# Safeguarding Children's Privacy in the Digital Age:
# An Assessment of GDPR Compliance and Data Tracking in Popular Mobile Apps

**Jeremiah Eze**

**Student Number: 101061078**

Submitted as part of the requirements for the award of the
MSc in Information Security at Royal Holloway, University of London.


Royal Holloway, University of London
Information Security Group
Egham, Surrey, TW20 0EX
United Kingdom

# Acknowledgements

In the first place, I am making this acknowledgement to the Lord Almighty for His grace and assistance during the formulation of this project. Without His strength and wisdom, it would have been impossible for me to finish this dissertation and thus, I am very grateful for His blessings to me from start to finish of this dissertation.

I extend my deepest appreciation to my supervisor whose unparalleled support in this venture has seen me through successfully complete this dissertation. Her valuable feedback and unwavering support have been instrumental in guiding me through the challenges of this research project and motivating me to strive for excellence in every aspect of my work. I am truly grateful for her dedication and commitment, to this endeavour.

I would love to express my deepest gratitude to my family and friends for being so interested in my work and for being instrumental in my work's completion. They have been more than supportive, patient and encouraging and I am grateful to have them here with me all through this process.

To all those who in one way or the other helped in the making of this journey, I say thank you very much. I must state that this achievement is not personal to me but a summary of support, knowledge and encouragement which has been provided by each of you.

# Table of Contents

# List of Figures



# List of Tables

# Summary

This dissertation is aimed at examining how children's apps have embraced the GDPR principles with an emphasis on the privacy of children in the digital age. Since there is a higher percentage of children who use mobile applications the issue of protecting their data has become more critical. Children are again at high risk of their privacy invasion because of their inability to understand the data usage and their own privacy rights thus making them prime victims of data use, profiling and selling.

The study is motivated by the critical importance of safeguarding children's data online and aims to identify the extent to which popular children's apps comply with GDPR's seven key principles: Lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. The study entails a cross-comparison of the 30 most downloaded children's apps and the analysis of their privacy policies to identify whether they adhere to the GDPR regulations to the extent of full, partial, or non-compliance.

Research shows that there is a high non-compliance rate with many of the applications audited. While there are apps like Epic that make full compliance on data collection practices, user rights, and security measures, there are others like Fulldive VR which lack compliance. Some of the usual failures are poor data minimization measures, ambiguous data retention periods, low transparency levels, and weak accountability frameworks. These gaps show that there are issues that app developers have when it comes to GDPR compliance especially in the areas that may be difficult to manage including data minimization and storage limitation principles.

The study also identifies a gap between the stated policies and practices in that most of the apps' stated policies do not match their practice as would be expected. This implies that there is a need for constant surveillance of the proactive measures, better compliance with the laws in this area, and better disclosure measures to guarantee that children data is shielded.

Recommendations derived from studying into this area call for clear and understandable messages concerning the data handling practices in the apps to be developed, careful evaluation on the ways of minimizing the use of collected data and precise handling of data. There is also the need to increase the parents and children's awareness and knowledge of their privacy rights and the consequences of sharing their information.

In conclusion, this study adds knowledge to the current literature on children's digital privacy, and simulates the continued need for research, enhanced policy enforcement and effective legal safeguards to protect the youngest generation in the digital frontier.

# Chapter 1 – Introduction

## 1.1 Project Motivation

Today's society is connected to screens and as a result, children are running with their heads first into the ocean of mobile application with educational and entertainment purposes. However, just like all things in this world, this digital revolution is not completely rosy; it comes with a black cloud of doubts on how effectively these applications protect the kids' data. Such population groups include children; they hardly understand the implications of privacy matters. Their info can be accrued and abused in a way that has long and catastrophic ramifications in their lives.

For measures to protect the individual especially the children the European Union has made a move through the GDPR. Nevertheless, by the time one gets down to its actual application many of children's apps often lack these qualities. Despite these guidelines outlined by the GDPR, a high percentage of apps still offend against privacy regulations and harvest much more data than they are supposed to or fail to give adequate information on the purpose and scope of the data they are collecting.

The idea for this project was drawn from genuine concern of privacy that children are exposing themselves to in the natural online environment. To address this, I will analyse the privacy policies of thirty popular children's apps from the Google Play Store to assess how well they adhere to the GDPR's seven fundamental principles: Lawfulness, fairness, and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Besides, via tracking tools, this research will establish the tracking technologies applied by these apps, providing an insight into the degree of data sharing and possible infringement of user's privacy.

This research is motivated by the urgent need to draw attention to the current state of the effectiveness of GDPR in the context of children's apps and provide suggestions for practical changes for the stakeholders and the policymakers. In achieving this, I hope to raise awareness on the necessity of sound privacy standards and help towards the establishment of a secure cybersphere for children. It is in this regard that this study seeks to address these pressing issues to ensure young users privacy rights are protected and the online environment is made secure for the vulnerable users.

## 1.2 Contribution

This thesis presents three contributions through a thorough examination of the privacy policies of thirty widely used children's apps on the Google Play Store. This research assesses their compliance with the seven fundamental principles of GDPR – lawfulness, transparency, data minimization, accuracy, storage limitation, and integrity and confidentiality. This assessment aims to offer a view of the level of GDPR adherence, within children's applications today.

Additionally, the study uses Exodus Privacy to perform an in-depth analysis of tracking within these applications which will reveal how extensively these apps track users and share their data with parties The results will provide insight into the potential privacy concerns related to apps, for children and evaluate the adequacy of existing privacy protections.

The dissertation also aims to impact app developers and policymakers by providing suggestions derived from the research results to encourage the adoption of improved privacy practices. The suggestions will center on increasing transparency in processes and reducing data collection while ensuring safeguards for data protection. Moreover, the research will emphasize the

significance of educating users to raise awareness, about privacy among children and their caretakers.
This dissertation aims to make a contribution, by focusing attention on these crucial aspects to enhance the safety of the online space for children while safeguard their privacy and data security in alignment with GDPR regulations.

## 1.3 Project Outline and Structure

This dissertation is systematically organized into several key chapters, each addressing distinct aspects of the research with some focus on privacy-enhancing technologies for children in chapter 2, particularly within the context of online apps and their compliance with GDPR (General Data Protection Regulation) standards. The structure ensures a comprehensive examination of the topic, guiding the reader from the foundational background through to the analysis, discussion, and final conclusions.

**Chapter 2 – Background**
In Chapter 2 there is an exploration of the rules governing children's privacy on the internet and technologies designed to safeguard privacy in that context. The chapter starts by highlighting the significance of safeguarding children's privacy and proceeds to examine the General Data Protection Regulation (GDPR) emphasizing its guidelines concerning children's data. Additionally, it briefly contrasts these GDPR regulations with those outlined in the Children's Online Privacy Protection Act (COPPA) though placing emphasis on ensuring compliance, with GDPR standards. The article delves into the difficulties that developers of applications encounter when following these rules. Emphasizes the importance of privacy enhancing technologies, in reducing risks setting the stage for examining privacy policies and data monitoring methods.

Section 2.1 focuses on the significance of safeguarding children's privacy in today's landscape by considering their vulnerabilities and the potential dangers posed by mobile applications that gather and analyse personal information. Section 2.2 provides an overview of the key legal frameworks, with a focus on GDPR's core principles and a brief comparison with COPPA to highlight key differences. In Section 2.3, the specific concerns related to children's apps, particularly data collection practices and GDPR compliance challenges, are discussed. Section 2.4 delves into privacy technologies that help protect privacy like encryption and anonymization. Section 2.5 takes a look at the rules around GDPR enforcement, and the obstacles regulators encounter as well as how it affects app development worldwide. Finally, Section 2.6 connects the regulatory background to the study, explaining how the legal and technological context informs the analysis of privacy policies and data tracking in children's apps.

**Chapter 3: Evaluation of Privacy Policies**
The chapter discusses the approach and results of assessing privacy policies for 30 kid's apps on the Google Play Store. It starts by explaining why these apps were chosen and stresses the significance of reviewing their privacy policies. It describes how the apps were picked for analysis and assessment based on GDPR adherence with a focus on seven criteria such, as legality, data reduction and responsibility. The assessment points out the negative aspects of the applications approaches, to privacy issues before wrapping up with a recap of significant discoveries and what they mean for safeguarding children's privacy.

**Chapter 4: Data Tracking Practices**
In Chapter 4 of this paper, it discusses how apps track data and whether they adhere to GDPR regulations using tools such as Exodus Privacy as a reference point. It begins by exploring how data tracking affects the privacy of children before delving into the methodology which explains how Exodus Privacy identified trackers and compared their findings to GDPR guidelines. The chapter reveals insights, on the frequency and kinds of trackers used their methods of collecting

data and level of transparency. It wraps up by summarizing these discoveries and discussing their significance in safeguarding children's data within apps.

**Chapter 5 - Discussion**

This section examines the deficiencies in meeting GDPR requirements observed in the privacy policies and data monitoring methods of apps designed for children. Building a connection between assessments and ultimate suggestions is pivotal here as it stresses the significance of recognizing these gaps. The approach utilized entails a framework for analyzing deficiencies to classify the concerns into matters along with technical and operational inadequacies. Through this analysis emerge drawbacks like incomplete privacy policies, limited data protection protocols and lacking internal adherence to regulations and their impacts, on relevant parties are deliberated upon. The chapter wraps up by summarizing these discoveries and preparing for the suggestions to come ahead.

In this chapter well as in the examination of privacy policy and data tracking implications are discussed in depth here. Suggestions are made for app developers and policymakers to enhance compliance with GDPR and improve privacy, for children. The chapter also outlines research directions and underscores the growing importance of privacy enhancing technologies.

**Chapter 6 - Conclusions**

The final section brings together the discoveries, from the thesis while pondering over the research goals and addressing the study's constraints. It also looks at how the research could influence the domain of privacy for children and proposes future possibilities to expand on this research.

### 1.3.1 Project Structure

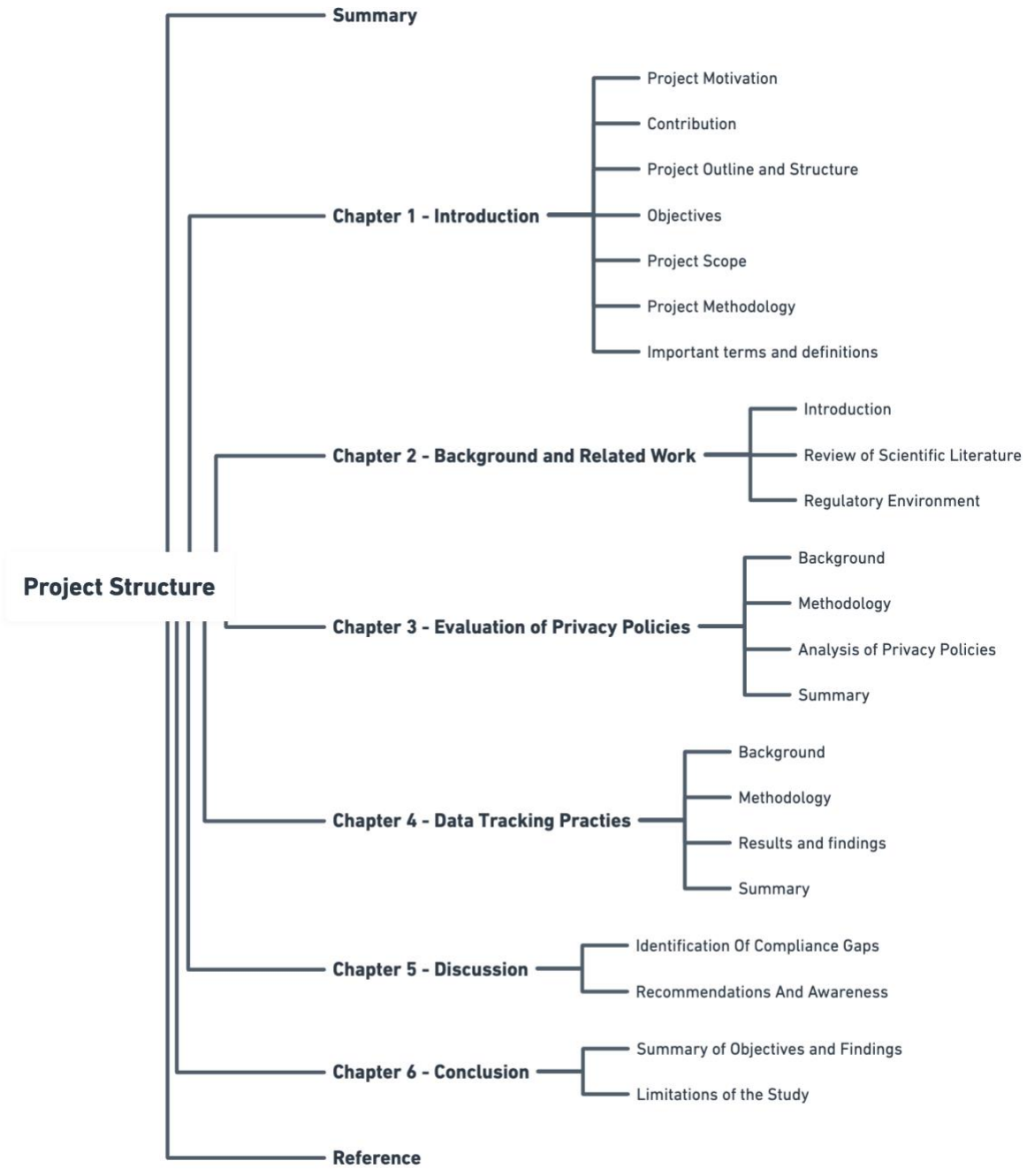



*Figure 1- Project Structure*

## 1.4 Objectives

The primary objective of this dissertation is to evaluate the compliance of popular children's apps with GDPR privacy standards and to assess their data tracking practices. This study aims to achieve the following specific objectives:

| Table 1 of 7 - Objectives | | |
|---|---|---|
| Objective | Description | Chapter |
| 1 | Evaluate the privacy policies of 30 children's apps for GDPR compliance, highlighting strengths and weaknesses. | Chapter 3 |
| 2 | Examine data tracking practices in apps, assess their GDPR compliance, and evaluate the impact on children's privacy. | Chapter 4 |
| 3 | Identify gaps in GDPR compliance in privacy policies and data tracking practices and discuss their implications. | Chapter 5 |
| 4 | Provide recommendations for improving GDPR compliance and enhancing children's online privacy and suggest areas for future research. | Chapter 6 |
| 5 | Summarize key findings, reflect on research objectives, and suggest future research directions. | Chapter 7 |

*Table 1- Objectives*

By achieving these objectives, this dissertation seeks to contribute to the creation of a safer and more privacy-respecting digital ecosystem for children.

## 1.5 Project Scope

This dissertation focuses on the evaluation of privacy-enhancing technologies and GDPR compliance within children's apps available on the Google Play Store. While children's online privacy is a global concern, this study specifically targets apps accessible in the European Union, where GDPR regulations are applicable.

In the comprehensive literature review in Chapter 2, the study acknowledges various aspects of digital privacy and security for children, including general privacy concerns and specific technologies designed to enhance privacy. While there are numerous regulatory frameworks and privacy-enhancing technologies worldwide, the primary focus will be on GDPR and its implementation in children's apps. Other regulatory frameworks such as COPPA will be discussed for context, but they will not be the primary focus.

