/csr/ict_tools.html`.

[92] C. Nyst, A. Gorostiaga, and P. Geary, "Children's online privacy & freedom of expression: Industry toolkit," 2018. https://www.unicef.org/csr/ict_tools.html.

[93] "Complying with coppa: Frequently asked questions," Jul 2020. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0.

[94] "Designing apps for children and families - play console help." https://support.google.com/googleplay/android-developer/answer/9893335?hl=en.

[95] "Families ads program." https://support.google.com/googleplay/android-developer/answer/9900633.

[96] A. Inc., "App store review guidelines." https://developer.apple.com/app-store/review/guidelines/.

[97] "Letter to the ico: Systemic breaches of the age appropriate design code," Nov 2022. https://5rightsfoundation.com/in-action/letter-to-the-ico-breaches-of-the-age-appropriate-design-code.html.

[98] J. Peter and P. M. Valkenburg, "Adolescents' online privacy: Toward a developmental perspective," in *Privacy online*, pp. 221–234, Springer, 2011.

[99] K. Raynes-Goldie and M. Allen, "Gaming privacy: a canadian case study of a children's co-created privacy literacy game," *Surveillance & Society*, vol. 12, no. 3, pp. 414–426, 2014.

[100] P. Pradeep and S. Sriram, "The virtual world of social networking sites: Adolescent's use and experiences," *Psychology and Developing Societies*, vol. 28, no. 1, pp. 139–159, 2016.

[101] C. Balleys and S. Coll, "Being publicly intimate: Teenagers managing online privacy," *Media, Culture & Society*, vol. 39, no. 6, pp. 885–901, 2017.

[102] W. Shin, J. Huh, and R. J. Faber, "Tweens' online privacy risks and the role of parental mediation," *Journal of Broadcasting & Electronic Media*, vol. 56, no. 4, pp. 632–649, 2012.

[103] P. Kumar, S. M. Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. 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*, vol. 1, no. CSCW, p. 64, 2017.

[104] S. Chaudron, R. Di Gioia, and M. Gemo, "Young children (0-8) and digital technology, a qualitative study across europe," *JRC Science for Policy Report*, 2018.

[105] P. Kumar, J. Vitak, M. Chetty, T. L. Clegg, J. Yang, B. McNally, and E. Bonsignore, "Co-designing online privacy-related games and stories with children," in *Proceedings of the 17th ACM Conference on Interaction Design and Children*, pp. 67–79, ACM, 2018.

[106] C. S. Silva, G. A. Barbosa, I. S. Silva, T. S. Silva, F. Mourão, and F. Coutinho, "Privacy for children and teenagers on social networks from a usability perspective: a case study on facebook," in *Proceedings of the 2017 ACM on Web Science Conference*, pp. 63–71, 2017.

[107] L. Zhang-Kennedy, C. Mekhail, Y. Abdelaziz, and S. Chiasson, "From nosy little brothers to stranger-danger: Children and parents' perception of mobile threats," in *Proceedings of the The 15th International Conference on Interaction Design and Children*, pp. 388–399, 2016.

[108] H. Jia, P. J. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, "Risk-taking as a learning process for shaping teen's online information privacy behaviors," in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, pp. 583–599, ACM, 2015.

[109] S. Jones, C. Johnson-Yale, S. Millermaier, and F. S. Pérez, "Us college students' internet use: Race, gender and digital divides," *Journal of Computer-Mediated Communication*, vol. 14, no. 2, pp. 244–264, 2009.

[110] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science*, vol. 4, no. 3, pp. 340–347, 2013.

[111] S. Barth and M. D. De Jong, "The privacy paradox–investigating discrepancies between expressed privacy concerns and actual online

behavior–a systematic literature review," *Telematics and informatics*, vol. 34, no. 7, pp. 1038–1058, 2017.

[112] S. Livingstone, K. Ólafsson, and G. Maier, "If children don't know an ad from information, how can they grasp how companies use their personal data," *Media Policy Project*, 2018.

[113] S. Chaudron, M. Beutel, V. Donoso Navarrete, M. Dreier, B. Fletcher-Watson, A. Heikkilä, V. Kontríková, R. Korkeamäki, S. Livingstone, J. Marsh, *et al.*, *Young Children (0-8) and digital technology: A qualitative exploratory study across seven countries*. JRC; ISPRA, Italy, 2015.

[114] J. Zhao, G. Wang, C. Dally, P. Slovak, J. Edbrooke-Childs, M. Van Kleek, and N. 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*, p. 106, ACM, 2019.

[115] G. H. Lapenta and R. F. Jørgensen, "Youth, privacy and online media: Framing the right to privacy in public policy-making," *First Monday*, 2015.

[116] L. Emanuel and D. Stanton Fraser, "Exploring physical and digital identity with a teenage cohort," in *Proceedings of the 2014 conference on Interaction design and children*, pp. 67–76, 2014.

[117] A. Acker and L. Bowler, "Youth data literacy: teen perspectives on data created with social media and mobile devices," 2018.

[118] L. Bowler, A. Acker, W. Jeng, and Y. Chi, ""it lives all around us": Aspects of data literacy in teen's lives," *Proceedings of the Association for Information Science and Technology*, vol. 54, no. 1, pp. 27–35, 2017.

[119] M. Murumaa-Mengel, "Drawing the threat: a study on perceptions of the online pervert among estonian high school students," *Young*, vol. 23, no. 1, pp. 1–18, 2015.

[120] L. Pangrazio and N. Selwyn, ""it's not like it's life or death or whatever": Young people's understandings of social media data," *Social Media+ Society*, vol. 4, no. 3, p. 2056305118787808, 2018.

[121] R. S. Best, "Growing up with the internet: 2nd report of session 2016–17," 2017.

[122] V. J. Rideout and E. Hamel, *The media family: Electronic media in the lives of infants, toddlers, preschoolers and their parents*. Henry J. Kaiser Family Foundation, 2006.

[123] J. C. Wright, A. C. Huston, E. A. Vandewater, D. S. Bickham, R. M. Scantlin, J. A. Kotler, A. G. Caplovitz, J. H. Lee, S. Hofferth, and J. Finkelstein, "American children's use of electronic media in 1997: A national survey," *Journal of Applied Developmental Psychology*, vol. 22, no. 1, pp. 31–47, 2001.

[124] S. Livingstone, K. Ólafsson, E. J. Helsper, F. Lupiáñez-Villanueva, G. A. Veltri, and F. Folkvord, "Maximizing opportunities and minimizing risks for children online: The role of digital skills in emerging strategies of parental mediation," *Journal of Communication*, vol. 67, no. 1, pp. 82–105, 2017.

[125] S. Livingstone, G. Mascheroni, and E. Staksrud, "European research on children's internet use: Assessing the past and anticipating the future," *New Media & Society*, vol. 20, no. 3, pp. 1103–1122, 2018.

[126] N. Kucirkova and M. Sakr, "Child–father creative text-making at home with crayons, ipad collage & pc," *Thinking Skills and Creativity*, vol. 17, pp. 59–73, 2015.

[127] E. W. Austin, "Exploring the effects of active parental mediation of television content," *Journal of Broadcasting & Electronic Media*, vol. 37, no. 2, pp. 147–158, 1993.

[128] L. M. Padilla-Walker and S. M. Coyne, ""turn that thing off!" parent and adolescent predictors of proactive media monitoring," *Journal of adolescence*, vol. 34, no. 4, pp. 705–715, 2011.

[129] M. St. Peters, M. Fitch, A. C. Huston, J. C. Wright, and D. J. Eakins, "Television and families: What do young children watch with their parents?," *Child development*, vol. 62, no. 6, pp. 1409–1423, 1991.