The project centres on assessing the compliance of selected children's apps with the GDPR's seven core requirements: lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality. The analysis will include a detailed review of the privacy policies of these apps as well as an examination of their data tracking practices using tools like Exodus Privacy.

While this study recognizes the broad scope of privacy issues and tracking practices across various digital platforms, it specifically hones in on mobile applications for children due to their increasing usage and the particular vulnerability of young users. Other related privacy concerns, such as those associated with general internet usage or other types of applications, will not be the primary focus of this research.

Furthermore, the research does not extend to evaluating the technical implementation of privacy-enhancing technologies within these apps or performing a technical audit of app security. Instead, it focuses on the legal and policy aspects of GDPR compliance and the observable tracking behaviours.

The terminology used throughout this work will remain consistent. Terms such as developers, policymakers, and guardians will refer to those responsible for creating, regulating, and supervising the use of children's apps. Privacy, data protection, and compliance will consistently refer to the adherence to GDPR standards and practices.

By narrowing the focus to these specific areas, this dissertation aims to provide a detailed and actionable analysis that can contribute to the development of safer digital environments for children, ensuring their privacy and data protection rights are adequately protected.

## 1.6 Project Methodology

In this section, I detail the methodology I employed in my research on safeguarding children's privacy, with a particular focus on GDPR compliance and tracking assessments. My approach involved a combination of literature review, practical analysis, and evaluation methods to comprehensively assess the privacy practices of selected applications.

### 1.6.1 Literature Review

To build a foundational understanding of GDPR compliance and privacy-enhancing technologies, I conducted an extensive literature review. This review included a wide range of academic sources, focusing on the latest research related to online privacy, particularly for children. I placed a strong emphasis on studies that explore GDPR's core principles, such as lawfulness, accountability, and transparency, as these were critical in evaluating the compliance of the apps in question.

In addition to the GDPR, I also examined literature on the Children's Online Privacy Protection Act (COPPA), although it was used more as a background reference rather than a primary framework for this research. The review of privacy-enhancing technologies provided me with insights into how these tools can help in safeguarding children's data, offering a necessary context for my analysis.

### 1.6.2 Practical Analysis and Evaluation

For the practical component of my research, I selected 30 different children's apps from the Google Play Store. The selection was based on their popularity and relevance to the target demographic. My primary goal was to analyze the privacy policies of these apps to determine their compliance with GDPR standards.

I began by thoroughly reviewing the privacy policies of each app, focusing on the seven core requirements of GDPR: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. Each app was assessed on how well it adhered to these principles, and I assigned individual scores based on my findings. This scoring system was designed to provide a clear, quantitative measure of each app's compliance level.

To confirm my discoveries thoroughly I performed a monitoring evaluation using the Exodus Privacy tool. This software enabled me to examine the tracking methods in the applications and uncover any privacy issues like the existence of trackers that could gather or distribute user data without clear disclosure. The results from this analysis were crucial in understanding the wider privacy implications of using these applications.

### 1.6.3 Document styling, formatting, and referencing.

The report is broken down into chapters and sections to make it easier to read from start to finish.

The stylistic decisions mentioned below have been implemented:

- **Bold** – It is used to highlight chapters and sections making it easier for readers to locate areas for further exploration and discussion. Highlighted phrases and headings serve as markers for discussion points and summaries, within the text.
- *Italic* - Titles of sources and specific terms are italicised.

The choice has been made to utilize the Harvard referencing format for citing sources in this work. This method employs an author date approach incorporating citations, within the text containing the authors name and the year of publication enclosed in parentheses. In instances of quotes the page numbers are also specified. A thorough compilation of references can be found in the Reference List located at the conclusion of the thesis.

## 1.7 Important Terms and Definitions

GDPR – General Data Protection Regulation
COPPA – Children's Online Privacy Protection Act
PETs – Privacy Enhancing Technologies
Apps – Mobile Software Applications

# Chapter 2 – Background and Related Work

In my research work I deeply analyze the literature and regulatory landscape that influence the privacy of children and the use of technology to enhance privacy in accordance with GDPR regulations. I emphasize the need to safeguard children's privacy in today's era of digital advancements by studying previous research related to GDPR and similar laws such as COPPA.I delve into the utilization of tracking technologies, in apps designed for children and present a summary of the regulatory landscape highlighting GDPR and COPPA laws while addressing the hurdles developers encounter in meeting compliance requirements. To conclude, I outline the regulatory learnings paving the way, for examining privacy protocols in the upcoming section.

## 2.1 Introduction

The way young people engage with technology has changed in recent years due to the explosive growth of kid-oriented mobile applications. These applications now play a role in children's daily activities by providing entertainment as well as learning experiences. They encompass a variety of offerings from engaging games to educational aids . However beneficial these child friendly apps may be there are concerns regarding data security and privacy implications. Given their understanding and the delicate nature of their personal information young users are particularly vulnerable to privacy breaches. Personal details like names and addresses well as behaviour patterns of children are considered sensitive information that can be misused if not handled carefully leading to potential risks such, as identity theft or unwarranted surveillance.

A key legislative framework intended to improve data protection and privacy within the European Union is the General Data Protection Regulation (GDPR), which went into effect in May 2018. In line with GDPR guidelines strict rules are set for collecting, handling, and retaining personal information highlighting the importance of transparent consent and effective communication. GDPR adherence, for applications meant for children is not just an obligation but also a moral imperative to safeguard the privacy and well-being of young individuals. App developers have an obligation to ensure that their privacy policies are clear and accessible and give parents and guardians adequate control over their children's data usage rights in compliance with the law. This dissertation aims to uncover industry practices and identify areas, for improvement by examining how popular children's gaming apps adhere to GDPR guidelines through the analysis of their privacy notifications and tracking methods.

### 2.1.1 Importance of Privacy Protection for Children

Safeguard children's privacy in the digital era is extremely important because of their specific vulnerabilities and the increasing hours they spend online. Children lack the understanding of the lasting effects of sharing personal details which makes them susceptible to dangers like identity theft, cyberbullying, and exposure to unsuitable content. Their online activities can be misused for tailored marketing. Influencing their choices and behaviours in ways that may not be clear, to them resultantly impacting their growth and welfare.

Regulations such as the General Data Protection Regulation (GDPR) which's applicable in the European Union and the Children's Online Privacy Protection Act (COPPA) enforced in the United States highlight the significance of safeguarding children's privacy from a legal standpoint. These regulations acknowledge that children need to be shielded due to their limited grasp of privacy risks and emphasize the importance of transparent data collection practices which require parental approval for minors, below specific age limits. The objective of this structure is to ensure that children's rights are upheld and that they are shielded from any potential harm that may arise from certain practices.

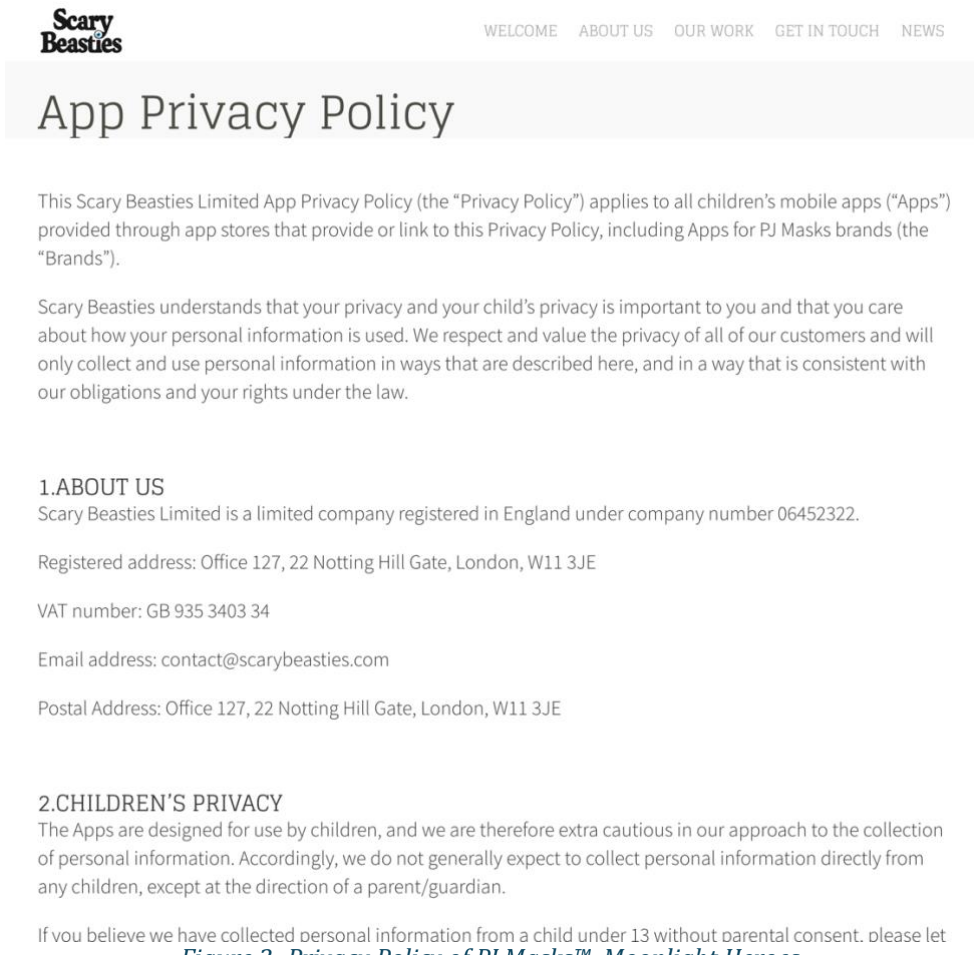
Protecting children's privacy goes beyond following the rules – it's about upholding ethical values that show a society's respect for human dignity and rights. We must ensure that kids have an online space to discover digital tools without putting their fundamental rights at risk. This

involves setting privacy protections in place teaching children, about online risks and promoting responsible digital behaviour. These steps can help children interact safely with technology and nurture their growth and happiness in the run.

### 2.1.2 Privacy Policy

Privacy policies play a role in overseeing personal data use in mobile apps aimed at children specifically. It's vital to communicate the kinds of information gathered and how it's used alongside outlining user rights for apps serving vulnerable groups, like kids a strong privacy policy is absolutely essential. It is essential for these guidelines to be straightforward and easy to understand while also adherent to legal regulations such as the General Data Protection Regulation (GDPR) applicable, in Europe and the Children's Online Privacy Protection Act (COPPA) enforced in the United States.

In this paper, we explore the critical elements that constitute an effective privacy policy for children's apps. We examine the rules set by GDPR and COPPA that focus on ensuring the safety of minor's information. Additionally, we will discuss the importance of getting consent from parents the responsibilities of those in charge of data and the requirements related to informing about data breaches. It's worth noting that a privacy policy serves as more than a legal requirement—it plays a crucial role in building trust, between the provider of the app and its users. By examining the privacy policies of various children's apps, we assess their compliance with these legal standards. This analysis highlights the strengths and weaknesses of existing practices, identifying common areas where apps fall short of regulatory expectations. Through this examination, we aim to underscore the need for rigorous enforcement of privacy policies to ensure that children's digital environments are safe, secure, and respectful of their rights.


Scary Beasties

WELCOME ABOUT US OUR WORK GET IN TOUCH NEWS

App Privacy Policy

This Scary Beasties Limited App Privacy Policy (the "Privacy Policy") applies to all children's mobile apps ("Apps") provided through app stores that provide or link to this Privacy Policy, including Apps for PJ Masks brands (the "Brands").

Scary Beasties understands that your privacy and your child's privacy is important to you and that you care about how your personal information is used. We respect and value the privacy of all of our customers and will only collect and use personal information in ways that are described here, and in a way that is consistent with our obligations and your rights under the law.

1.ABOUT US

Scary Beasties Limited is a limited company registered in England under company number 06452322.

Registered address: Office 127, 22 Notting Hill Gate, London, W11 3JE

VAT number: GB 935 3403 34

Email address: contact@scarybeasties.com

Postal Address: Office 127, 22 Notting Hill Gate, London, W11 3JE

2.CHILDREN'S PRIVACY

The Apps are designed for use by children, and we are therefore extra cautious in our approach to the collection of personal information. Accordingly, we do not generally expect to collect personal information directly from any children, except at the direction of a parent/guardian.

If you believe we have collected personal information from a child under 13 without parental consent, please let

*Figure 2- Privacy Policy of PJ Masks™: Moonlight Heroes*

## 2.2 Review of the Scientific Literature

In this section, I am going to review literature on the relevant topics pertaining to this research. Looking at what other articles say about GDPR and privacy standards as a whole. After that we will examine the research on the areas of mobile software applications (henceforth known as 'apps') for kids and the various concerns on privacy. We also dive deep into privacy enhancing technologies ranging from website extensions to touch interaction patterns, all tailored to mitigate risk improve privacy in the online space.

### 2.2.1 GDPR and Privacy Standards

Introduction and Global Diffusion

The General Data Protection Regulation (GDPR) is a set of rules for handling personal information that came into force on May 25th in the year 2018. It sets out guidelines for how data should be processed and stored for people living in the European Union (EU, 2016). This law was created to enhance the EUs safeguards for information due to the evolving privacy issues brought about by fast paced advancements in digital technology (Li et al., 2019). In my examination of the matter at hand I've discovered that the GDPR isn't a crucial aspect of contemporary data security in the EU but also has greatly impacted privacy regulations worldwide. Serving as a force in globalizing privacy rules the GDPR has established fresh standards for safeguarding personal information influencing approaches, in different sectors and locations.

The significance of the GDPR was emphasized more due to the incident involving Cambridge Analytica that involved unauthorized harvesting of personal information from 87 million Facebook users. This incident heightened worldwide worries about privacy and the idea of "surveillance capitalism " emphasizing the pressing requirement for privacy safeguards. In reaction, to this occurrence Facebook pledged to harmonize its operations with the GDPR on a level (Bennett, 2018). The scandal also revealed the background of information privacy as a significant public policy concern that emerged in the 1960s and 1970s amid worries about government monitoring activities. The apprehensions spurred the creation of data privacy regulations based on principles that have now been adopted worldwide through international agreements, like the OECD Guidelines and the Council of Europe's 1981 Convention.

During the 1990s era emerged the EU Data Protection Directive with a goal to align data protection initiatives throughout Europe and establish a model for norms in this field of regulation. With my exploration into this subject matter, I discovered that the swift technological progress witnessed in the early years of the 21st century gave rise to significant hurdles due to differing interpretations of existing data protection regulations. These obstacles triggered a call for an updated approach. Ultimately paved the way for the inception of the GDPR proposal in 2012 and its subsequent enforcement, in 2018 (Bennett, 2018). Today's GDPR is seen by many as the extensive data protection regulation globally and has the ability to influence more alignment in international policies, on privacy and data protection.