[130] L. Plowman, J. McPake, and C. Stephen, "Just picking it up? young children learning with technology at home," *Cambridge Journal of Education*, vol. 38, no. 3, pp. 303–319, 2008.

[131] D. Holloway and L. Green, "The internet of toys," *Communication Research and Practice*, vol. 2, no. 4, pp. 506–519, 2016.

[132] G. Roberts-Holmes, "Playful and creative ict pedagogical framing: a nursery school case study," *Early Child Development and Care*, vol. 184, no. 1, pp. 1–14, 2014.

[133] S. Price, C. Jewitt, and L. Crescenzi, "The role of ipads in preschool children's mark making development," *Computers & Education*, vol. 87, pp. 131–141, 2015.

[134] N. Darling and L. Steinberg, "Parenting style as context: An integrative model.," *Psychological bulletin*, vol. 113, no. 3, p. 487, 1993.

[135] M. S. Eastin, B. S. Greenberg, and L. Hofschire, "Parenting the internet," *Journal of communication*, vol. 56, no. 3, pp. 486–504, 2006.

[136] L. D. Rosen, N. A. Cheever, and L. M. Carrier, "The association of parenting style and child age with parental limit setting and adolescent myspace behavior," *Journal of Applied Developmental Psychology*, vol. 29, no. 6, pp. 459–471, 2008.

[137] G. Kirkham, "Chaudron, s., di gioia, r., gemo, m.(2018). young children (0-8) and digital technology. a qualitative study across europe. eur 29070. publication office of the european union.," *Pedagogika*, vol. 68, no. 3, 2018.

[138] T. S. Castro, M. C. M. d. Ponte, A. M. F. R. Jorge, and S. Batista, "Crescendo entre ecrãs," *Literacia, Media e Cidadania*, pp. 144–157, 2017.

[139] P. Nikken and J. Jansz, "Developing scales to measure parental mediation of young children's internet use," *Learning, Media and technology*, vol. 39, no. 2, pp. 250–266, 2014.

[140] M. Valcke, S. Bonte, B. De Wever, and I. Rots, "Internet parenting styles and the impact on internet use of primary school children," *Computers & Education*, vol. 55, no. 2, pp. 454–464, 2010.

[141] K. C. Montgomery, "Youth and surveillance in the facebook era: Policy interventions and social implications," *Telecommunications Policy*, vol. 39, no. 9, pp. 771–786, 2015.

[142] K. C. Montgomery, J. Chester, and T. Milosevic, "Children's privacy in the big data era: Research opportunities," *Pediatrics*, vol. 140, no. Supplement 2, pp. S117–S121, 2017.

[143] R. Binns *et al.*, "Tracking on the web, mobile and the internet of things," *Foundations and Trends® in Web Science*, vol. 8, no. 1–2, pp. 1–113, 2022.

[144] J. Bailey, "A perfect storm: How the online environment, social norms and law shape girls' lives," 2015.

[145] W. Shin and H. Kang, "Adolescents' privacy concerns and information disclosure online: The role of parents and the internet," *Computers in Human Behavior*, vol. 54, pp. 114–123, 2016.

[146] A. Micheti, J. Burkell, and V. Steeves, "Fixing broken doors: Strategies for drafting privacy policies young people can understand," *Bulletin of Science, Technology & Society*, vol. 30, no. 2, pp. 130–143, 2010.

[147] "Tracking compliance and scope." `https://www.w3.org/TR/tracking-compliance/`.

[148] J. Schwartz, "Giving the web a memory cost its users privacy," *New York Times*, vol. 4, no. 01, 2001.

[149] "ios." `https://www.apple.com/ios`.

[150] "Android operating system." `https://www.android.com/`.

[151] "Application fundamentals nbsp;: nbsp; android developers." `https://developer.android.com/guide/components/fundamentals`.

[152] "Android permissions overview." `https://developer.android.com/guide/topics/permissions/overview`.

[153] C. Spensky, J. Stewart, A. Yerukhimovich, R. Shay, A. Trachtenberg, R. Housley, and R. K. Cunningham, "Sok: Privacy on mobile devices–it's complicated," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 3, pp. 96–116, 2016.

[154] ENISA, "Privacy and data protection in mobile applications: A study on the app development ecosystem and the technical implementation of gdpr," 2018.

[155] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman, "50 ways to leak your data: An exploration of apps' circumvention of the android permissions system," in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 603–620, 2019.

[156] S. Son, D. Kim, and V. Shmatikov, "What mobile ads know about mobile users.," in *NDSS*, 2016.

[157] M. Tahaei, R. Abu-Salma, and A. Rashid, "Stuck in the permissions with you: Developer & end-user perspectives on app permissions & their privacy ramifications," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, pp. 1–24, 2023.

[158] J. Duball, "Apple's att rollout presents uncertain path for adtech," May 2021. https://iapp.org/news/a/apples-att-rollout-presents-uncertain-path-for-adtech/.

[159] T. Rona and AppsFlyer, "Att opt-in rates are much higher than anticipated," Jun 2022. https://www.appsflyer.com/blog/trends-insights/att-opt-in-rates-higher/.

[160] "Advertising id - play console help." https://support.google.com/googleplay/android-developer/answer/6048248#zippy=%2Ctargetingdevices-without-an-advertising-id%2Cpersistent-identifiers-including-android-id.

[161] K. Kaye, "Use of limit ad tracking drops as ad blocking grows," May 2016. https://adage.com/article/privacy-and-regulation/limit-ad-tracking-drops-ad-blocking-grows/303911.

[162] S. Arzt, S. Rasthofer, C. Fritz, E. Bodden, A. Bartel, J. Klein, Y. Le Traon, D. Octeau, and P. McDaniel, "Flowdroid: Precise context, flow, field, object-sensitive and lifecycle-aware taint analysis for android apps," in *Acm Sigplan Notices*, vol. 49, pp. 259–269, ACM, 2014.

[163] L. Batyuk, M. Herpich, S. A. Camtepe, K. Raddatz, A.-D. Schmidt, and S. Albayrak, "Using static analysis for automatic assessment and mitigation of unwanted and malicious activities within android applications," in *2011 6th International Conference on Malicious and Unwanted Software*, pp. 66–72, IEEE, 2011.

[164] M. Egele, C. Kruegel, E. Kirda, and G. Vigna, "Pios: Detecting privacy leaks in ios applications.," in *NDSS*, pp. 177–183, 2011.

[165] J. Lin, B. Liu, N. Sadeh, and J. I. Hong, "Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings," in *10th Symposium On Usable Privacy and Security ({SOUPS} 2014)*, pp. 199–212, 2014.

[166] M. Christodorescu, S. Jha, S. A. Seshia, D. Song, and R. E. Bryant, "Semantics-aware malware detection," in *2005 IEEE symposium on security and privacy (S&P'05)*, pp. 32–46, IEEE, 2005.

[167] P. Faruki, A. Bharmal, V. Laxmi, M. S. Gaur, M. Conti, and M. Rajarajan, "Evaluation of android anti-malware techniques against dalvik bytecode obfuscation," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 414–421, IEEE, 2014.

[168] D. Maiorca, D. Ariu, I. Corona, M. Aresu, and G. Giacinto, "Stealth attacks: An extended insight into the obfuscation effects on android malware," *Computers & Security*, vol. 51, pp. 16–31, 2015.

[169] M. Lindorfer, M. Neugschwandtner, L. Weichselbaum, Y. Fratantonio, V. Van Der Veen, and C. Platzer, "Andrubis–1,000,000 apps later: A view on current android malware behaviors," in *2014 third international workshop on building analysis datasets and gathering experience returns for security (BADGERS)*, pp. 3–17, IEEE, 2014.