GDPR Certification Mechanisms

In my investigation of the certification methods outlined in the GDPRs Article 42 section which're crucial for ensuring uniform compliance and building trust through privacy certifications and seals, I discovered that these methods serve as important instruments for organizations to showcase their commitment to GDPR regulations. The involvement of Data Protection Authorities (DPAs) is key in this process as they define the standards for certifications and supervise their execution. This oversight does not guarantee a consistent application of GDPR rules, across different regions but also strengthens the responsibility of organizations (Bennett, 2018).
In line with the framework of the GDPR regulations these certification methods blend input from DPAs with the potential for rigorous enforcement striking a harmonious balance in regulatory measures. From my investigations it has come to light that organizations are encouraged to

embrace compliance aids like Data Protection Impact Assessments (DPIAs) and codes of conduct to showcase their dedication to data protection. By obtaining certifications or privacy seals businesses can furnish evidence of their adherence, to regulations, which proves especially beneficial during inquiries (Bennett, 2018).

Furthermore, the co-regulatory framework of the GDPR that I studied closely highlights the significance of collaboration between regulators and businesses. This framework enables DPAs to offer advice and support while still maintaining the power to levy fines for violations. The implementation of certification systems outlined in Article 42 demonstrates the GDPRs strategy, towards data protection. It seeks not to ensure compliance but also to promote the adoption of industry best practices (Bennett, 2018).

Impact of App Stores on GDPR Compliance

During my research into how app stores uphold GDPR regulations compliance standards and regulations I discovered that app stores play a role, in making sure that mobile apps follow the transparency and accountability rules required by the GDPR law. Acting as overseers of sorts, app stores. Uphold rules that give importance to these specific requirements thus promoting an environment that values safeguard of data and privacy within the mobile application network (Krämer, 2024).

App stores play a role in enforcing GDPR compliance by setting out rules and recommendations that app creators need to adhere to for ensuring openness in how they handle data. These platforms are essential for ensuring that developers meet GDPR standards concerning user consent and data handling transparency in privacy policies. By implementing these guidelines and review procedures by app stores encourages developers to enhance the transparency of their data management practices which leads to users having control, over their personal information (Krämer, 2024).

I've found that developers encounter significant obstacles in adherence, to the GDPR guidelines enforced by app stores as well. These hurdles involve understanding legal obligations creating straightforward and precise privacy policies securing legitimate user consent and establishing strong data protection protocols. It is imperative for developers to tackle these challenges in order to fully comply with GDPR rules and uphold transparency and accountability in their data handling procedures. Since October 2018 it has been mandatory for developers to include a privacy policy link when releasing or updating an app on the Apple App Store. The same requirement has been in effect on the Google Play Store for apps handling information since July 2016 and for all apps on the Play Store, from the second quarter of 2022 (Frey, 2021).

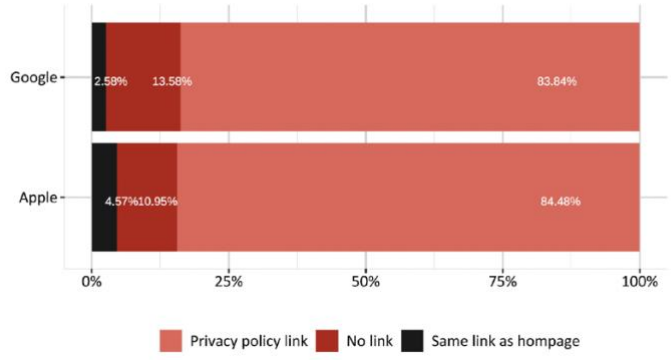



*Figure 3- Apps with privacy policy (Krämer, 2024).*

In Figure 3 its noted that certain developers attempted to avoid the requirement of sharing a privacy policy by using the link as their developer homepage. Despite the GDPR being in effect

since 2018 many apps continue to fall of informing users about how their data is being handled; this is evident, from the number of apps lacking a privacy policy link (Krämer, 2024).

In the realm of app development and data privacy regulation like GDPR compliance stands out in importance for app creators as app stores act as enforcers of transparency and responsibility standards in this regard. Despite their role in upholding data security and privacy principles developers often face hurdles when it comes to meeting these requirements by tackling these obstacles head on and collaborating closely with app stores to boost GDPR adherence developers can play a part in fostering a more privacy oriented landscape, for smartphone applications that puts user rights and data safeguarding at the forefront.

Perceptions of GDPR Implementation

During my research into how people view General Data Protection Regulation (GDPR) after experiencing it firsthand I looked at a study that surveyed employees who stayed at their companies through GDPRs implementation and beyond to see what they thought about its costs and benefits as well as its overall impact, on their work environment (source; Buckley et al. 2024).

| H7 Questions | Strongly disagree | Disagree | Mildly disagree | Neither agree or disagree | Mildly agree | Agree | Strongly agree |
|---|---|---|---|---|---|---|---|
| GDPR means makes me feel more in control of personal my data | 2.0% | 3.9% | 3.9% | 14.7% | 9.8% | 42.2% | 23.5% |
| GDPR is good for the consumer | 1.0% | 1.0% | 1.0% | 8.8% | 4.9% | 46.1% | 37.3% |
| GDPR is good for my company | 0.0% | 0.0% | 5.9% | 28.4% | 6.9% | 45.1% | 13.7% |
| On balance, GDPR is worth it | 1.0% | 1.0% | 4.9% | 13.7% | 5.9% | 50.0% | 23.5% |

*Table 2- Questions relating to the main research question: 'do you think it is worth it?'(Buckley et al., 2024)*

According to the data in Table 2 and observations made during the study's interviews with participants reveal that while most individuals demonstrate awareness of their rights as outlined in the GDPR when reminded of them; however, their understanding regarding the authority overseeing data protection remains somewhat limited, in scope. Moreover, though this limitation exists participants do acknowledge shifts taking place within their respective organizations concerning data management procedures. Signifying an acknowledgment of the compromises necessary to adhere to regulatory standards. Many individuals mentioned that they felt comforted knowing that their own data is handled with a degree of attention as that of their employer's client's data The general sentiment towards GDPR appears positive, among those tasked with complying with its rules (Buckley et al., 2024).

Moreover, the research indicates that employees view the GDPR as advantageous not for their personal privacy but also for their organizations. This positive perspective differs from the negative portrayal of regulatory adherence. The favorable response implies that the GDPR is appreciated for its contribution, to improving data security protecting privacy rights and promoting accountability within companies. The results highlight how crucial it is to make use of this employee assistance and incorporate their input to enhance GDPR continuously so that it can effectively influence data procedures and maintain privacy regulations (Buckley et al., 2024).

In conclusion, this study's findings reveal perspectives from individuals directly involved in the execution of GDPR guidelines. It delves into the shifts in data management strategies acknowledgment of privacy entitlements and the dilemmas that companies encounter. The research confronts prevalent pessimism linked to adherence, to regulations shedding light on

GDPRs advantages in fostering ethical data management and emphasizing its crucial function in safeguarding privacy amid the contemporary digital realm.

### 2.2.2 Children's Apps and Privacy Concerns

Children's Privacy Concerns in Digital Environments

In today's age and the era of mobile apps specifically for children's use; the issue surrounding the privacy of children has garnered more awareness and concern recently. Given the risks that children encounter online platforms pose in terms of personal data security; safeguard measures have now become increasingly crucial. Regulatory standards such as the General Data Protection Regulation (GDPR) play a role in ensuring the safety of these vulnerable demographics by outlining clear rules and criteria for data protection and privacy in digital realms (Department for Science, Innovation and Technology, 2021).

The issue of children's privacy is becoming more concerning due to the reliance of services that children use regularly on personal data as a core component. Thinking about how one out of every five internet users in the UK's a child emphasizes the importance of safeguard Children enjoy their online experiences while ensuring that their personal information remains secure. Complying with data protection regulations isn't about following the law; it also shows a commitment, to valuing and safeguard children's privacy appropriately. This strategy helps establish confidence with parents and users by guaranteeing that online services cater to children's needs in a secure and suitable manner. The General Data Protection Regulation (GDPR) accentuates the significance of safeguarding children's information through its guidelines and is a key focus for entities such as the Information Commissioner's Office (ICO) responsible for ensuring compliance, with these responsibilities. Failure to comply could result in regulatory measures such as penalties and limitations on data handling to tackle violations of the UK GDPR guidelines (Department for Science, Innovation and Technology, 2021).

In essence this conversation underscores the importance of regulatory guidelines like GDPR in protecting children's personal information in the digital realm particularly when it comes to mobile applications. By following these data protection rules and setting up privacy measures companies can establish a safer online space, for kids guaranteeing that their privacy is valued and shielded effectively.

Age-Appropriate Design and Data Protection

The paper discussing "Information technologies putting children at risk of privacy exposure" explores the practices outlined in the Age Suitable Design Code and its core values that influence the development of applications that safeguard childrens privacy. This code highlights the significance of creating services like apps with a focus on what is best for children while guarantee that they are suitable, for their age group and prioritize their privacy rights (Crepax et al., 2022).

The Code of Practice for Designing Apps for Kids emphasizes guidelines that developers and creators should follow to create kid friendly apps. These guidelines involve prioritizing the well-being of children in app design decisions and setting privacy settings to high as a default option. It also involves collecting necessary data and presenting clear information about data practices in a way that is easy for children to understand and ensuring top notch data protection and security standards are maintained (Department for Science; Innovation; Technology & Department, for Digital Culture Media & Sport, 2021). By adhering to these guidelines and standards developers of applications can establish a secure and privacy aware online setting, for kids.

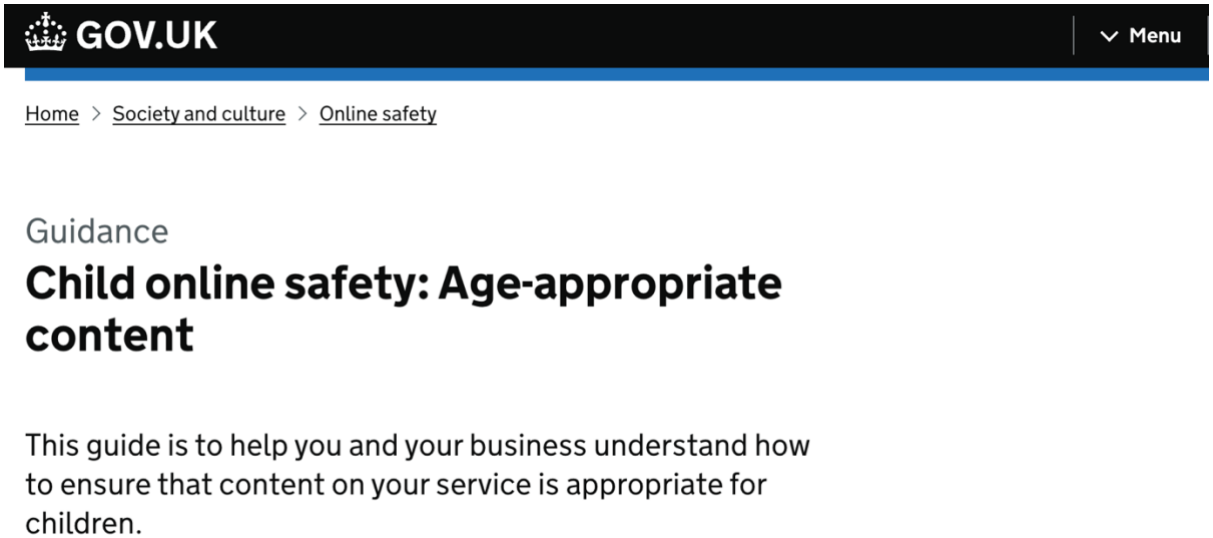



*Figure 4- An Age-Appropriate content guide posted by the UK Government ( Department for Science, Innovation and Technology and Department for Digital, Culture, Media & Sport, 2021).*

In addition to that point is the importance of performing Data Protection Impact Assessments (DPIAs) as they're crucial for evaluating the risks linked to how data is managed in applications aimed at childrens use. DPIAs play a role, in recognizing and addressing possible privacy concerns at an early stage of developing an app to guarantee that childrens personal information is dealt with in a responsible and secure manner. By performing Data Protection Impact Assessments (DPIAs) developers can actively tackle privacy issues in advance. This approach helps adhere to data protection laws such as the GDPR. Emphasizes safeguarding childrens privacy in online settings (Department for Science and Innovation and Department, for Digital Culture Media & Sport, 2021).

The guidelines outlined in the Age-Appropriate Design Code of Practice offer insights, on developing apps that uphold childrens privacy rights by following essential principles that prioritize the well-being of the child. It is crucial to conduct Data Protection Impact Assessments (DPIAs) to evaluate and address risks related to data management in apps for children while ensuring that their personal information is handled in a way that protects their privacy and enhances their online safety.

Data Handling and Commercial Features in Children's Apps

The assessment of how data's managed and the business aspects present in apps for kids involves a thorough review of practices gleaned from different research studies and content analyses It sheds light on the significance of adhering to GDPR regulations and highlights the importance of improving supervision and design methods These investigations delve into how children's apps handle collecting data and utilizing it as well as sharing it along, with the economic features integrated into these virtual platforms. Through an examination of these factors in the study conducted by Jib et al. the research points out possible privacy concerns and areas where adherence to GDPR guidelines might be lacking This sheds light on ways to better protect children's personal data and maintain transparency, in managing data practices (Jibb et al., 2022).

| | Privacy policy | | Social media | | Permissions requested | | Data security | |
|---|---|---|---|---|---|---|---|---|
| | Methods | Results | Methods | Results | Methods | Results | Methods | Results |
| Bry *et al*[43] | Evaluated app store page and/or downloaded app manually | *Privacy policy presence:* Less than 5% of apps | | | | | Evaluated app store page and/or downloaded app manually | *Login and/or password presence:* Less than 5% of apps |
| Cheng *et al*[24] | | | | | | | Evaluated app store page and/or downloaded app manually | *Investigator-developed security assessment scale:* 6% of apps rated as excellent; 10% of apps rated as good |
| Das *et al*[20] | Statistics calculated with web-based readability calculator | *Privacy policy readability:* average reading grade level (12.8) higher than average US adult level (8.0) | | | | | | |
| Liu *et al*[22] | | | Comparison of app library package names with libraries relevant to social networks | *Potential for social medial sharing:* 20% of apps | Examination of privacy grade as listed in online crowdsourced dataset | *Potential for permission requests:* 82% of apps use few permissions for unusual purposes; 10% may use permissions in this way | | |
| Meyer *et al*[23] | | | Evaluated app store page and/or downloaded app manually | *Social media links:* 14% of apps | Evaluated app store page and/or downloaded app manually | *Permission requests:* 100% of apps Requests for notifications (100%), files/photo storage (53%), phone (13%), microphone (8%), camera (7%); and location (4%). | | |
| Musgrave *et al*[50] | | | | | | | Evaluated app store page and/or downloaded app manually | *Login and/or password presence:* 90% of apps required logins; 70% required passwords |
| Reyes *et al*[18] | | | | | | | Automated analysis of whether data transmissions are protected | *Data encryption:* 40% of apps do not use TLS* |

*Table 3- App privacy-related and security-related evaluation methods and results (Jibb et al. 2022).*

When looking into GDPR compliance in relation to children's apps adherence to the guidelines set by the regulation is evident through these assessments The GDPR emphasizes the importance of handling children's personal data with care and requires explicit consent for any processing activities involving minors. Any deficiencies, in compliance found in how these apps handle data not only pose privacy risks but also have potential legal ramifications. It appears that certain applications might adhere to the GDPR standards while others could fall short in critical aspects and place children at risk of unnecessary privacy vulnerabilities.