[170] W. Enck, P. Gilbert, S. Han, V. Tendulkar, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: an information-flow tracking system for realtime privacy monitoring on smartphones," *ACM Transactions on Computer Systems (TOCS)*, vol. 32, no. 2, p. 5, 2014.

[171] L. Qiu, Z. Zhang, Z. Shen, and G. Sun, "Apptrace: Dynamic trace on android devices," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7145–7150, IEEE, 2015.

[172] G. Sarwar, O. Mehani, R. Boreli, and M. A. Kaafar, "On the effectiveness of dynamic taint analysis for protecting against private information leaks on android-based devices.," in *SECRYPT*, vol. 96435, 2013.

[173] A. Le, J. Varmarken, S. Langhoff, A. Shuba, M. Gjoka, and A. Markopoulou, "Antmonitor: A system for monitoring from mobile devices," in *Proceedings of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsharing of Big (Internet) Data*, pp. 15–20, 2015.

[174] A. Rao, J. Sherry, A. Legout, A. Krishnamurthy, W. Dabbous, and D. Choffnes, "Meddle: middleboxes for increased transparency and control of mobile traffic," in *Proceedings of the 2012 ACM conference on CoNEXT student workshop*, pp. 65–66, 2012.

[175] A. Razaghpanah, N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, P. Gill, M. Allman, and V. Paxson, "Haystack: In situ mobile traffic analysis in user space," *arXiv preprint arXiv:1510.01419*, pp. 1–13, 2015.

[176] J. Zang, K. Dummit, J. Graves, P. Lisker, and L. Sweeney, "Who knows what about me? a survey of behind the scenes personal data sharing to third parties by mobile apps," *Technology Science*, vol. 30, 2015.

[177] B. Krupp, J. Hadden, and M. Matthews, "An analysis of web tracking domains in mobile applications," in *13th ACM Web Science Conference 2021*, pp. 291–298, 2021.

[178] K. Kollnig, A. Shuba, R. Binns, M. Van Kleek, and N. Shadbolt, "Are iphones really better for privacy? comparative study of ios and android apps," *arXiv preprint arXiv:2109.13722*, 2021.

[179] P. International, "How apps on android share data with facebook (even if you don't have a facebook account)," 2018.

[180] M. C. Grace, W. Zhou, X. Jiang, and A.-R. Sadeghi, "Unsafe exposure analysis of mobile in-app advertisements," in *Proceedings of the*

fifth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp. 101–112, ACM, 2012.

[181] V. F. Taylor and I. Martinovic, "To update or not to update: Insights from a two-year study of android app evolution," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pp. 45–57, 2017.

[182] T. Book and D. S. Wallach, "An empirical study of mobile ad targeting," *arXiv preprint arXiv:1502.06577*, 2015.

[183] K. A. Bamberger, S. Egelman, C. Han, A. Elazari Bar On, and I. Reyes, "Can you pay for privacy? consumer expectations and the behavior of free and paid apps," *Berkeley Technology Law Journal*, vol. 35, 2020.

[184] C. Han, I. Reyes, A. Elazari Bar On, J. Reardon, Á. Feal, S. Egelman, and N. Vallina-Rodriguez, "Do you get what you pay for? comparing the privacy behaviors of free vs. paid apps," 2019.

[185] S. Seneviratne, H. Kolamunna, and A. Seneviratne, "A measurement study of tracking in paid mobile applications," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pp. 1–6, 2015.

[186] C. Han, I. Reyes, Á. Feal, J. Reardon, P. Wijesekera, N. Vallina-Rodriguez, A. Elazar, K. A. Bamberger, and S. Egelman, "The price is (not) right: Comparing privacy in free and paid apps," *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 3, 2020.

[187] J. Anderson, J. Bonneau, and F. Stajano, "Inglorious installers: Security in the application marketplace.," in *WEIS*, Citeseer, 2010.

[188] "Can google's non-advertising revenue streams mitigate impact of slowing advertising growth?," Nov 2019. `https://www.forbes.com/sites/greatspeculations/2019/11/04/can-googles-non-advertising-revenue-streams-mitigate-impact-of-slowing-adver`

[189] M. Allen, "Sean parker unloads on facebook:"god only knows what it's doing to our children's brains."," *Axios. Com*, 2017.

[190] B. Kidron, A. Evans, J. Afia, J. R. Adler, H. Bowden-Jones, L. Hackett, A. Juj, A. K. Przybylski, A. Rudkin, and Y. Scot, "Disrupted childhood: the cost of persuasive design," 2023.

[191] R. Foundation, "Pathways: How digital design puts children at risk," July 2021.

[192] T. H. Davenport and J. C. Beck, "The attention economy," *Ubiquity*, vol. 2001, no. May, pp. 1–es, 2001.

[193] K. C. Berridge and T. E. Robinson, "What is the role of dopamine in reward: hedonic impact, reward learning, or incentive salience?," *Brain research reviews*, vol. 28, no. 3, pp. 309–369, 1998.

[194] B. Kidron and A. Rudkin, "Digital childhood: Addressing childhood development milestones in the digital environment.," 2017.

[195] B. Carter, P. Rees, L. Hale, D. Bhattacharjee, and M. S. Paradkar, "Association between portable screen-based media device access or use and sleep outcomes: a systematic review and meta-analysis," *JAMA pediatrics*, vol. 170, no. 12, pp. 1202–1208, 2016.

[196] G. A. DeGangi, *Pediatric disorders of regulation in affect and behavior: A therapist's guide to assessment and treatment*. Academic Press, 2017.

[197] J. Vincent, "Former facebook exec says social media is ripping apart society," *The verge*, vol. 11, 2017.

[198] A. Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, *et al.*, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–41, 2017.

[199] B. J. Fogg, "A behavior model for persuasive design," in *Proceedings of the 4th international Conference on Persuasive Technology*, pp. 1–7, 2009.

[200] R. H. Thaler and C. R. Sunstein, *Nudge: Improving decisions about health, wealth, and happiness*. Penguin, 2009.

[201] C. Nodder, *Evil by design: Interaction design to lead us into temptation*. John Wiley & Sons, 2013.

[202] J. Redström, "Persuasive design: Fringes and foundations," in *International Conference on Persuasive Technology*, pp. 112–122, Springer, 2006.

[203] E. Stolterman and H. G. Nelson, "The design way," 2012.

[204] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The dark (patterns) side of ux design," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, pp. 1–14, 2018.

[205] A. Alter, *Irresistible: The rise of addictive technology and the business of keeping us hooked*. Penguin, 2017.

[206] H. Brignull, "Dark patterns: inside the interfaces designed to trick you," Aug 2013. `http://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you`.

[207] H. Brignull, "Deceptive design." `https://darkpatterns.org`.

[208] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side: Privacy dark strategies and privacy dark patterns.," *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 4, pp. 237–254, 2016.

[209] A. Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan, "Dark patterns at scale: Findings from a crawl of 11k shopping websites," *Proceedings of the ACM on Human-Computer Interaction*, vol. 3, no. CSCW, pp. 1–32, 2019.

[210] G. Conti and E. Sobiesk, "Malicious interface design: exploiting the user," in *Proceedings of the 19th international conference on World wide web*, pp. 271–280, 2010.

[211] N. C. Council, "Deceived by design, how tech companies use dark patterns to discourage us from exercising our rights to privacy," *Norwegian Consumer Council Report*, 2018.

[212] "Edps opinion on the legislative package "a new deal for consumers"." `https://edps.europa.eu/`

data-protection/our-work/publications/opinions/edps-opinion-legislative-package-new-deal-consumers_en.

[213] N. Singer, "When websites won't take no for an answer," *New York Times*, vol. 15, no. 5, p. 2016, 2016.

[214] J. Newman and J. Jerome, "Press start to track privacy and the new questions posed by modern video game technology," *AIPLA QJ*, vol. 42, p. 527, 2014.

[215] Leanplum, "Personalize or bust: the impact on app engagement," 2016.

[216] R. Botsman, "Who can you trust?: How technology brought us together and why it might drive us apart," 2017.

[217] G. Wells, J. Horwitz, and D. Seetharaman, "Facebook knows instagram is toxic for teen girls, company documents show," *The Wall Street Journal*, vol. 14, 2021.

[218] H. C. Woods and H. Scott, "# sleepyteens: Social media use in adolescence is associated with poor sleep quality, anxiety, depression and low self-esteem," *Journal of adolescence*, vol. 51, pp. 41–49, 2016.

[219] T. Newlove-Delgado, F. Marcheselli, T. Williams, D. Mandalia, J. Davis, S. McManus, M. Savic, W. Treloar, and T. Ford, "Mental health of children and young people in england, 2022-wave 3 follow up to the 2017 survey," 2022.

[220] E. A. Vogels, "Teens and cyberbullying 2022," 2022.

[221] S. Y. Sohn, P. Rees, B. Wildridge, N. J. Kalk, and B. Carter, "Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: a systematic review, meta-analysis and grade of the evidence," *BMC psychiatry*, vol. 19, no. 1, pp. 1–10, 2019.

[222] M. Samara, A. A. Massarwi, A. El-Asam, S. Hammuda, P. K. Smith, and H. Morsi, "The mediating role of bullying and victimisation on the relationship between problematic internet use and substance abuse among adolescents in the uk: The parent–child relationship as a moderator," *Frontiers in Psychiatry*, vol. 12, 2021.

[223] M. T. Maza, K. A. Fox, S.-J. Kwon, J. E. Flannery, K. A. Lindquist, M. J. Prinstein, and E. H. Telzer, "Association of habitual checking behaviors on social media with longitudinal functional brain development," *JAMA pediatrics*, vol. 177, no. 2, pp. 160–167, 2023.

[224] B. Clarke, R. Atkinson, and S. Svaneas, "How children use mobile devices at school and at home," Sep 2015. https://www.internetmatters.org/wp-content/uploads/2015/12/T4S-How-Children-Use-Mobile-Devices-at-School-and-at-Home-7.10.15.pdf.

[225] B. He, H. Xu, L. Jin, G. Guo, Y. Chen, and G. Weng, "An investigation into android in-app ad practice: Implications for app developers," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*, pp. 2465–2473, IEEE, 2018.

[226] L. Jin, B. He, G. Weng, H. Xu, Y. Chen, and G. Guo, "Madlens: Investigating into android in-app ad practice at api granularity," *IEEE Transactions on Mobile Computing*, vol. 20, no. 3, pp. 1138–1155, 2019.

[227] L. Gevelber, "Micro-moments now: 3 new consumer behaviors playing out in google search data," *Think with Google*, 2017.

[228] J. Kint, "Behavioral advertising: The mirage built by google," Jun 2019. https://digitalcontentnext.org/blog/2019/06/06/behavioral-advertising-the-mirage-built-by-google/.

[229] F. Myrstad and I. Tjøstheim, "Out of control. how consumers are exploited by the online advertising industry," 2021.

[230] J. Ryan and C. Santos, "An unending data breach immune to audit? can the tcf and rtb be reconciled with the gdpr?," *Can the TCF and RTB be reconciled with the GDPR*, 2022.

[231] "Applovin: The suite of solutions for your mobile games," Aug 2022. https://www.applovin.com/.

[232] "Facebook app ads." https://developers.facebook.com/docs/app-ads/.

[233] "Facebook audience network." https://developers.facebook.com/products/audience-network/.

[234] D. Geradin and D. Katsifis, "An eu competition law analysis of online display advertising in the programmatic age," *European Competition Journal*, vol. 15, no. 1, pp. 55–96, 2019.

[235] "Google advertising brands." https://www.blog.google/technology/ads/new-advertising-brands/.

[236] F. J. Z. Borgesius, "Singling out people without knowing their names–behavioural targeting, pseudonymous data, and the new data protection regulation," *Computer Law & Security Review*, vol. 32, no. 2, pp. 256–271, 2016.

[237] A. Rieke, H. Yu, D. Robinson, J. van Hoboken, *et al.*, "Data brokers in an open society," 2016.

[238] W. Christl, K. Kopp, and P. U. Riechert, "Corporate surveillance in everyday life," *Cracked Labs*, vol. 6, pp. 2017–10, 2017.

[239] K. Hill, "I got access to my secret consumer score. now you can get yours, too.," Nov 2019. https://www.nytimes.com/2019/11/04/business/secret-consumer-score-access.html.

[240] "Adobe cloud advertising health audience segments." https://linder.tv/docs/AdobeAdvertisingCloud.pdf, journal=Linder TV.

[241] "Liveramp: Data connectivity platform," Feb 2022. https://liveramp.com/partner-directory/?segment=data.

[242] R. Binns and E. Bietti, "Dissolving privacy, one merger at a time: Competition, data and third party tracking," *Computer Law & Security Review*, vol. 36, p. 105369, 2020.

[243] G. Johnson, S. Shriver, and S. Goldberg, "Privacy & market concentration: Intended & unintended consequences of the gdpr," *Available at SSRN 3477686*, 2022.

[244] "What is ad mediation?," Jun 2022. https://www.is.com/glossary/ad-mediation/.

[245] "Alphabet, form 10-k." https://abc.xyz/investor/static/pdf/20210203_alphabet_10K.pdf?cache=b44182d.

[246] I. Intelligence, "Mobile ad market and privacy restrictions - trends for 2022," May 2022. https://www.emarketer.com/Article/Mobile-Moves-Majority-Share-of-Googles-Worldwide-Ad-Revenues/1014633.

[247] S. Bellman, J. Murphy, S. Treleaven-Hassard, J. O'Farrell, L. Qiu, and D. Varan, "Using internet behavior to deliver relevant television commercials," *Journal of Interactive Marketing*, vol. 27, no. 2, pp. 130–140, 2013.

[248] C. R. Taylor and L. Carlson, "The future of advertising research: New directions and research needs," *Journal of Marketing Theory and Practice*, vol. 29, no. 1, pp. 51–62, 2021.

[249] G. Kerr and J. Richards, "Redefining advertising in research and practice," *International Journal of Advertising*, vol. 40, no. 2, pp. 175–198, 2021.

[250] "Emotional and sentiment targeting." https://www.admantx.com/emotional-and-sentiment-targeting/.

[251] "The basics of micro-moments," 2016. https://www.thinkwithgoogle.com/consumer-insights/consumer-journey/micro-moments-understand-new-consumer-behavior/.

[252] S. L. Calvert, "Children as consumers: Advertising and marketing," *The future of children*, pp. 205–234, 2008.

[253] L. F. Bright and T. Daugherty, "Does customization impact advertising effectiveness? an exploratory study of consumer perceptions of advertising in customized online environments," *Journal of Marketing Communications*, vol. 18, no. 1, pp. 19–37, 2012.

[254] J. Yan, N. Liu, G. Wang, W. Zhang, Y. Jiang, and Z. Chen, "How much can behavioral targeting help online advertising?," in *Proceedings of the 18th international conference on World wide web*, pp. 261–270, 2009.

[255] F. Zhao, S. Egelman, H. M. Weeks, N. Kaciroti, A. L. Miller, and J. S. Radesky, "Data collection practices of mobile applications played by preschool-aged children," *JAMA pediatrics*, vol. 174, no. 12, pp. e203345–e203345, 2020.

[256] S. Levin, "Facebook told advertisers it can identify teens feeling 'insecure'and 'worthless'," *The Guardian*, vol. 1, 2017.