The study highlights the requirement for stricter regulatory supervision and stronger design approaches in creating apps for children's use They stress the importance of enhanced oversight to guarantee compliance with data protection laws and to prioritize the privacy rights of young users through measures such, as regular audits and enforcement actions. In addition, to this the implementation of enhanced design strategies. Like incorporating privacy focused design principles and creating functionalities that cater specifically to the requirements and comprehension of children - can greatly enhance the privacy and security of children's interactions.

In summary the characteristics of commerce and the ways data is managed in apps for kids emphasized in these studies underscore the need to ensure that app development adheres to GDPR regulations. The results support the need for supervision and enhanced design strategies to safeguard children's privacy mitigate privacy threats and encourage responsible data handling, in the digital spaces where children now spend a significant amount of time.

Involving Children and Parental Perspectives in Privacy Design

The study highlights the significance of including kids and parents in creating privacy settings to understand the advantages of a user focused strategy that considers economic backgrounds (Dempsey et al., 2022; Amâncio et al., 2023). Involving children, in the design phase enables developers to customize privacy options based on the requirements and viewpoints of young users to ensure that the controls are easy to use and efficient.

When kids help create privacy alerts and settings themselves, they learn more about rights and the impact of sharing data online. This interactive method gives them a sense of control, over their activities and helps them understand privacy safeguards better (Dempsey et al., 2022). Also, when kids are part of shaping these tools they are more apt to grasp and utilize them well resulting in privacy protection.

Parental participation is extremely important in guiding childrens use of technology and online platforms. Parental views regarding privacy are shaped by economic factors and greatly impact how privacy safeguards are put into practice within the family environment (Amâncio et al. 2023). In societies that value data protection highly, parents tend to be more attentive, in monitoring their childrens behavior and advocating for stricter privacy measures.

Economic inequalities also affect issues with privacy and the enforcement of rules and regulations well. In countries, with incomes the lack of technology and resources can make it difficult to establish strong privacy safeguards, which could put children at higher risk (Amâncio et al., 2023). These obstacles underscore the importance of promoting privacy awareness and education initiatives that are specifically designed for cultural and economic settings.

Developers and policymakers can craft privacy solutions by taking into account the viewpoints of children and parents as well as considering cultural and economic differences. This method does not boost safeguarding childrens privacy but also promotes the growth of digital skills and responsible online conduct, in various settings.

In addition to that the privacy policies in apps and websites, for children are usually not easy to find or understand enough as they are often hidden in hard to find sections or presented in formats that are not user friendly (Jibb et al., 2022). To resolve these problems, it is suggested that privacy policies should be shown prominently and might benefit from using features or visual tools to involve users and improve their comprehension of how data is managed.

To sum up the discussion on safeguarding childrens privacy in the age demands a combination of tech solutions and educational programs along with thorough scrutiny of privacy regulations signifies the diverse strategy essential for this cause to be successful. Encouraging skills acquisition advocating for clear privacy policies and adhere compliance with legal requirements can collectively establish a safer and more protected online space, for children thereby appropriately upholding their privacy rights.

Conclusion: Implications for Future Research and Policy

This section outlines the obstacles and prospects in protecting childrens privacy by highlighting the importance of ongoing research and advancements in policies regarding the matter. As technology progresses and children engage more with platforms it is essential to enhance privacy safeguards to tackle issues like data breaches, unauthorized data gathering and personalized

advertising (Zhao et al., 2022). Continuous research is critical, for pinpoint privacy risks and shaping impactful policies that uphold childrens rights in this digital era.

Concern about issues in targeted advertising is still prevalent in the discussion. Evaluating childrens activities through targeted advertising poses critical inquiries regarding privacy of data manipulation and the possible negative effects on childrens welfare (Zhao et al., 2022). It is crucial for advertising strategies to give priority to the well-being of children by guaranteeing transparency and fairness while complying with regulations such, as COPPA to safeguard young viewers.

Understanding how to use technology safely is important for kids to navigate the world securely and confidently. Youngsters can learn about privacy risks. Gain the knowledge to make wise choices on the internet through digital literacy programs. This education helps children safeguard their privacy rights and stand up for themselves in the realm (Zhao et al., 2022). Teaching kids about staying online and protecting their data is crucial, for developing responsible digital citizens who can withstand online dangers.

To sum up the situation regarding childrens privacy concerns; it is essential to adopt a strategy involving ethical advertising methods and strong policy frameworks alongside educating about digital literacy comprehensively. By focusing on these aspects collectively stakeholders can strive towards establishing a digital space that safeguards childrens welfare and respects their privacy entitlement in today's digital landscape.

### 2.2.3 Data Tracking Practices

Introduction

The study delves into the connection between how data is monitored in mobile applications and ensuring adherence to privacy rules like GDPR (Kollnig, 2021). Many app creators share user information with companies for tasks like ads and behaviour analysis without clear user consent raising serious privacy issues and highlighting the importance of being transparent and obtaining informed consent under regulations such, as GDPR.

The research mainly looks into how app developers let users know about their data practices through to understand privacy policies before collecting data (Kollnig, 2021). It probably investigates what's, in these policies. If users are well informed about data collection and if the policies comply with GDPR rules. Moreover, the study could analyze how tracking methods differ between platforms such as Android and iOS as well as between free and paid applications and various regions, like the EU compared to non-EU countries in order to emphasize the diverse privacy practices and regulatory hurdles on a global scale.

According to regulations that prioritize transparency and obtaining user consent legally to protect data privacy standards outlined in GDPR compliance laws (Kollnig, 2021) research likely indicates that numerous app creators may not meet these requirements entirely as expected. Placing users at risk of data gathering and distribution issues. This non-compliance situation underscores how difficult it remains to guarantee that privacy guidelines are not just available but also easily understandable and truly mirror real world data handling procedures.

To sum up the findings of the papers suggest that privacy policies play a role in overseeing how data tracking is handled in mobile applications with a specific focus on GDPR adherence. They also highlight the complexities in ensuring transparency and safeguard user information on a scale across various locations and platforms. Through examining these aspects, the study offers perspectives into the wider conversation about online privacy enforcing regulations and the necessity, for ongoing policy updates to address changing privacy threats.

Analysis of Privacy Policies and Data Sharing

The study delves into the privacy guidelines of applications by looking at how these documents reveal information about sharing data and tracking methods by third parties (Mehrnezhad, 2020). It evaluates the clarity of these guidelines in informing users about data collection and the risks involved with it. The results show a difference in how clearly privacy policies convey information about data sharing and tracking processes while underscoring the persistent difficulties, in user awareness and understanding.

| Position | | PC Browser | Mobile Browser |
|---|---|---|---|
| Bottom | Overall | 43% | 48% |
| | Right | 5% | 1% |
| | Left | 2% | - |
| Middle | Overlay | 22% | 11% |
| | In-page | 1% | 1% |
| Top | Overlay | 7% | 2% |
| | In-page | 11% | 8% |
| Full-page | | - | 20% |
| No notice | | 9% | 9% |

*Table 4- Privacy Notice User Control Options in Top 116 Eu Websites, Pc Vs. Mobile (Mehrnezhad, 2020).*

| Position | Android App |
|---|---|
| Full-page | 16% |
| Middle | 8% |
| Bottom | 7% |
| Top | 1% |
| No notice | 51% |
| Left behind log-in | 17% |

*Table 5- Privacy Notice User Control Options In 101 Corresponding Android Apps (Of 116 Eu Websites) (Mehrnezhad, 2020).*

One important focus of the study involves examining how privacy measures differ among platforms like Android and iOS as well as between regions such as the EU and non-EU countries. This contrast highlights variations in the enforcement of data security protocols and levels of adherence to GDPR within geographical and technological contexts. These disparities create difficulties, for individuals seeking to understand and manage their privacy rights amidst a landscape that is not uniform throughout.

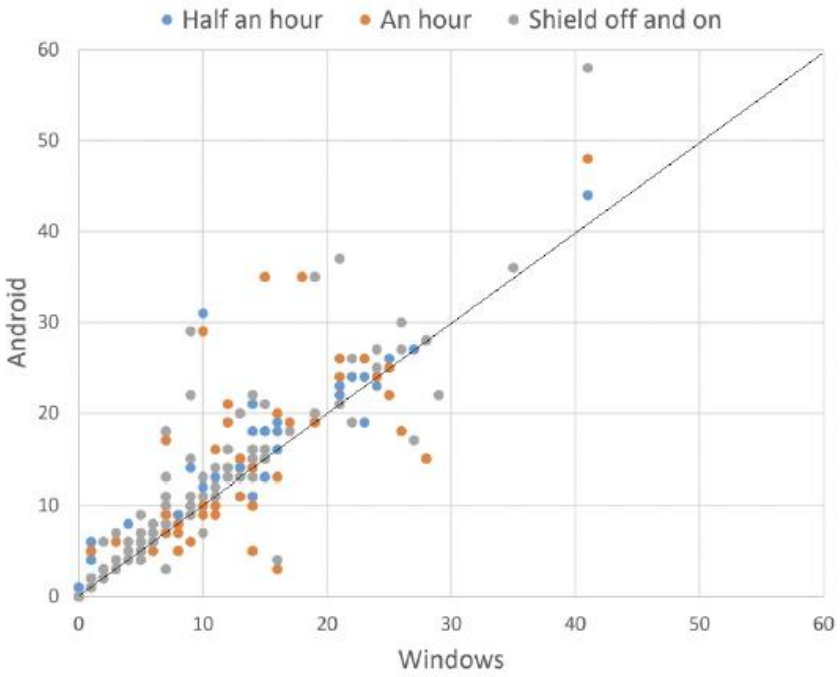



*Figure 5- Scatter chart of tracking activities blocked by Brave in Windows vs. Android in three different test conditions for 116 websites (Mehrnezhad, 2020).*

Furthermore, the research highlights the challenges that app developers and regulators encounter in adhering to GDPR regulations especially when dealing with privacy measures and regional regulations (Mehrnezhad, 2020). The results indicate that upholding data protection protocols necessitates not just precise regulatory directives but also technological innovations and user centric resources, for improving clarity and empowering users.

In summary of the study findings reveal information about the difficulties of following GDPR regulations within mobile applications specifically related to sharing data and tracking by third parties. The research emphasizes the importance of communication increased user control and standardized privacy information contributing to the wider conversation on safeguard personal information and enforcing regulations, in mobile platforms.

Impact of GDPR on Data Tracking Practices

The introduction of the General Data Protection Regulation (GDPR) brought about a change in how data tracking is handled in the realm of mobile applications. Prior to GDPR coming into effect lack of clarity regarding data tracking practices was common; app developers frequently shared user data with parties for advertising and behaviour analysis without full disclosure to users concerning these practices contributing to increased privacy concerns and a general lack of awareness among users, about the extent of their information being monitored (Kollnig, 2021).

Following the GDPR implementation post its enforcement aimed at ensuring transparency and user control by requiring app developers to offer explicit privacy policies and secure user consent before gathering data hasn't been consistently followed through as expected. Surveys indicate that despite the existence of GDPR rules potential data sharing with parties commonly occurred when users just viewed the privacy policies page suggestive of persistent hurdles, in achieving complete compliance with regulations (Kollnig, 2021). It seems that even though there has been some progress made in this area there are still issues, with how privacy policies are enforced and how user data is handled.

The development of data monitoring methods within the scope of GDPR illustrates advancements alongside challenges too visible to ignore. Despite the growing focus on openness and approval in this area numerous software designers are still grappling with achieving harmonization, between their methods and the stipulations of GDPR. This struggle encompasses difficulties associated with data encryption, communication of data sharing practices and prompt responses to user queries regarding data management (Kollnig et al., 2021). The persistent lack of clarity, in areas highlights the importance of continual initiatives to enhance data security measures and guarantee that users are adequately informed about the utilization of their data.

Ultimately even though GDPR has brought about shifts in data monitoring methods there are still major hurdles in meeting complete compliance and openness. The study emphasizes the necessity for watchfulness and enhancement in privacy procedures emphasizing how vital it is for users to be informed and responsible, in protecting their personal information within the mobile application environment.

Cross-Platform Privacy Evaluation and Global Tracking Practices

The study probably delves into the intricacies of privacy disclosures and tracking methods on online platforms with special attention to mobile devices environment. It investigates how privacy permissions are displayed to users and the choices they have in managing tracking processes. It points out differences in privacy procedures and adherence to laws such, as the GDPR (Kollnig, 2021).

One important part of the study focuses on comparing privacy notifications across platforms, like PCs web browsers and mobile apps to see how they are presented and what messages they convey to users alike. Furthermore, the study probably assesses how well Privacy Enhancing Technologies (PETs) and privacy notifications on platforms are working in maintaining user trust and safeguarding data while pinpointing disparities that could erode user confidence, in data protection.

The research on a global scale explores how mobile tracking systems function intricately with a focus on third party advertising and tracking services that are widely used in this ecosystem. It highlights the connections that facilitate data sharing practices and uncovers how app developers partner with third parties to gather and assess user data. This intricate web of data exchange and collaboration raises privacy issues particularly when users are oblivious, to being monitored (Mehrnezhad, 2020).

The study also emphasizes how privacy laws like GDPR have an influence on how data is shared and tracked online. Even though there are rules in place that require companies to be clear about data sharing and get consent from users many apps still share information, with companies when users check privacy policies. This situation shows why we need enforcement of regulations and more transparency to make sure users can manage their personal information when using mobile apps (Kollnig, 2021).

In summary studying both platform privacy assessments and global tracking practices provides valuable insights into the difficulties of ensuring transparency uniformity and adherence to data protection regulations. The research contributes to the conversation, on protecting user privacy and maintaining data security standards in today's intricate digital environment by analyzing privacy policies tracking behaviours and the business aspects of data sharing.

Conclusion and Future Directions

The study highlights the difficulties in overseeing data tracking practices on online platforms due to issues with privacy notifications and user control features not being consistent enough The research shows that there are notable deficiencies, in following GDPR rules especially regarding

how transparent data collection and user consent procedures are These disparities create significant challenges in adequately protecting user privacy (Kollnig, 2021).

To tackle these concerns mentioned in the documents emphasize the importance of monitoring and improving privacy policies over time is crucial to guarantee that online services comply with changing regulatory requirements and enhance user safety measures effectively in place This ongoing process is vital for addressing the deficiencies, in existing privacy procedures and ensuring that data monitoring is carried out openly and responsibly (Mehrnezhad, 2020).

In the future of us lie numerous paths for further exploration as indicated by the study's findings. Such as advancing Privacy Enhancing Technologies (PETs) establishing consistent privacy protocols across various platforms and investigating the effects of new technologies on mobile data tracking practices. By delving into these research areas and avenues like this we can enhance privacy measures significantly. Empower users to better manage their personal information (Kollnig, 2021).

Furthermore, it's crucial to emphasize the significance of educating users when it comes to safeguarding data privacy. Teaching users about tracking methods potential risks involved and their entitlements under data privacy regulations is essential for enabling them to make choices. Through promoting a culture that values privacy efforts in user education can play a role, in establishing a digital space that is both respectful and transparent (Mehrnezhad 2020).