[257] K. Hill, "Data broker was selling lists of rape victims, alcoholics, and "erectile dysfunction sufferers"," *Forbes*, vol. 19, no. September, 2013.

[258] A. Hern and F. H. Ledegaard, "Children 'interested in' gambling and alcohol, according to facebook," *The Guardian*, vol. 6, 2019.

[259] M. Buijzen, E. A. Van Reijmersdal, and L. H. Owen, "Introducing the pcmc model: An investigative framework for young people's processing of commercialized media content," *Communication Theory*, vol. 20, no. 4, pp. 427–450, 2010.

[260] D. R. John, "Consumer socialization of children: A retrospective look at twenty-five years of research," *Journal of consumer research*, vol. 26, no. 3, pp. 183–213, 1999.

[261] C. Hoffner, "Children's wishful identification and parasocial interaction with favorite television characters," *Journal of Broadcasting & Electronic Media*, vol. 40, no. 3, pp. 389–402, 1996.

[262] A. Nairn and C. Fine, "Who's messing with my mind? the implications of dual-process models for the ethics of advertising to children," *International Journal of Advertising*, vol. 27, no. 3, pp. 447–470, 2008.

[263] S. M. Neeley and D. W. Schumann, "Using animated spokes-characters in advertising to young children: does increasing attention to advertising necessarily lead to product preference?," *Journal of Advertising*, vol. 33, no. 3, pp. 7–23, 2004.

[264] L. Hudders, P. De Pauw, V. Cauberghe, K. Panic, B. Zarouali, and E. Rozendaal, "Shedding new light on how advertising literacy can affect children's processing of embedded advertising formats: A future research agenda," *Journal of Advertising*, vol. 46, no. 2, pp. 333–349, 2017.

[265] Y. Verhellen, C. Oates, P. De Pelsmacker, and N. Dens, "Children's responses to traditional versus hybrid advertising formats: The moderating role of persuasion knowledge," *Journal of Consumer Policy*, vol. 37, pp. 235–255, 2014.

[266] M. Meyer, V. Adkins, N. Yuan, H. M. Weeks, Y.-J. Chang, and J. Radesky, "Advertising in young children's apps: A content analysis," *Journal of developmental & behavioral pediatrics*, vol. 40, no. 1, pp. 32–39, 2019.

[267] L. J. Moses and D. A. Baldwin, "What can the study of cognitive development reveal about children's ability to appreciate and cope with advertising?," *Journal of public policy & marketing*, vol. 24, no. 2, pp. 186–201, 2005.

[268] G. Britain, *Children and parents: Media use and attitudes report 2018*. Ofcom, 2018.

[269] I. Reyes, P. Wijesekera, J. Reardon, A. E. B. On, A. Razaghpanah, N. Vallina-Rodriguez, and S. Egelman, ""won't somebody think of the children?" examining coppa compliance at scale," *Proceedings on Privacy Enhancing Technologies*, vol. 2018, no. 3, pp. 63–83, 2018.

[270] A. Ekambaranathan, J. Zhao, and M. Van Kleek, ""money makes the world go around": Identifying barriers to better privacy in children's apps from developers' perspectives," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–15, 2021.

[271] D. Moher, A. Liberati, J. Tetzlaff, D. G. Altman, and P. Group*, "Preferred reporting items for systematic reviews and meta-analyses: the prisma statement," *Annals of internal medicine*, vol. 151, no. 4, pp. 264–269, 2009.

[272] H. Chen, H. F. Leung, B. Han, and J. Su, "Automatic privacy leakage detection for massive android apps via a novel hybrid approach," vol. 0, 2017.

[273] Z. Bohluli and H. R. Shahriari, "Detecting privacy leaks in android apps using inter-component information flow control analysis," 2018.

[274] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill, "Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem," 2018.

[275] N. Kesswani, H. Lyu, and Z. Zhang, "Analyzing android app privacy with gp-pp model," *IEEE Access*, vol. 6, 2018.

[276] R. Slavin, X. Wang, M. B. Hosseini, J. Hester, R. Krishnan, J. Bhatia, T. D. Breaux, and J. Niu, "Pvdetector: A detector of privacy-policy violations for android apps," 2016.

[277] P. Kotak, S. Bhandari, A. Zemmari, and J. Joshi, "Unmasking privacy leakage through android apps obscured with hidden permissions," 2021.

[278] R. Boussada, B. Hamdane, F. Kamoun, and L. A. Saidane, "Surveying and analyzing privacy issues in contact tracing apps," 2021.

[279] O. Haggag, S. Haggag, J. Grundy, and M. Abdelrazek, "Covid-19 vs social media apps: Does privacy really matter?," vol. 2021-May, 2021.

[280] A. Prasad, M. Clark, H. L. Nguyen, R. Ruiz, and E. Xiao, "Analyzing privacy practices of existing mhealth apps," 2020.

[281] S. J. Juneidi, "Covid-19 tracing contacts apps: Technical and privacy issues," *International Journal of Advances in Soft Computing and its Applications*, vol. 12, 2020.

[282] S. Kumar and R. Shanker, "Your privacy is not so private: Unveiling android apps privacy framework from the dark," 2018.

[283] K. Ito, H. Hasegawa, Y. Yamaguchi, and H. Shimada, "Detecting privacy information abuse by android apps from api call logs," vol. 11049 LNCS, 2018.

[284] M. Lindh and J. Nolin, "Information we collect: Surveillance and privacy in the implementation of google apps for education," *European Educational Research Journal*, vol. 15, 2016.

[285] S. S. Mitchell, ""warning! you're entering a sick zone": The construction of risk and privacy implications of disease tracking apps," *Online Information Review*, vol. 43, 2019.

[286] Y. M. Al-Sharo, "Networking issues for security and privacy in mobile health apps," *International Journal of Advanced Computer Science and Applications*, vol. 10, 2019.

[287] A. S. Ali and Z. F. Zaaba, "A study on contact tracing apps for covid-19: Privacy and security perspective," *Webology*, vol. 18, 2021.

[288] L. S. C. Ramos and D. Bhattacharya, "Covid-19: Privacy and confidentiality issues with contact tracing apps," vol. 2020-January, 2021.

[289] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android vpn permission-enabled apps," vol. 14-16-November-2016, 2016.

[290] L. Baumgartner, A. Dmitrienko, B. Freisleben, A. Gruler, J. Hochst, J. Kuhlberg, M. Mezini, R. Mitev, M. Miettinen, A. Muhamedagic, T. D. Nguyen, A. Penning, D. Pustelnik, F. Roos, A. R. Sadeghi, M. Schwarz, and C. Uhl, "Mind the gap: Security privacy risks of contact tracing apps," 2020.

[291] F. Zhao, L. Gao, Y. Zhang, Z. Wang, B. Wang, and S. Guo, "You are where you app: An assessment on location privacy of social applications," vol. 2018-October, 2018.

[292] S. Zhao, X. Luo, X. Ma, B. Bai, Y. Zhao, W. Zou, Z. Yang, M. H. Au, and X. Qiu, "Exploiting proximity-based mobile apps for large-scale location privacy probing," *Security and Communication Networks*, vol. 2018, 2018.

[293] L. Yu, X. Luo, X. Liu, and T. Zhang, "Can we trust the privacy policies of android apps?," 2016.

[294] M. Liu, H. Wang, Y. Guo, and J. Hong, "Identifying and analyzing the privacy of apps for kids," 2016.

[295] T. Brüggemann, J. Hansen, T. Dehling, and A. Sunyaev, "An information privacy risk index for mhealth apps," vol. 9857 LNCS, 2016.

[296] S. Zimmeck, Z. Wang, L. Zou, R. Iyengar, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S. M. Bellovin, and J. Reidenberg, "Automated analysis of privacy requirements for mobile apps," vol. FS-16-01 - FS-16-05, 2016.

[297] K. Zhu, X. He, B. Xiang, L. Zhang, and A. Pattavina, "How dangerous are your smartphones? app usage recommendation with privacy preserving," *Mobile Information Systems*, vol. 2016, 2016.

[298] N. Kesswani and F. Lin, "How privacy invasive android apps are?," 2016.

[299] A. Quattrone, L. Kulik, E. Tanin, K. Ramamohanarao, and T. Gu, "Privacypalisade: Evaluating app permissions and building privacy into smartphones," 2016.

[300] H. Xu, Y. Zhou, C. Gao, Y. Kang, and M. R. Lyu, "Spyaware: Investigating the privacy leakage signatures in app execution traces," 2016.

[301] A. Youssef and A. F. Shosha, "Quantitave dynamic taint analysis of privacy leakage in android arabic apps," vol. Part F130521, 2017.

[302] A. Hamed, H. K.-B. Ayed, and D. Machfar, "Assessment for android apps permissions a proactive approach toward privacy risk," 2017.

[303] D. Zhang, Y. Guo, D. Guo, R. Wang, and G. Yu, "Contextual approach for identifying malicious inter-component privacy leaks in android apps," 2017.

[304] L. Rosenfeld, J. Torous, and I. V. Vahia, "Data security and privacy in apps for dementia: An analysis of existing privacy policies," *American Journal of Geriatric Psychiatry*, vol. 25, 2017.

[305] M. Hatamian, J. Serna, K. Rannenberg, and B. Igler, "Fair: Fuzzy alarming index rule for privacy analysis in smartphone apps," vol. 10442 LNCS, 2017.

[306] D. Liu, X. Gao, and H. Wang, "Location privacy breach: Apps are watching you in background," 2017.

[307] V. Jain, S. Bhandari, V. Laxmi, M. S. Gaur, and M. Mosbah, "Sniffdroid: Detection of inter-app privacy leaks in android," in *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 331–338, IEEE, 2017.

[308] L. Hutton, B. A. Price, R. Kelly, C. McCormick, A. K. Bandara, T. Hatzakis, M. Meadows, and B. Nuseibeh, "Assessing the privacy of

mhealth apps for self-tracking: Heuristic evaluation approach," *JMIR mHealth and uHealth*, vol. 6, 2018.

[309] Y. He, Q. Li, and K. Sun, "Linkflow: Efficient large-scale inter-app privacy leakage detection," vol. 238, 2018.

[310] S. E. Polykalas, G. N. Prezerakos, F. D. Chrysidou, and E. D. Pylarinou, "Mobile apps and data privacy: When the service is free, the product is your data," vol. 2018-January, 2018.

[311] G. Das, C. Cheung, C. Nebeker, M. Bietz, and C. Bloss, "Privacy policies for apps targeted toward youth: Descriptive analysis of readability," *JMIR mHealth and uHealth*, vol. 6, 2018.

[312] J. Ren, M. Lindorfer, D. J. Dubois, A. Rao, D. Choffnes, and N. Vallina-Rodriguez, "Bug fixes, improvements, ... and privacy leaks - a longitudinal study of pii leaks across android app versions," 2018.

[313] Y. Nan, Z. Yang, X. Wang, Y. Zhang, D. Zhu, and M. Yang, "Finding clues for your secrets: Semantics-driven, learning-based privacy discovery in mobile apps," 2018.

[314] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg, "A multilateral privacy impact analysis method for android apps," vol. 11498 LNCS, 2019.

[315] K. Huckvale, J. Torous, and M. E. Larsen, "Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation," *JAMA Network Open*, vol. 2, 2019.

[316] J. M. Robillard, T. L. Feng, A. B. Sporn, J. A. Lai, C. Lo, M. Ta, and R. Nadler, "Availability, readability, and content of privacy policies and terms of agreements of mental health apps," *Internet Interventions*, vol. 17, 2019.

[317] Y. Chen, M. Zha, N. Zhang, D. Xu, Q. Zhao, X. Feng, K. Yuan, F. Suya, Y. Tian, K. Chen, X. Wang, and W. Zou, "Demystifying hidden privacy settings in mobile apps," vol. 2019-May, 2019.

[318] N. Momen, M. Hatamian, and L. Fritsch, "Did app privacy improve after the gdpr?," *IEEE Security and Privacy*, vol. 17, 2019.

[319] H. M. A. Maqsood, K. N. Qureshi, F. Bashir, and N. U. Islam, "Privacy leakage through exploitation of vulnerable inter-app communication on android," 2019.

[320] K. O'Loughlin, M. Neary, E. C. Adkins, and S. M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression," *Internet Interventions*, vol. 15, 2019.

[321] M. V. Stoicescu, S. Matei, and R. Rughinis, "Sharing and privacy in dating apps," 2019.

[322] P. Calciati, K. Kuznetsov, A. Gorla, and A. Zeller, "Automatically granted permissions in android apps: An empirical study on their prevalence and on the potential threats for privacy," 2020.

[323] J. L. Kröger, J. Lindemann, and D. Herrmann, "How do app vendors respond to subject access requests?: A longitudinal privacy study on ios and android apps," 2020.

[324] K. Alkhattabi, A. Alshehri, and C. Yue, "Security and privacy analysis of android family locator apps," 2020.

[325] H. Wen, Q. Zhao, Z. Lin, D. Xuan, and N. Shroff, "A study of the privacy of covid-19 contact tracing apps," vol. 335, 2020.

[326] J. Benjumea, J. Ropero, O. Rivera-Romero, E. Dorronzoro-Zubiete, and A. Carrasco, "Assessment of the fairness of privacy policies of mobile health apps: Scale development and evaluation in cancer apps," *JMIR mHealth and uHealth*, vol. 8, 2020.

[327] L. Verderame, D. Caputo, A. Romdhana, and A. Merlo, "On the (un)reliability of privacy policies in android apps," 2020.

[328] E. Farooq, M. A. N. U. Ghani, Z. Naseer, and S. Iqbal, "Privacy policies' readability analysis of contemporary free healthcare apps," 2020.

[329] M. Zhang, A. Chow, and H. Smith, "Covid-19 contact-tracing apps: Analysis of the readability of privacy policies," 2020.

[330] T. Sharma, M. M. Islam, A. Das, S. M. Haque, and S. I. Ahmed, "Privacy during pandemic: A global view of privacy practices around covid-19 apps," 2021.

[331] D. J. Leith and S. Farrell, "Contact tracing app privacy: What data is shared by europe's gaen contact tracing apps," vol. 2021-May, 2021.

[332] V. Ang and L. K. Shar, "Covid-19 one year on-security and privacy review of contact tracing mobile apps," 2021.

[333] L. Yu, X. Luo, J. Chen, H. Zhou, T. Zhang, H. Chang, and H. K. Leung, "Ppchecker: Towards accessing the trustworthiness of android apps' privacy policies," *IEEE Transactions on Software Engineering*, vol. 47, 2021.

[334] M. Hatamian, S. Wairimu, N. Momen, and L. Fritsch, "A privacy and security analysis of early-deployed covid-19 contact tracing android apps," *Empirical Software Engineering*, vol. 26, 2021.

[335] J. J. Flors-Sidro, M. Househ, A. Abd-Alrazaq, J. Vidal-Alaball, L. Fernandez-Luque, and C. L. Sanchez-Bocanegra, "Analysis of diabetes apps to assess privacy-related permissions: systematic search of apps," *JMIR Diabetes*, vol. 6, 2021.