To sum up the matter at hand; dealing with the issues surrounding data tracking necessitates a strategy that involves continually improving privacy policies and embracing new technologies while also educating users effectively.

### 2.2.4 Privacy Enhancing Technologies

In today's world where kids are taking part in online activities regularly، protecting their privacy and safety has become a top priority، The rise of various online platforms and ever-changing cyber risks highlight the need, for strong actions to secure childrens privacy online (Zhang-Kennedy et al., 2017). Privacy enhancing technologies (PETs) seen as a solution to address this pressing issue. They provide solutions designed to reduce risks and support children and parents in navigating the challenges of the internet world (O'Hara, 2022).

In this part of the exploration into landscape geared towards safeguard childrens online privacy is a focus on five important research studies and their goal to highlight the importance of PETs in enhancing childrens online safety and propose ideas for future research and advancements, in this field.
The literature reviews chosen for inspection showcase viewpoints and methods in tackling the complex issues surrounding childrens privacy online ranging from suggesting child friendly browser add-ons to creating rating systems for Internet connected toys (IoToys). Each study provides perspectives on how Privacy Enhancing Technologies (PETs) are shaping the realm of digital safety, for children.
Given this context it aims to offer a summary of current PET solutions highlighting their features advantages and drawbacks It also aims to emphasize the crucial role of PET in creating a secure online space for kids enabling them to explore digital realms, with self-assurance and strength.
This literature review aims to add to the existing knowledge on tools, for safeguarding childrens privacy by analyzing research findings and insights to guide future studies and policy efforts aimed at enhancing children digital safety.

### 2.2.5 Children Online Privacy

**Child Safe Browser Extension** (Alhossen et al., 2021).This paper introduces a child-safe browser extension aimed at shielding children from inappropriate and potentially harmful online content. Leveraging machine learning algorithms, the proposed extension aims to detect and either block or blur violent and adult images encountered during internet browsing sessions. The rationale behind the proposal stems from the recognized risks posed by exposure to such content on children's psychological and emotional well-being, highlighting the limitations of existing solutions like parental controls and safe search engines.

The implementation strategy for the proposed system involves a three-step process: image collection, testing, and action based on the outcomes. Initially, a web scraper retrieves all images from a webpage, which are then processed by a trained machine learning algorithm, specifically a Convolutional Neural Network (CNN), to identify inappropriate content. Subsequently, the system takes appropriate measures to either block or blur the identified images.

The authors envision the extension to be hosted in a cloud environment, facilitating faster operation with minimal impact on browser performance. Emphasizing its lightweight and user-friendly design, the proposed system aims to outperform traditional solutions utilizing machine learning algorithms.

While acknowledging limitations such as the inability to detect more complex inappropriate content, such as sexually suggestive advertisements, the paper concludes that the proposed system represents a significant stride towards enhancing children's online safety. It asserts that with further refinement, particularly through the adoption of more sophisticated machine learning models, the proposed extension holds promise in providing a safer browsing environment for children.

Evaluation of the Effectiveness and Usability of the Proposed Extension

The thesis provides an evaluation of the proposed extension's effectiveness in detecting adult and violent images and the accuracy of its prediction results by the machine learning algorithm. Experimental findings indicate an accuracy rate of approximately 85% in detecting such images, suggesting the extension's capability to mitigate exposure to harmful content.

However, while the paper offers insights into the extension's performance, there is a lack of evaluation regarding its usability in real-world scenarios. A comprehensive assessment encompassing factors like installation ease and effectiveness in blocking or blurring inappropriate content would enhance the understanding of the extension's practical utility.

Discussion on Potential Enhancements or Integration with Existing PETs

The proposed child-safe browser extension presents a significant advancement in protecting children from online risks. While it operates independently, there are possibilities for combining existing PETs in a way that strengthens online safety in a comprehensive manner. For instance, integration with parental control software could augment the extension's capabilities, offering parents a holistic set of tools to monitor and regulate their children's online activities. Additionally, refining the image recognition algorithm using advanced machine learning techniques like CNNs could enhance detection accuracy.

Moreover, expanding device support to encompass mobile platforms would extend the reach and impact of the extension, catering to the diverse digital needs of modern families.

In summary, while the proposed child-safe browser extension represents a commendable effort in bolstering children's online privacy and safety, potential enhancements and integration with existing PETs could further enhance its efficacy and reach in safeguarding children online.

**Children designing privacy warnings** (Dempsey et al., 2022). The study "Children Designing Privacy Warnings: Informing a Set of Design Guidelines" endeavors to tackle concerns surrounding children's online safety by exploring how children can design warning messages related to online privacy. Conducted with 141 UK-based school children aged between 7 and 13,

the study tasks participants with creating privacy warning messages using personas and privacy risk scenarios.
Results indicate that children are capable of designing privacy-related warning messages for others. Through qualitative content analysis, common characteristics in the designs emerge, culminating in the development of design guidelines. These guidelines emphasize the importance of capturing attention, clarity of language, separation from the action intervened, and the use of appropriate visuals (Dempsey et al., 2022).
The research contributes a set of design guidelines informed by children, intended to assist designers in crafting effective online safety interventions. These guidelines underscore principles such as attention, knowledge dissemination, and compliance, facilitating children's mindful decision-making regarding data disclosure.
Overall, the study offers valuable insights to designers tasked with creating privacy warnings for children. It emphasizes the significance of crafting age-appropriate and comprehensible warnings to empower children in making privacy-conscious choices, thereby fostering safer digital environments.

Examination of the Developed Design Guidelines and Their Applicability
The developed design guidelines provide crucial insights for designers aiming to create privacy interventions for children, focusing on preventing the disclosure of personal information online. The guidelines encompass key principles:

**Attention:** Warnings should attract children's attention through engaging design and messaging, ensuring readability from a distance.
**Knowledge:** Providing basic information allows children to comprehend privacy issues, utilizing teaching methods aligned with children's cognitive abilities.
**Compliance:** Warnings must prompt action, offering clear recommendations and practical tips accompanied by pictorials and stories to aid understanding and compliance.

Applicability of the guidelines extends to various digital settings where children provide personal information, such as internet browsers or social media platforms. By adhering to these guidelines, designers can equip children with the knowledge and tools to navigate online privacy risks effectively (Dempsey et al., 2022).

Consideration of How These Guidelines Can Inform the Design of PETs for Children's Online Privacy
The guidelines offer valuable insights for designing Privacy-Enhancing Technologies (PETs) tailored to children's online privacy. PET designers can leverage these guidelines in the following ways:
**Attention Component**: Employing engaging graphics and popular characters to capture children's attention within PETs.
**Knowledge Component**: Delivering concise messages in child-friendly language, supplemented with relatable examples to enhance understanding of privacy risks.
**Compliance Component**: Communicating clear instructions using understandable language and digital imagery to prompt compliance and mitigate risk-prone behaviors.

Separation from the Action Intervened: Ensuring warnings are perceived as external advice and do not interfere with user activities.
Integration of these guidelines throughout PET development stages can enhance accessibility and comprehension, ultimately contributing to the effectiveness of PETs in safeguarding children's online privacy.

**Child Shield: A rating system for assessing privacy and security of internet of toys** (Allana et al., 2021). The paper introduces a methodology for evaluating the privacy and security of Internet of Things (IoT) toys, proposing a rating system named ChildShield to convey these ratings to consumers. It highlights the absence of a standardized labelling system for the internet safety of toys as a significant concern. Through the collection of 12 Internet of Toys (IoToys) available on the market and a review of literature, the authors identify factors influencing IoToys' privacy and security. The proposed rating system categorizes IoToys' overall rating using four colours and employs a QR code to direct consumers to a webpage outlining the scoring methods. However, the proposed rating system lacks testing to assess its effectiveness in informing consumers or influencing manufacturers' practices. Although future research may include studying user acceptance, plans for such research remain unclear. Moreover, there is no indication of collaboration with regulatory entities to integrate privacy and security checks into IoToy design. Additionally, the paper does not advocate for a holistic measure of trustworthiness encompassing both privacy and security. While a labelling system aids communication of essential aspects, it may not guarantee product safety.

Evaluation of the Methodology and Effectiveness of ChildShield in Assessing IoToys' Privacy and Security

The methodology for assessing IoToys privacy and security appears robust, incorporating a literature review and the collection of popular IoToys. Nine factors influencing IoToys' privacy and security are identified, and a rubric is developed to assess each factor, resulting in an overall score. However, ChildShield's effectiveness in informing consumers and shaping manufacturers' practices remains untested. While it may assist parents in informed purchasing decisions, it cannot guarantee product safety. The absence of a global safety standard and non-uniform internet safety regulations further complicate matters. Additionally, evaluation of interoperability and dependence among IoT devices and networks is overlooked, adding complexity to privacy and security concerns.

Discussion on the Potential Integration of ChildShield into Existing PET Frameworks

Integrating ChildShield into existing Privacy Enhancing Technology (PET) frameworks could enhance its usability and effectiveness. PET frameworks aim to protect individual privacy while enabling data sharing or collection for specific purposes. ChildShield's inclusion within these frameworks could serve as a complementary privacy tool for IoT applications. By contributing to product classification based on privacy and security, PET systems may aid compliance efforts and ensure IoToys' safety. However, it should be noted that ChildShield's rating system only addresses privacy and security factors and does not fully cover regulatory compliance issues. As such, its integration into PET frameworks should complement other privacy-enhancing tools and regulatory requirements necessary for comprehensive data protection.

**POCKET: A tool for protecting children's privacy online** (Bélanger et al.,2013). The POCKET framework offers a novel and legally sound solution for automating compliance with the Children's Online Privacy Protection Act (COPPA). It provides parents with an intuitive interface to configure privacy choices for their children and subsequently enforces these policies on the client machine. Developed with careful consideration of legal and technical requirements, POCKET integrates the Privacy Preference Platform project (P3P) framework for storing and enforcing privacy preferences securely. It follows a phased approach, including registration, installation, transaction, and post-transaction phases, ensuring a comprehensive solution for COPPA compliance. Moreover, POCKET addresses the behavioural environment by offering user-friendly interfaces and maintaining activity logs for accountability.

Overall, POCKET is well-designed to address the challenges of COPPA compliance, offering an automated and user-friendly solution that empowers parents to protect their children's privacy online.

Assessment of POCKET's Feasibility, Usability, and Legal Implications

**Feasibility:** POCKET's feasibility relies on the established Privacy Preference Platform project (P3P) framework, which enables parents to configure and enforce privacy preferences effectively. By leveraging this widely adopted technical solution, POCKET ensures robust feasibility in automating COPPA compliance.

**Usability:** POCKET excels in usability, providing an easy-to-use interface for parents to configure privacy choices for their children. Additionally, it maintains activity logs to enhance accountability, although technical support may be necessary during initial setup, especially for less tech-savvy parents.

**Legal Implications**: POCKET's effectiveness in COPPA compliance is well-established, aligning with legal requirements for parental consent before collecting information from children under 13. By offering automated solutions derived from COPPA compliance principles, POCKET serves as a legally sound tool for safeguarding children's online privacy.

Considering its feasibility, usability, and legal implications, POCKET emerges as an effective and reliable tool for parents seeking to uphold their children's online privacy.

Exploration of its Potential Role in Enhancing Children's Online Privacy

In light of the increasing importance of children's online privacy, exacerbated by widespread data collection practices, POCKET assumes a crucial role. COPPA mandates parental consent for collecting information from children under 13, yet existing business practices and technical approaches often fall short in effectively safeguarding children's privacy.

POCKET addresses this gap by offering an automated solution for enforcing COPPA compliance. By empowering parents to configure and enforce privacy policies, POCKET enhances children's online privacy significantly. Parents gain control over the information collected from their children, ensuring adherence to their configured policies and legal requirements like COPPA. Moreover, POCKET fosters accountability through activity logs, providing assurance in case of disputes.

Overall, POCKET stands as a pivotal tool in the ongoing efforts to enhance children's online privacy, offering a user-friendly and legally compliant solution to mitigate risks associated with online data collection.

**Touch Behaviour Based Age Estimation Toward Enhancing Child Safety** (Hossain and Haberfeld, 2020). This research investigates age estimation based on touch behaviour patterns, particularly tapping patterns on smartphones and tablets. Data was collected from users spanning a wide age range, from 5 to 61 years, and analysed to train and test various regressors and classifiers. The study aims to estimate a user's age based on their touch interactions to develop a child-safe browser capable of filtering out age-inappropriate content.

Results indicate that participants' touch behaviour patterns can effectively predict age using machine learning techniques. The methodology achieved mean absolute errors of 3.451 years for phones and 3.027 years for tablets, with accuracies of 73.63% for phones and 82.28% for tablets. While the study offers innovative techniques and includes a diverse age group for data collection, it is limited by focusing solely on tapping data and neglecting other interactions like swipes and zooms.

Overall, the research presents promising results for developing Privacy Enhancing Technologies (PETs) for child safety, especially in age-appropriate content filtering. Future studies could explore additional touch behaviours to improve age estimation accuracy and bolster online child safety.

Examination of the Accuracy and Ethical Considerations of Age Estimation Technologies

Age estimation technologies raise ethical concerns regarding accuracy, privacy, and bias. Accuracy is a primary concern due to variations in behaviour patterns and potential hindrances

to precise age assessments. Privacy issues arise as individuals may be reluctant to share personal touch behaviour patterns, particularly concerning children who may lack privacy awareness.
Moreover, the potential for bias in these technologies poses ethical challenges, especially if certain demographics or behaviours are favoured over others. This can lead to unequal access to online content and perpetuate stereotypes or prejudices.
While age estimation technologies may enhance child safety and online security, their accuracy and ethical implications necessitate careful consideration and discussion.

Discussion on Potential Applications in PETs for Children's Online Safety
Touch behaviour-based age estimation methodologies hold promise for PETs aimed at children's online safety. These technologies can monitor a child's device usage and automatically filter out inappropriate content without requiring explicit data from the child, thus protecting their privacy.
Additionally, PETs incorporating touch-based methodologies can provide parents with reports on their child's usage behaviour, allowing for effective monitoring while respecting privacy. Educationally, these PETs can be valuable for understanding students' learning processes and providing personalized feedback and support.
In conclusion, further research and development in touch behaviour-based age estimation methodologies can significantly enhance online security and privacy for children, offering a safer browsing experience and better educational support.

## 2.3 Regulatory Environment

In this section, I examine the regulatory framework that governs the collection, processing, and protection of children's data in online environments. Its critical to comprehend the landscape to evaluate whether childrens applications comply with privacy regulations particularly under the European Union's General Data Protection Regulation (GDPR).

### 2.3.1 General Data Protection Regulation (GDPR)

The GDPR, which came into effect in May 2018, is a comprehensive data protection regulation that applies to all member states of the European Union. It imposes rules on the management of personal information and places special emphasis on safeguarding the data of vulnerable individuals such, as children.

One important aspect of the GDPR that is significant for this study is Article 8's focus on the conditions governing a child's consent regarding services and information platforms. To ensure that children, under 16 (or an age determined by each country) are protected adequately in terms of their personal information handling activities online. Moreover, the GDPR emphasizes the importance of clear and easy to understand privacy policies when catering to audiences to promote transparency and accountability.