[336] I. W. B. Sentana, M. Ikram, M. A. Kaafar, and S. Berkovsky, "Empirical security and privacy analysis of mobile symptom checking apps on google play," 2021.

[337] S. Wairimu and N. Momen, "Privacy analysis of covid-19 contact tracing apps in the eu," vol. 12556 LNCS, 2021.

[338] S. J. De and R. Shukla, "An analysis of privacy policies of public covid-19 apps: Evidence from india," *Journal of Public Affairs*, 2021.

[339] F. Mohsen, H. Abdelhaq, and H. Bisgin, "Security-centric ranking algorithm and two privacy scores to mitigate intrusive apps," vol. 34, 2022.

[340] B. X. Chen, "How to protect your privacy as more apps harvest your data," May 2017. `https://www.nytimes.com/2017/05/03/technology/personaltech/how-to-protect-your-privacy-as-more-apps-harvest-your-data.html`.

[341] A. Acquisti and J. Grossklags, "Privacy and rationality in individual decision making," *IEEE security & privacy*, vol. 3, no. 1, pp. 26–33, 2005.

[342] J. Angulo, S. Fischer-Hübner, E. Wästlund, and T. Pulls, "Towards usable privacy policy display and management," *Information Management & Computer Security*, 2012.

[343] A. M. McDonald and L. F. Cranor, "The cost of reading privacy policies," *Isjlp*, vol. 4, p. 543, 2008.

[344] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[345] P. Wisniewski, A. K. Ghosh, H. Xu, M. B. Rosson, and J. M. Carroll, "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*, pp. 51–69, ACM, 2017.

[346] J. Corbin and A. Strauss, *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[347] J. Rieman, M. Franzke, and D. Redmiles, "Usability evaluation with the cognitive walkthrough," in *Conference companion on Human factors in computing systems*, pp. 387–388, 1995.

[348] B. E. John and H. Packer, "Learning and using the cognitive walkthrough method: a case study approach," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 429–436, 1995.

[349] "Adjust: Set up apps for children." `https://help.adjust.com/en/article/apps-for-children-android-sdk`.

[350] "Age appropriate design code standard 4: Transparency." `https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/4-transparency/`.

[351] "Common sense media." `https://www.commonsensemedia.org/`.

[352] "Understand app privacy amp; security practices with google play's data safety section - android." https://support.google.com/googleplay/answer/11416267?hl=en&co=GENIE.Platform%3DAndroid.

[353] "Piwik pro analytics suite: On-premises amp; private cloud," Oct 2022. https://piwik.pro/.

[354] "Create data privacy moments maps." https://ico.org.uk/for-organisations/childrens-code-design-guidance/create-data-privacy-moments-maps/.

[355] https://developer.apple.com/app-store/review/guidelines/.

[356] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[357] G. Guest, A. Bunce, and L. Johnson, "How many interviews are enough? an experiment with data saturation and variability," *Field methods*, vol. 18, no. 1, pp. 59–82, 2006.

[358] M. Q. Patton, *Qualitative research & evaluation methods*. sage, 2002.

[359] V. Braun, V. Clarke, N. Hayfield, and G. Terry, "Thematic analysis," in *Handbook of research methods in health social sciences*, pp. 843–860, Springer, 2018.

[360] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and psychological measurement*, vol. 20, no. 1, pp. 37–46, 1960.

[361] H. Wang, Y. Guo, Z. Ma, and X. Chen, "Wukong: A scalable and accurate two-phase approach to android app clone detection," in *Proceedings of the 2015 International Symposium on Software Testing and Analysis*, pp. 71–82, 2015.

[362] M. Linares-Vásquez, A. Holtzhauer, C. Bernal-Cárdenas, and D. Poshyvanyk, "Revisiting android reuse studies in the context of code obfuscation and library usages," in *Proceedings of the 11th Working Conference on Mining Software Repositories*, pp. 242–251, 2014.

[363] M. T. Baldassarre, A. Bianchi, D. Caivano, and G. Visaggio, "An industrial case study on reuse oriented development," in *21st IEEE International Conference on Software Maintenance (ICSM'05)*, pp. 283–292, IEEE, 2005.

[364] W. C. Lim, "Effects of reuse on quality, productivity, and economics," *IEEE software*, vol. 11, no. 5, pp. 23–30, 1994.

[365] M. Morisio, D. Romano, and I. Stamelos, "Quality, productivity, and learning in framework-based development: An exploratory case study," *IEEE Transactions on Software Engineering*, vol. 28, no. 9, pp. 876–888, 2002.

[366] B. Clifton, "Why is google analytics free?," Aug 2020. `https://brianclifton.com/blog/2007/07/23/why-is-google-analytics-unique-free/`.

[367] J. A. Obar and A. Oeldorf-Hirsch, "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Communication & Society*, vol. 23, no. 1, pp. 128–147, 2020.

[368] H. Assal and S. Chiasson, "'think secure from the beginning': A survey with software developers," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, p. 289, ACM, 2019.

[369] "Choosing a business model - app store." `https://developer.apple.com/app-store/business-models/`.

[370] "Using the freemium business model - app store." `https://developer.apple.com/app-store/freemium-business-model/`.

[371] S. Sigg, E. Lagerspetz, E. Peltonen, P. Nurmi, and S. Tarkoma, "Exploiting usage to predict instantaneous app popularity: Trend filters and retention rates," *ACM Transactions on the Web (TWEB)*, vol. 13, no. 2, pp. 1–25, 2019.

[372] "Ads and monetization - play console help." `https://support.google.com/googleplay/android-developer/answer/9898834`.

[373] "Participate in the families ads program - play console help." https://support.google.com/googleplay/android-developer/answer/9283445.

[374] M. Nouwen, M. Van Mechelen, and B. Zaman, "A value sensitive design approach to parental software for young children," in *Proceedings of the 14th International Conference on Interaction Design and Children*, pp. 363–366, 2015.

[375] A. Hiniker, K. Sobel, and B. Lee, "Co-designing with preschoolers using fictional inquiry and comicboarding," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 5767–5772, ACM, 2017.

[376] J. Smith, B. Johnson, E. Murphy-Hill, B. Chu, and H. R. Lipford, "Questions developers ask while diagnosing potential security vulnerabilities with static analysis," in *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering*, pp. 248–259, ACM, 2015.

[377] J. Xie, B. Chu, H. R. Lipford, and J. T. Melton, "Aside: Ide support for web application security," in *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 267–276, ACM, 2011.

[378] "User privacy and data use - app store." https://developer.apple.com/app-store/user-privacy-and-data-use/.

[379] C. Newton, "Apple's move to make advertising harder on ios 14 is part of a trend," Aug 2020. https://www.theverge.com/interface/2020/8/27/21402744/apple-idfa-facebook-fight-ads-advertising.

[380] J. R. Vickery, "'i don't have anything to hide, but...': the challenges and negotiations of social and mobile media privacy for non-dominant youth," *Information, Communication & Society*, vol. 18, no. 3, pp. 281–294, 2015.

[381] J. W. Creswell and J. D. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2017.

[382] D. A. Dillman, J. D. Smyth, and L. M. Christian, *Internet, phone, mail, and mixed-mode surveys: The tailored design method*. John Wiley & Sons, 2014.

[383] R. M. Groves, F. J. Fowler Jr, M. P. Couper, J. M. Lepkowski, E. Singer, and R. Tourangeau, *Survey methodology*. John Wiley & Sons, 2011.

[384] A. Rubin and E. R. Babbie, *Research methods for social work*. , 2007.

[385] S. Sudman, N. M. Bradburn, and N. Schwarz, *Thinking about answers: The application of cognitive processes to survey methodology*. Jossey-Bass, 1996.