This section also talks about the focus of GDPRs data minimization. Stresses the significance of gathering only essential data for the intended goal. The rule is especially important, for applications aimed at. Expected to be used by children because it limits how much personal information these apps can collect without a specific legal justification.

### 2.3.2 Children's Online Privacy Protection Act (COPPA)

While my main research area centers on ensuring compliance with GDPR regulations it's crucial to mention the Children's Online Privacy Protection Act (COPPA) a key regulatory measure in the United States designed to safeguard the online privacy of children under 13 by placing specific obligations, on websites and online platforms that gather information from young users.

Under COPPA rules operators must get approval before gathering kids personal data similar to GDPRs child data safeguarding demands albeit with distinct age limits and compliance methods outlined differently in the regulations as well as mandating websites to furnish a detailed privacy policy outlining their data handling practices clearly and thoroughly. Although this dissertation does not center on COPPA exclusively its core tenets present a standpoint, for comparison shedding light on the worldwide importance placed on safeguarding childrens online privacy.

### 2.3.3 Compliance Challenges for App Developers

Many app developers find it a challenge to meet the requirements of GDPR and COPPA despite the defined rules in place, by these regulations. Creating privacy policies that're legally sound yet easy to understand for users poses a common hurdle. The changing landscape of app updates and external partnerships adds another layer of complexity to compliance efforts requiring constant evaluation and documentation of data handling practices.

In this paper we will delve into problems that developers face including lack of transparency and not getting the right consent along with collecting too much data unnecessarily. With a look at these difficulties, I want to emphasize how vital it is to uphold strong privacy measures and the continuous need for monitoring and adjustments to ensure adherence, to regulatory norms.

### 2.3.4 Enforcement and Penalties

GDPR enforcement is overseen by national Data Protection Authorities (DPAs) who are empowered to probe and penalize organizations found violating the regulations. Fines for breaching the rules can be up to €20 million or 4% of a companys global annual revenue (whichever is greater). This segment will delve into enforcement measures taken against businesses with a focus, on safeguarding childrens privacy to showcase the possible repercussions of non-compliance.

COPPA violations in the US are regulated by the Federal Trade Commission (FTC) whereas under GDPR in the EU each member state is responsible for enforcing the regulations within their jurisdictional boundaries This section will explore and compare how enforcement mechanisms differ and their implications, for app developers working across various regions.

### 2.3.5 Implications for the Study

The foundation of this dissertation is built upon the framework that sets the stage for examining the privacy policies and tracking methods of apps designed for children within a legal framework contextually appropriate setting. Understanding the demands specified by GDPR is crucial in evaluating whether the chosen apps adhere to regulations and, in suggesting informed enhancements to privacy measures.

This part lays the foundation for the evaluation phase in which I will assess the apps compliance with the regulatory guidelines outlined here. By anchoring the research in the context my goal is to guarantee that the conclusions and suggestions are not only pertinent but also legally valid adding value to the larger conversation about safeguarding childrens privacy, in today’s digital era.

# Chapter 3 – Evaluation Of Privacy Policies

In this section of my thesis, I summarize how I studied and what I discovered while reviewing the privacy policies of 30 kid's apps that can be downloaded from the Google Play Store. The review process kicks off with a talk on the standards used to pick out these apps and stresses the crucial nature of evaluating their privacy policies. After that, I go into detail, about the techniques used to choose to examine and assess the apps in terms of following the General Data Protection Regulation (GDPR). The assessment centers on seven GDPR criteria including the legality of data processing and responsible handling of data quantity as well as maintaining accountability measures in place related to privacy policies of these applications; the section wraps up with an overview of main discoveries and their impact, on safeguarding of children's privacy.

## 3.1 Background

A systematic approach was employed in selecting these apps. I prioritized high levels of engagement amongst other reasons to represent a significant area of concern when it comes to the collection and handling of sensitive personal data.

The significance of assessing these privacy policies is emphasized by the necessity to adhere to industry norms and regulations like the General Data Protection Regulation (GDPR). In this research project, we carefully examined each app's privacy policy to assess if it was fully compliant partially compliant or non-compliant, with recognized data protection principles. Each app was assigned a compliance rating to quantify how effectively they comply with privacy rules.

Through this assessment process the research aims to add to the conversation surrounding online privacy and safeguard of data especially with regards to at risk groups such as youngsters. The results of this examination will not showcase the existing level of adherence to privacy regulations in commonly used apps for children but will also offer direction for guardian's, teachers and decision makers worried about safeguarding childrens data, in the digital era.

## 3.2 Methodology

A detailed explanation of the methods used to select, analyze, and rate the apps based on GDPR compliance.

### 3.2.1 Selection of Apps

The process of choosing apps was carefully planned out to focus on apps popular among kids under the age of sixteen that can be found in categories like education and games in the Google Play Store because these are the ones children use frequently and enjoy the most. The reason behind this choice is that these used apps pose a higher risk of data misuse given their popularity, among young users so it's important to closely examine how they handle privacy issues.

Even if there were no worries about privacy specifically mentioned beforehand when it comes to these applications' popularity warrants a detailed review. Should the privacy policies of apps with users effectively protect user data? This research aims to investigate the dangers related to data gathering and utilization, in apps frequently used by kids.

Image of Selected Apps

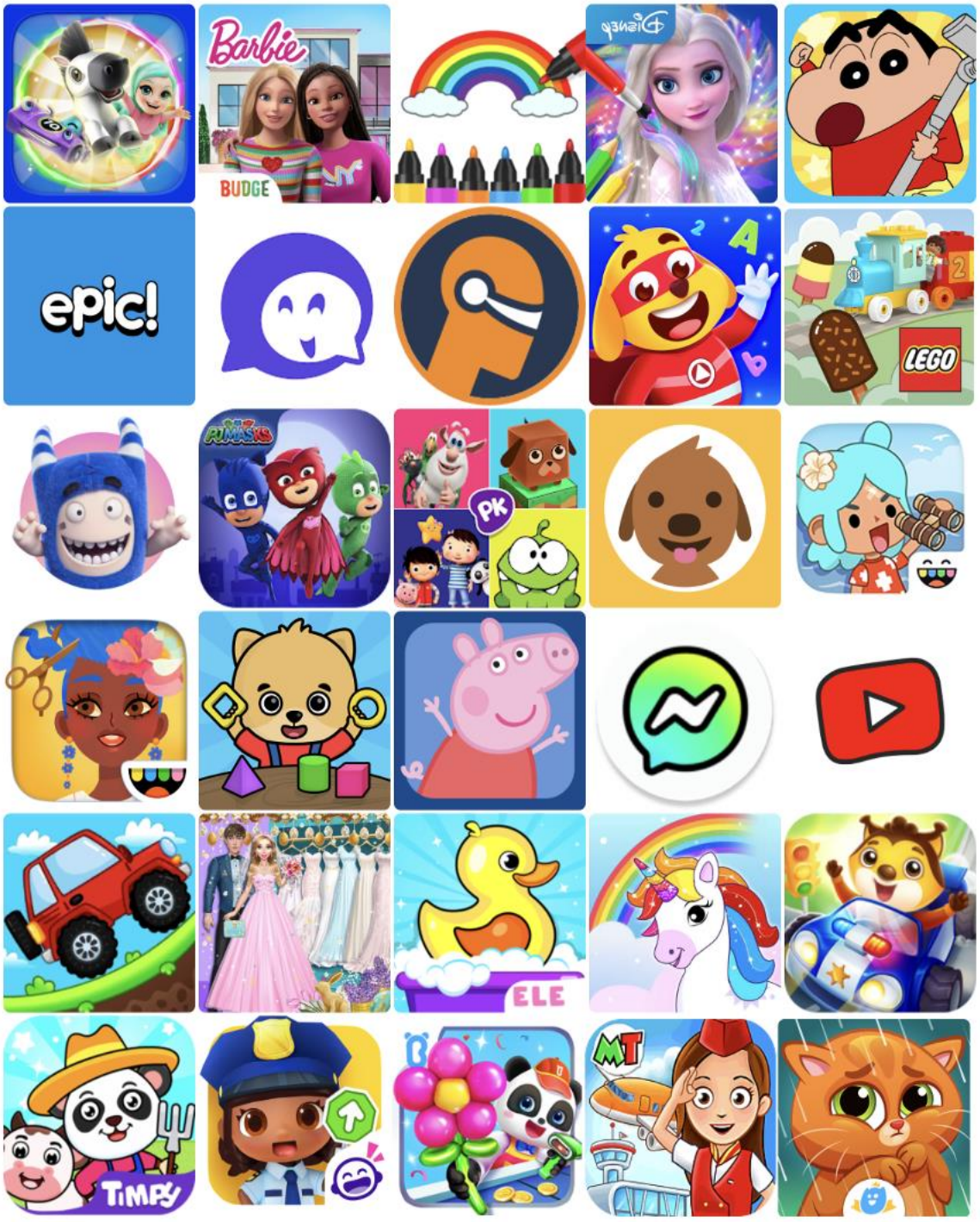



*Figure 6- Selected children app icons.*

### 3.2.2 Criteria for Analysis

The analysis was centered around seven GDPR principles that were used as the basis for reviewing the privacy policies in question The scoring system, for compliance measured how well the privacy policies aligned with these specific GDPR principles:

- Lawfulness, Fairness, and Transparency
- Purpose Limitation
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality (Security)
- Accountability

For each principle, I evaluated whether the privacy policy:

- Fully Complies: Meets all key aspects of the GDPR principle with clear, explicit descriptions and adequate measures.
- Partially Complies: Addresses some aspects of the principle but lacks detail, clarity, or full implementation.
- Non-Compliant: Fails to meet the principle's requirements or lacks sufficient information to determine compliance.

### 3.2.3 Scoring and Analysis

I used these factors to generate a score for the compliance of each apps privacy policy.

Scoring Factors:

- Clarity and Transparency: The extent to which the policy clearly communicates its procedures to users.
- Specificity: Whether the policy provides specific details (e.g., retention periods, security measures).
- Breadth: Coverage of all necessary aspects of the principle.
- User Rights: Information on how users can exercise their GDPR rights (e.g., access, rectification, erasure).
- Children's Data: Special consideration for compliance related to children under 13, in alignment with GDPR's emphasis on protecting minors.

Each principle was scored out of 3:

3 points: Full compliance.
2 points: Partial compliance.
0 points: Non-compliance.

The final score was calculated by combining all the scores to determine the overall level of compliance achieved.

Benchmarks

- The main reference point for GDPR compliance is the text of the GDPR itself. with a specific emphasis on the legal obligations and explanations provided in the recitals to elaborate on the principles, in greater depth.

Consistency and Objectivity:
To ensure consistency and objectivity:

- Standardized Criteria: Used the same criteria for each principle across different apps and policies.
- Clear Definitions: Defined what constitutes full, partial, and non-compliance for each principle.
- Documentation: Documented the reasoning behind each rating to maintain a record of the decision-making process.

Addressing Potential Biases

- Objectivity Measures: I employed a method grounded in specific criteria to minimize subjectivity, in the evaluation process of each principles score was determined by established factors to prevent personal biases from impacting the ratings.
- Peer Review: While a structured peer review process was not carried out specifically in this case study report the methodology was crafted with transparency and reproducibility in mind. This approach enables interested parties to scrutinize the assessments if necessary.

Conclusion
The system for measuring compliance was created with care to fairly evaluate GDPR adherence by examining important principles in a structured manner. The system seeks to offer an precise evaluation of GDPR compliance for apps designed for children through the use of standardized criteria and clear reasoning, behind each score.

## 3.3 Analysis of Privacy Policies

This section provides an evaluation of thirty privacy policies based on the following GDPR principles: Lawfulness, Fairness, and Transparency (L.F.T), Purpose Limitation (P.L), Data Minimization (D.M), Accuracy (ACC), Storage Limitation (S.L), Integrity and Confidentiality (I & T) and Accountability (ACCT). Each policy is assessed as Fully Compliant (Fully), Partially Compliant (Partial), or Non-Compliant (Non-C).

Table 6 of 7 - GDPR Compliance Analysis of Privacy Policies

| APP | Developer | L.F. T | P. L. | D.M. | ACC. | S. L | I & T | ACCT. | C/S |
|---|---|---|---|---|---|---|---|---|---|
| Applaydu family games | Ferrero Trading Lux S.A. | Fully | Partial | Partial | Fully | Partial | Partial | Partial | 16/21 = 76% |
| Barbie dream house | Budge Studios | Partial | Fully | Partial | Fully | Partial | Fully | Partial | 17/21 = 81% |
| Colouring & Drawing for Kids | Toy Tap LLC | Fully | Fully | Partial | Fully | Partial | Fully | Partial | 18/21 = 86% |
| Crayon Shinchan Little Helper | Neos | Partial | Fully | Partial | Partial | Non-C | Fully | Partial | 14/21 = 67% |
| Disney Coloring World | StoryToys | Partial | Partial | Partial | Non-C | Non-C | Partial | Partial | 10/21 = 48% |
| My Town Airport games for kids | My Town Games Ltd | Partial | Partial | Fully | Non-C | Non-C | Partial | Partial | 11/21 = 52% |
| Epic - Kids' Books & Reading | Epic! Creations Inc | Fully | Fully | Fully | Fully | Fully | Fully | Fully | 21/21 = 100% |
| Fulldive VR - Virtual Reality | Browser by Fulldive Co. | Partial | Partial | Non-C | Non-C | Partial | Non-C | Non-C | 6/21 = 29% |
| KidiCom Chat™ | VTech Electronics Ltd. | Partial | Partial | Partial | Non-C | Non-C | Partial | Partial | 10/21 = 48% |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Kiddopia - Kids Learning Games | Kiddopia Inc. | Partial | Fully | Partial | Partial | Partial | Fully | Partial | 16/21 = 76% |
| LEGO | StoryToys | Partial | Partial | Partial | Non-C | Partial | Partial | Partial | 12/21 = 57% |
| Oddbods Oddlife | Weyo Pty Ltd | Partial | Fully | Partial | Partial | Non-C | Partial | Partial | 13/21 = 62% |
| PJ Masks™: Moonlight Heroes | Scary Beasties Limited | Partial | Partial | Fully | Non-C | Fully | Partial | Partial | 14/21 = 67% |
| PlayKids+ Kids Learning Games | Playkids BV | Fully | Fully | Partial | Fully | Fully | Fully | Partial | 19/21 = 90% |
| Sago Mini World | Play Piknik | Partial | Partial | Fully | Non-C | Fully | Partial | Partial | 14/21 = 67% |
| Toca Boca | Toca Boca | Partial | Partial | Partial | Non-C | Partial | Partial | Non-C | 10/21 = 48% |
| Toca Boca Jr Hair Salon | Play Piknik | Partial | Fully | Partial | Partial | Partial | Non-C | Partial | 13/21 = 62% |
| Bubbu – My Virtual Pet Cat | Bubadu | Partial | Partial | Partial | Non-C | Non-C | Partial | Non-C | 8/21 = 38% |
| Toddler games for girls & boys | Bimi Boo Kids Learning Games for Toddlers FZ-LLC | Partial | Partial | Fully | Non-C | Non-C | Partial | Partial | 11/21 = 52% |
| World of Peppa Pig | Find Your Fun | Partial | Fully | Partial | Partial | Partial | Fully | Partial | 16/21 = 76% |
| Messenger for Kids | Meta Platforms, Inc. | Partial | Fully | Partial | Non-C | Partial | Partial | Non-C | 10/21 = 48% |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| YouTube Kids | Google LLC | Partial | Fully | Partial | Partial | Partial | Non-C | Partial | 13/21 = 62% |
| Car Wash & Race Games for Kids | GunjanApps Studios | Partial | Fully | Fully | Non-C | Non-C | Partial | Non-C | 8/21 = 38% |
| Blondie Bride Perfect Wedding | Promedia Studio | Partial | Fully | Fully | Non-C | Non-C | Partial | Partial | 12/21 = 57% |
| ElePant Kids Educational Games | GunjanApps Studios | Partial | Fully | Fully | Non-C | Non-C | Partial | Non-C | 10/21 = 48% |
| Unicorn Games | IDZ Digital Private Limited | Partial | Fully | Partial | Non-C | Partial | Non-C | Partial | 11/21 = 52% |
| Baby Panda's Town: Life | BabyBus | Partial | Partial | Partial | Non-C | Partial | Partial | Partial | 12/21 = 57% |
| Car Games for Kids & Toddlers | Amaya Kids - learning games for 3-5 years old | Partial | Fully | Partial | Fully | Partial | Non-C | Partial | 14/21 = 67% |
| Timpy Kids Animal Farm Games | Timpy Games for Kids, Toddlers & Baby | Partial | Fully | Partial | Partial | Partial | Non-C | Partial | 13/21 = 62% |
| URban city | SUBARA | Fully | Fully | Partial | Fully | Partial | Fully | Partial | 18/21 = 86% |
| Average | | Partial | Fully | Partial | Non-C | Partial | Partial | Partial | 62% |

*Table 6- GDPR Compliance Analysis of Privacy Policies*

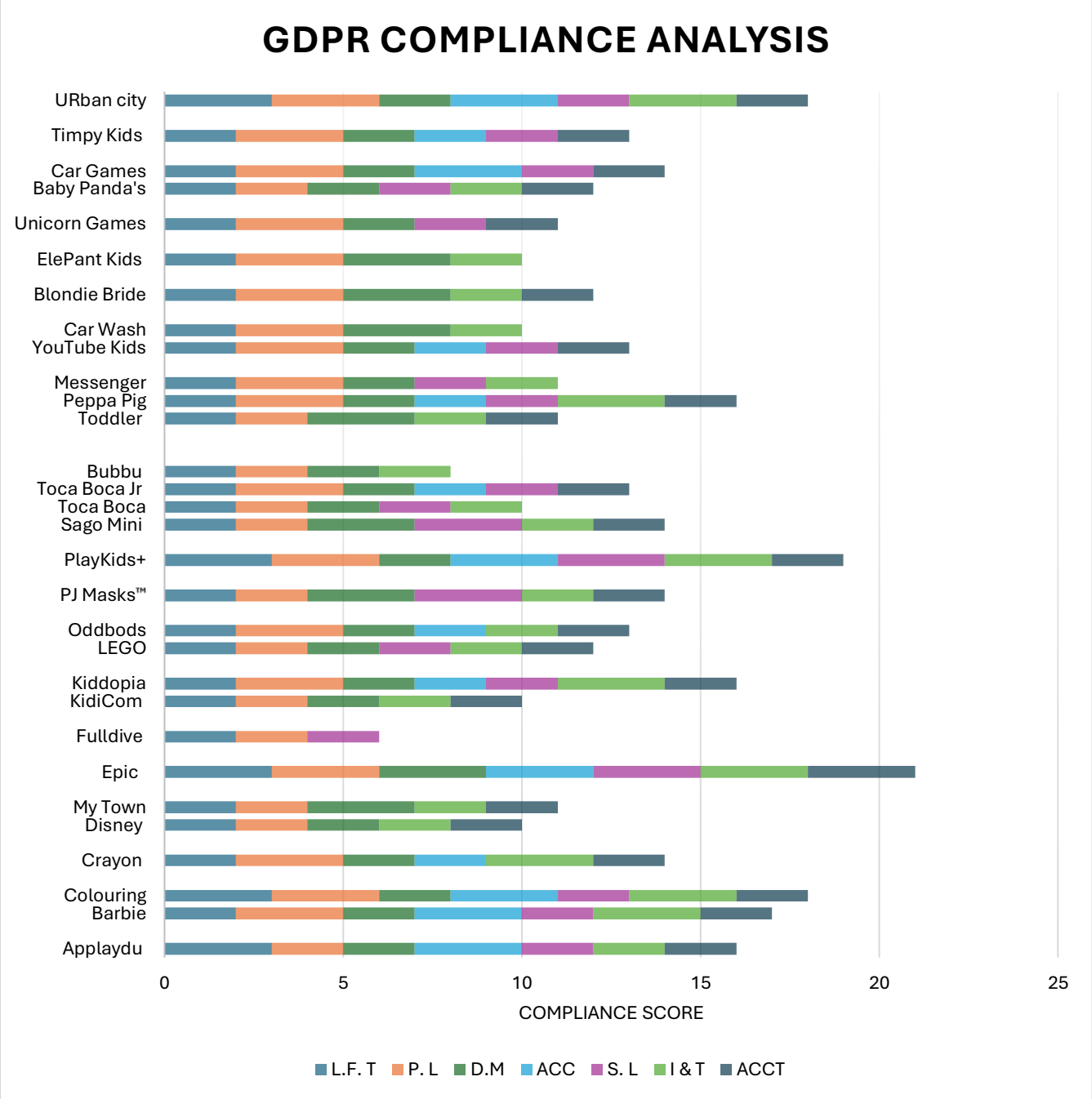



*Figure 7- Chart showing the GDPR Compliance of 30 Children Apps*

### 3.3.1 Lawfulness, Fairness, and Transparency

The principle of Lawfulness and Transparency within the GDPR mandates that personal information should be handled in a way that's legal and transparent to the individual concerned while also ensuring fairness, in data processing to prevent any unwarranted harm to individuals. It's important for data subjects to know how their data is being used. Who is collecting it and why. And to understand their rights fully informedly. Here's a chart that outlines how well 30 childrens apps are meeting the criteria of Lawfulness and Transparency.

**Report**

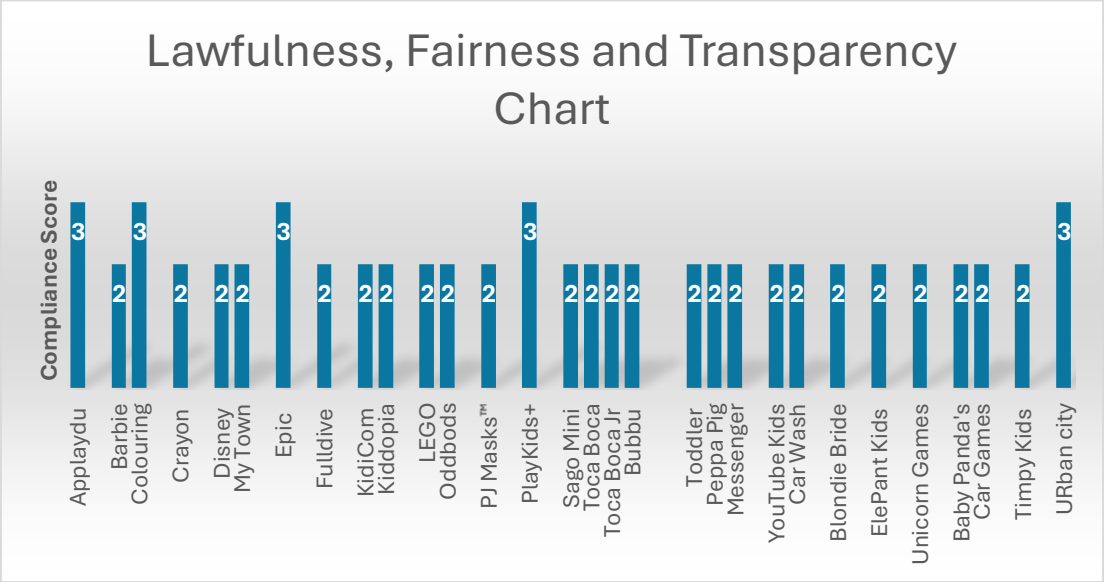



*Figure 8- Chart showing Lawfulness, Fairness and Transparency performance.*

### 3.3.2 Purpose Limitation

The Principle of Purpose Limitation states that personal information should only be gathered for clear reasons that are lawful and not used in ways that go against those initial purposes. This requires organizations to outline why they collect data from the start and ensure that any future use of the data aligns with the original intent. If there is a need to use the data for a purpose it should be, within the scope of the original consent or a new legal basis must be established. Here is a diagram displaying how well the 30 childrens apps stick to their intended purpose.

**Report**

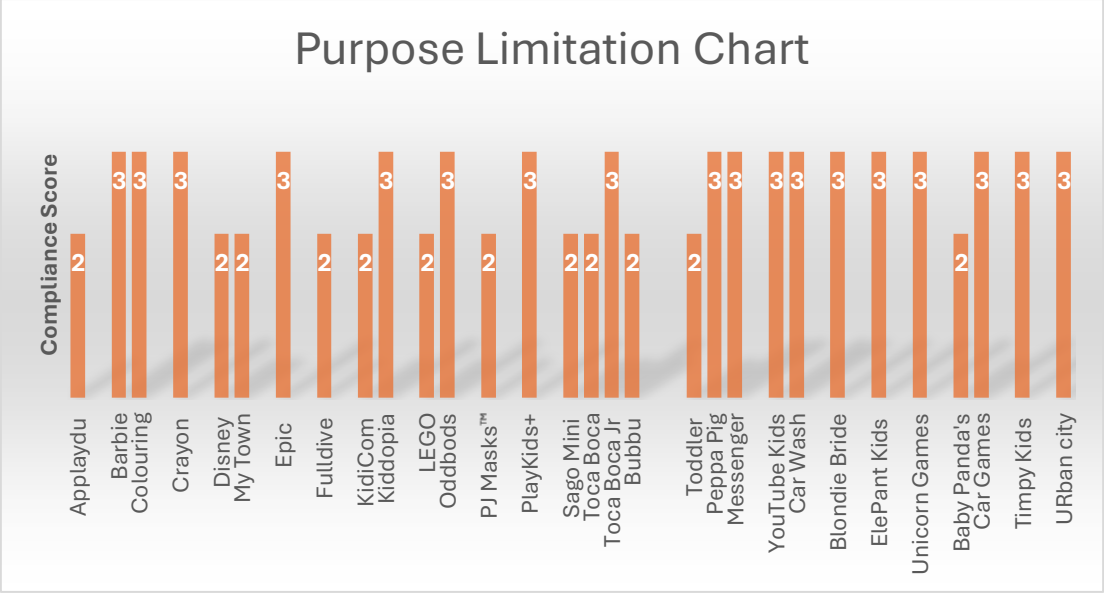



*Figure 9- Chart showing Purpose Limitation performance.*

### 3.3.3 Data Minimization and Accuracy

Data Minimization involves ensuring that the personal information gathered is suitable and necessary, for the intended purposes of processing it ethically. This guideline underscores the significance of collecting essential data required to achieve the desired goal to minimize the chances of excessive collection or improper use of data. Accuracy dictates that personal information should be precise and regularly updated when needed. Incorrect data should be promptly. Removed to uphold the accuracy and reliability of information maintained by entities. Here is a chart displaying the data minimization effectiveness of 30 childrens apps.

**Report**

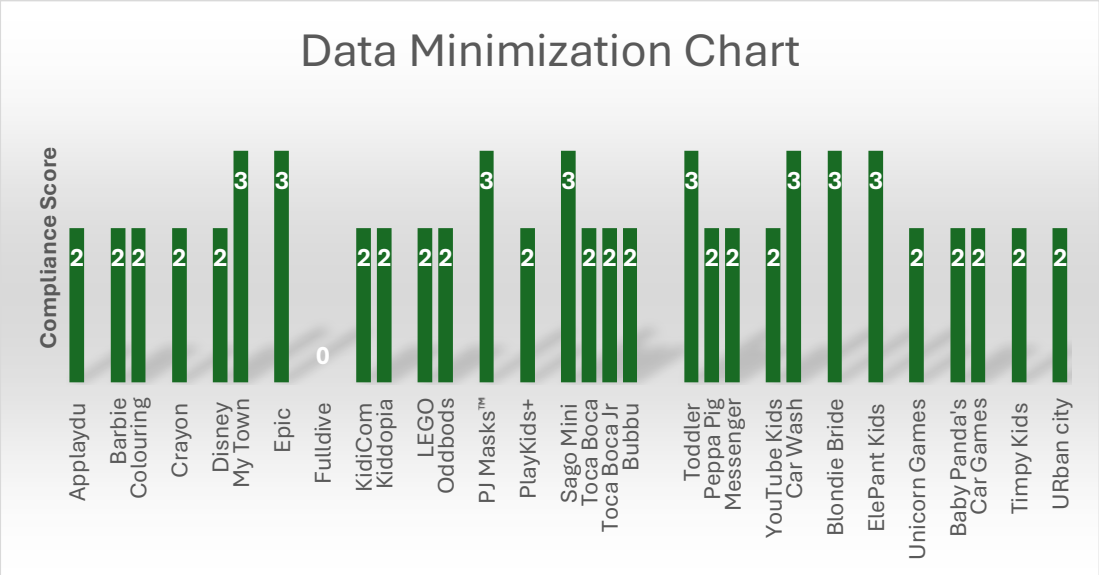



*Figure 10- Chart showing Data Minimization performance.*

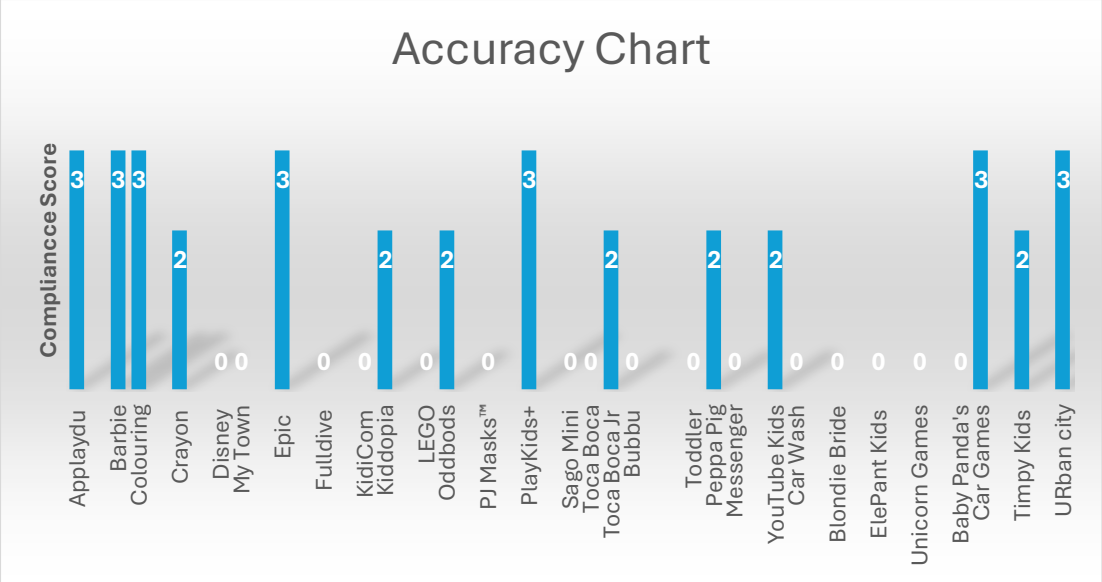



*Figure 11- Chart showing Accuracy performance.*

### 3.3.4 Storage Limitation

The Storage Limitation principle in GDPR states that personal information must only be held in a way that allows identifying individuals for long as needed for the intended data processing purposes. Once the data is no longer necessary for those purposes it should either be securely. Anonymized to prevent unauthorized access. This principle focuses on restricting data retention to the shortest duration necessary, for valid business or legal reasons thus lowering the chances of data breaches and improving privacy safeguards. Here is a graph displaying the storage capacity performance of 30 childrens apps.