[386] A. Ekambaranathan, J. Zhao, and M. Van Kleek, "Understanding value and design choices made by android family app developers," in *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–10, 2020.

[387] J. Zimmerman, J. Forlizzi, and S. Evenson, "Research through design as a method for interaction design research in hci," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 493–502, 2007.

[388] H. W. Rittel and M. M. Webber, "Dilemmas in a general theory of planning," *Policy sciences*, vol. 4, no. 2, pp. 155–169, 1973.

[389] C. Frayling, "Research in art and design," *Royal College of Art research papers*, vol. 1, pp. 1–5, 1993.

[390] J. Zimmerman, E. Stolterman, and J. Forlizzi, "An analysis and critique of research through design: towards a formalization of a research approach," in *proceedings of the 8th ACM conference on designing interactive systems*, pp. 310–319, 2010.

[391] P. Lunenfeld, *Design research: Methods and perspectives*. MIT press, 2003.

[392] P. J. Stappers, "Doing design as a part of doing research," in *Design research now*, pp. 81–91, Birkhäuser, 2012.

[393] J. Zimmerman and J. Forlizzi, "Speed dating: providing a menu of possible futures," *She Ji: The Journal of Design, Economics, and Innovation*, vol. 3, no. 1, pp. 30–50, 2017.

[394] S. Davidoff, M. K. Lee, A. K. Dey, and J. Zimmerman, "Rapidly exploring application design through speed dating," in *International conference on ubiquitous computing*, pp. 429–446, Springer, 2007.

[395] J. Forlizzi, C. DiSalvo, J. Zimmerman, B. Mutlu, and A. Hurst, "The sensechair: The lounge chair as an intelligent assistive device for elders," in *Proceedings of the 2005 conference on Designing for User eXperience*, pp. 31–es, 2005.

[396] J. X. Chen, F. Vitale, and J. McGrenere, "What happens after death? using a design workbook to understand user expectations for preparing their data," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2021.

[397] A. Desjardins, H. R. Biggs, C. Key, and J. E. Viny, "Iot data in the home: Observing entanglements and drawing new encounters," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2020.

[398] M. Blythe, E. Encinas, J. Kaye, M. L. Avery, R. McCabe, and K. Andersen, "Imaginary design workbooks: Constructive criticism and practical provocation," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pp. 1–12, 2018.

[399] W. Gaver, "Making spaces: how design workbooks work," in *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 1551–1560, 2011.

[400] R. Y. Wong, D. K. Mulligan, E. Van Wyk, J. Pierce, and J. Chuang, "Eliciting values reflections by engaging privacy futures using design workbooks," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 1–26, 2017.

[401] J. Knapp, J. Zeratsky, and B. Kowitz, *Sprint: How to solve big problems and test new ideas in just five days*. Simon and Schuster, 2016.

[402] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A" nutrition label" for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, pp. 1–12, 2009.

[403] T. Berners-Lee, "Protecting people from states," 2021. https://securingourdigitalfuture.com/2021/09/19/protecting-people-from-states/.

[404] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[405] B. Saunders, J. Sim, T. Kingstone, S. Baker, J. Waterfield, B. Bartlam, H. Burroughs, and C. Jinks, "Saturation in qualitative research: exploring its conceptualization and operationalization," *Quality & quantity*, vol. 52, pp. 1893–1907, 2018.

[406] V. Dignum, M. Penagos, K. Pigmans, and S. Vosloo, "Policy guidance on ai for children," 2020.

[407] A. Senarath, M. Grobler, and N. A. G. Arachchilage, "Will they use it or not? investigating software developers' intention to follow privacy engineering methodologies," *ACM Transactions on Privacy and Security (TOPS)*, vol. 22, no. 4, pp. 1–30, 2019.

[408] M. T. Baldassarre, V. Santa Barletta, D. Caivano, and M. Scalera, "Integrating security and privacy in software development," *Software Quality Journal*, vol. 28, no. 3, pp. 987–1018, 2020.

[409] Jan 2022. https://standards.ieee.org/.

[410] "Certification schemes." https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/certification-schemes-detailed-guidance/.

[411] L. H. Iwaya, M. A. Babar, and A. Rashid, "Privacy engineering in the wild: Understanding the practitioners' mindset, organisational culture, and current practices," *arXiv preprint arXiv:2211.08916*, 2022.

[412] M. Van Kleek, I. Liccardi, R. Binns, J. Zhao, D. J. Weitzner, and N. Shadbolt, "Better the devil you know: Exposing the data sharing

practices of smartphone apps," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 5208–5220, ACM, 2017.

[413] H. Almuhimedi, F. Schaub, N. Sadeh, I. Adjerid, A. Acquisti, J. Gluck, L. F. Cranor, and Y. Agarwal, "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*, pp. 787–796, 2015.

[414] `https://www.fairtrade.net/`.

[415] `https://www.bcorporation.net/`.

[416] A. Longfield, "Who knows what about me," 2018.

[417] P. C. Kumar, M. Chetty, T. L. Clegg, and J. Vitak, "Privacy and security considerations for digital technology use in elementary schools," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2019.

[418] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[419] S. Livingstone and A. Blum-Ross, "Parenting for a digital future... the book!," *Parenting for a Digital Future*, 2018.

[420] C. Z. Liu, Y. A. Au, and H. S. Choi, "Effects of freemium strategy in the mobile app market: An empirical study of google play," *Journal of Management Information Systems*, vol. 31, no. 3, pp. 326–354, 2014.

[421] E. C. Smizer, "Epic games v. apple: Tech-tying and the future of antitrust," *Loy. LA Ent. L. Rev.*, vol. 41, p. 215, 2021.

[422] `https://www.apple.com/privacy/labels/`.

[423] M. Kim, "Developers raise alarm over their cut of google play pass' subscription money," *IGN*, Sep 2019. `https://www.ign.com/articles/2019/09/24/developers-raise-alarm-over-their-cut-of-google-play-pass-subscription-money`

[424] M. Ragnedda and G. Destefanis, *Blockchain and web 3.0: social, economic, and technological challenges*. Routledge, 2019.

[425] A. Robertson, "Google bans tracking tool that sold users' location data," Aug 2021. https://www.theverge.com/2021/8/12/22621685/google-ban-safegraph-android-user-data-location-tracking.

[426] E. Neundorfer and A. J. Perez, "Clearcommprivacy: communicating app privacy behavior in android," in *Proceedings of the 2022 ACM Southeast Conference*, pp. 248–253, 2022.

[427] J. Brooke *et al.*, "Sus-a quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.

[428] "Vue.js - the progressive javascript framework." https://vuejs.org/.

[429] "Vuetify - a material design framework for vue.js." https://vuetifyjs.com/en/.

[430] "Gunicorn." https://gunicorn.org/.

[431] "Flask." https://flask-rest-api.readthedocs.io/en/stable/.

[432] "nginx." https://nginx.org/en/.

[433] "Countly analytics." https://count.ly/.

[434] "Parse platform." https://parseplatform.org/.

[435] "Piwik." https://piwik.pro/.

[436] I. Neo4j, "Neo4j: The world's leading graph database," 2021. https://neo4j.com/.

[437] M. Bostock, "Data-driven documents." https://d3js.org/.

[438] M. Tahaei, A. Frik, and K. Vaniea, "Deciding on personalized ads: Nudging developers about user privacy," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pp. 573–596, 2021.

[439] Pluja, "Awesomeme privacy - a curated list of services and alternatives that respect your privacy.." https://github.com/pluja/awesome-privacy.

[440] T. Li, E. Louie, L. Dabbish, and J. I. Hong, "How developers talk about personal data and what it means for user privacy: A case study of a developer forum on reddit," *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW3, pp. 1–28, 2021.