**Report**

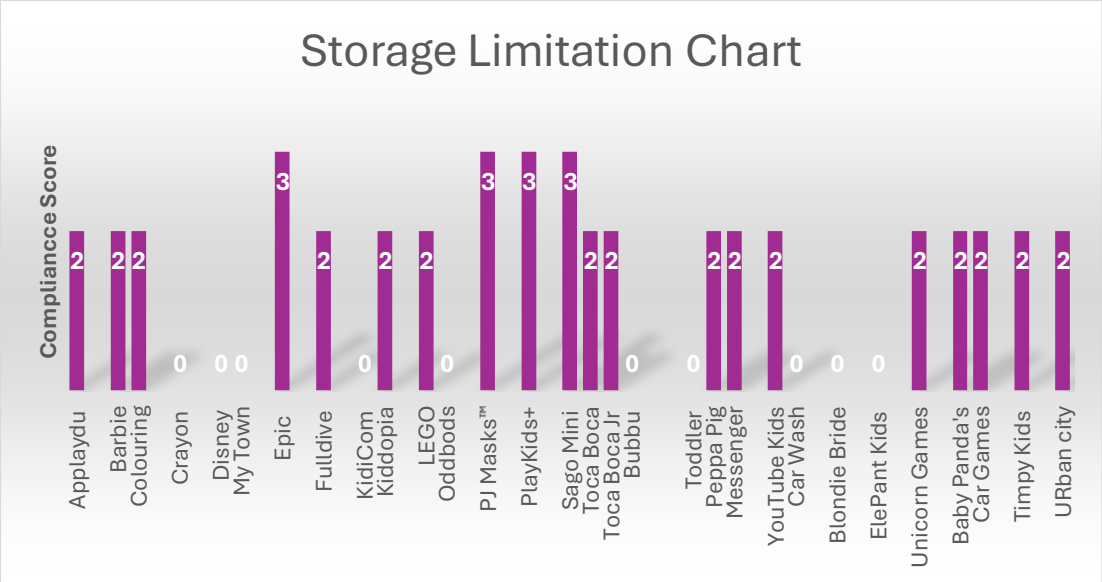



*Figure 12- Chart showing Storage Limitation performance.*

### 3.3.5 Integrity and Confidentiality

To maintain Integrity and Confidentiality standards it is crucial that personal information is handled securely to prevent access or misuse and to prevent accidental loss or damage to the data. Companies should put in place security measures like encryption and access controls along, with data storage solutions to protect personal information effectively. This approach highlights the importance of data security protocols to uphold the trust of individuals whose data is being processed and to adhere to the legal requirements outlined in GDPR. Here's a chart displaying how well the 30 childrens apps protect privacy and maintain confidentiality.

**Report**

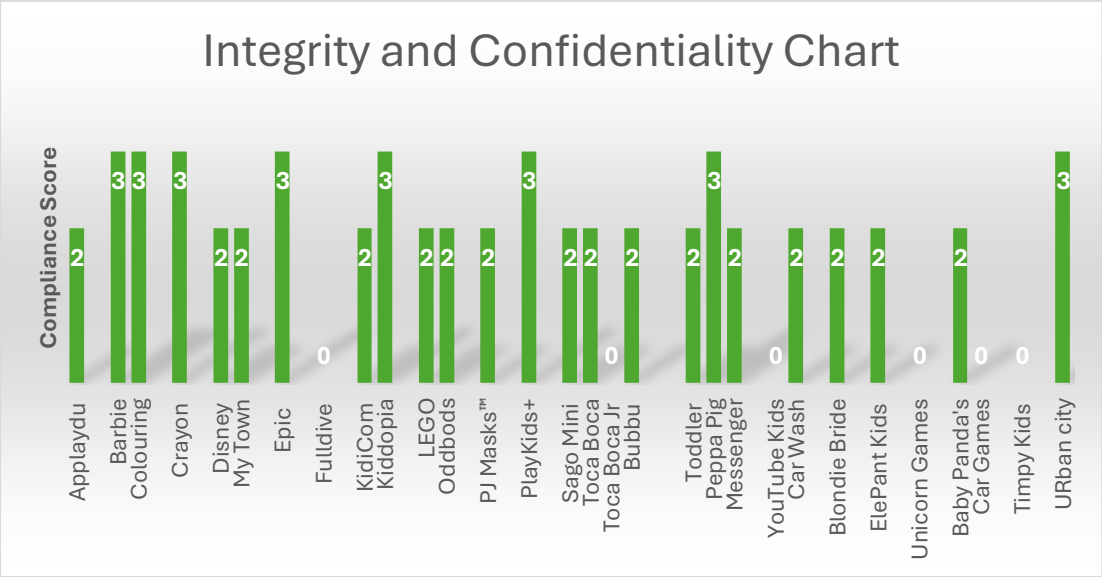



*Figure 13- Chart showing Integrity and Confidentiality performance.*

### 3.3.6 Accountability

The principle of Accountability mandates that organizations must take ownership of ensuring and showcasing adherence to GDPR regulations by implementing data protection measures and carrying out routine assessments while maintaining detailed records of processing activities to prove compliance to both regulators and data subjects under the GDPR guidelines. Through Accountability practices in place not in theory but also in real world application it cultivates a culture of data protection and ongoing surveillance. Here is a visual representation indicating the accountability ratings, for the 30 childrens apps.

**Report**


*Figure 14- Chart showing Accountability performance.*

## 3.4 Summary

This section examines how the privacy guidelines of 30 liked childrens applications on the Google Play Store align with critical GDPR standards by scrutinizing their approach to following GDPRs guidelines such, as Legality and Transparency in use of personal data integrity and confidentiality.

The assessment shows the extent to which these applications comply with privacy regulations and points out their advantages and drawbacks clearly. The section wraps up with an overview of the main discoveries and how they can impact safeguarding childrens privacy. Providing useful perspectives, for parents, teachers and decision makers.

# Chapter 4 – Data Tracking Practices

My research focuses on examining the tracking methods utilized in childrens apps and evaluating their adherence to GDPR guidelines using tools such as Exodus Privacy. To begin with I introduce the notion of data tracking and its significance in safeguarding childrens privacy. In addition, I describe the approaches I employed which involved utilizing Exodus Privacy to identify trackers and validating these results against GDPR regulations. Furthermore, my study delves into the outcomes regarding the frequency and categories of trackers present providing insights into their implications, for childrens privacy. In wrapping up I'll highlight the takeaways and discuss how they affect safeguarding data, in apps designed for kids.

## 4.1 Background

Data tracking in apps is a major concern when it comes to applications made for kids since tracking features included in these apps can observe how users behave and gather personal data to share with external parties without clear permission from the users themselves. A situation that raises privacy concerns, for children who may not fully grasp the consequences of data collection or possess the independence to consent knowingly. The GDPR has set rules to safeguard user data with a focus on minor's protection; apps are required to seek explicit consent and provide clear information when gathering personal data while also being open, about their data handling practices.

In the realm of children's applications regulations play a more vital role because of the vulnerability of this group. Children's information is extremely delicate. Mishandling it can result in privacy breaches with enduring effects. Hence comprehending the tracking methods employed in applications and assessing their adherence to GDPR is crucial not just for safeguarding childrens privacy but also, for guaranteeing that app creators abide by lawful and ethical norms.

In this chapter, we explore the details of how tracking is carried out in apps for children. What kind of data is gathered and how it might be shared with others outside the app's environment. By concentrating on GDPR adherence, in this study, we want to unveil whether these apps uphold the privacy rights of children, or they miss the mark when it comes to meeting standards.

## 4.2 Methodology

In this part of the paper, we describe the methods used to examine how data tracking is done in the children's apps that were chosen for review. We mainly relied on Exodus Privacy as our primary tool to detect any trackers in Android applications. To make sure we have an assessment of the situation we compared the results, from Exodus Privacy with what is mandated by the GDPR regarding consent, transparency and sharing of data practices.

### 4.2.1 Tracking Analysis Using Exodus Privacy

Exodus Privacy served as the tool for identifying and examining trackers integrated into the childrens apps selected for this research study. The tool scans applications for recognized tracking libraries. Generates comprehensive reports on the types of trackers identified and their potential implications on user privacy. The initial step involved choosing childrens apps from the Google Play Store based on their download counts, user feedback and suitability, for the intended age bracket.

The team examined each application with the help of Exodus Privacy to uncover a list of trackers concealed within the code of the apps. They classified these trackers according to their purposes like analytics or advertising. Delved into how they functioned and what information they gather for potential third-party use. This section elucidates the aspects of the analysis process such, as app selection criteria and the key functions of Exodus Privacy that were utilized in this study.

### 4.2.2 Data Sharing with Third Parties

Cross-Verification with GDPR Requirements

In order to check if the tracking methods identified comply with GDPR regulations the information gathered from Exodus Privacy was compared with the standards set by GDPR. This process included checking whether the applications had easy to understand privacy policies obtained clear permission from users (or their guardians for minors) and revealed the specific reasons, for collecting and sharing data with external parties.

The GDPR ensures that any handling of data must follow guidelines and treat minors fairly and transparently. Users should have access, to their collected information. Expect their data to be handled securely. A recent study examined how well apps upheld these rules by analyzing their privacy policies and comparing them with the tracking data identified by Exodus Privacy.

During the verification process discrepancies were found between the privacy policies of the apps and how they actually collect data leading to an analysis of GDPR compliance levels and potential breaches of childrens privacy rights

## 4.3 Results and Findings

Presents the findings from the tracking analysis, including the prevalence of trackers, category of the apps, number of permissions and the last date it was updated.

Table 7 of 7 - Application Tracking Analysis

| App | Category | Tracker Count | Total Permissions | Last Analysis Date |
|---|---|---|---|---|
| Applaydu family games | Education | 1 | 16 | July 13, 2024 |
| Barbie dream house | Entertainment | 1 | 10 | July 13, 2024 |
| Colouring & Drawing for Kids | Education | 4 | 13 | July 14, 2024 |
| Crayon Shinchan Little Helper | Educational | 3 | 10 | July 23, 2024 |
| Disney Coloring World | Entertainment | 1 | 12 | July 13, 2024 |
| My Town Airport games for kids | Educational | 13 | 8 | July 17, 2024 |
| Epic - Kids' Books & Reading | Educational | 8 | 10 | July 14, 2024 |
| Fulldive VR - Virtual Reality | Entertainment | 6 | 12 | July 15, 2024 |

| | | | | |
|---|---|---|---|---|
| KidiCom Chat™ | Communication | 0 | 10 | July 17, 2024 |
| Kiddopia - Kids Learning Games | Educational | 3 | 22 | July 13, 2024 |
| LEGO | Games | 1 | 11 | July 13, 2024 |
| Oddbods Oddlife | Games | 6 | 9 | July 24, 2024 |
| PJ Masks™: Moonlight Heroes | Entertainment | 4 | 7 | July 17, 2024 |
| PlayKids+ Kids Learning Games | Entertainment | 15 | 15 | July 17, 2024 |
| Sago Mini World | Games | 3 | 11 | July 20, 2024 |
| Toca Boca | Games | 2 | 14 | July 17, 2024 |
| Toca Boca Jr Hair Salon | Educational | 3 | 6 | July 14, 2024 |
| Bubbu – My Virtual Pet Cat | Game | 29 | 13 | July 22, 2024 |
| Toddler games for girls & boys | Game | 1 | 6 | July 15, 2024 |
| World of Peppa Pig | Game | 3 | 12 | July 14, 2024 |
| Messenger for Kids | Communication | 3 | 40 | July 13, 2024 |
| YouTube Kids | Entertainment | 2 | 16 | July 19, 2024 |
| Car Wash & Race Games for Kids | Game | 3 | 9 | July 20, 2024 |
| Blondie Bride Perfect Wedding | Game | 3 | 9 | July 20, 2024 |
| ElePant Kids Educational Games | Game | 3 | 19 | July 20, 2024 |
| Unicorn Games | Game | 1 | 10 | July 15, 2024 |
| Baby Panda's Town: Life | Educational | 8 | 10 | July 13, 2024 |
| Car Games for Kids & Toddlers | Game | 0 | 7 | July 15, 2024 |
| Timpy Kids Animal Farm Games | Game | 7 | 9 | July 20, 2024 |

| | | | | |
|---|---|---|---|---|
| URban city | Game | 10 | 15 | July 24, 2024 |

*Table 7- Application Tracking Analysis*

### 4.3.1 Analysis of Tracking Practices

In this part of the study, we analyze closely the tracking methods used in known mobile apps for kids and consider how they impact childrens privacy rights. We also review how these methods comply with the General Data Protection Regulation (GDPR) a law aimed at safeguarding the information of EU residents and offering extra protection, for minors.

Tracking Practices in Children's Apps

Our analysis of 30 popular children's apps revealed a concerning prevalence of tracking mechanisms. On average, each app contained five distinct trackers, with some applications significantly exceeding this average. Notably, four apps were found to have an exceptionally high number of trackers—15, 29, 13, and 10 respectively. These apps, categorized under entertainment, gaming, educational, and gaming, illustrate a broad spectrum of tracker proliferation across different types of children's apps.

The growing number of trackers gives rise to privacy issues as these tools are commonly deployed to gather information about user actions and choices for purposes such as personalized advertising and user profiling or potentially sharing the data with external entities This becomes especially troublesome in the case of apps designed for children due to their vulnerable nature and the strict safeguards provided for them by GDPR regulations.

Permissions and Privacy Implications

In addition to tracking mechanisms, we also analyzed the number of permissions requested by these apps, as identified through Exodus Privacy, a tool for analyzing the privacy implications of mobile applications. On average, each app requested 12.3 permissions. The nature of these permissions ranged from access to sensitive data, such as location and camera, to more benign requests, like network access. However, the cumulative effect of these permissions, when combined with the presence of multiple trackers, potentially exposes children to significant privacy risks.

The large amount of permissions and trackers in these apps not heightens the risk of data leaks but also prompts questions about the need and scale of data gathering practices in them. According to GDPR regulations data collection must abide by the principles of minimizing data usage and restricting its purpose to what is necessary. This entails that any collected data should be appropriate relevant and kept to a minimum for the purpose it serves. The presence of a number of trackers and permission requests in some childrens apps may indicate a potential departure, from these principles.

GDPR Compliance and Children's Privacy

The GDPR offers increased safeguards for childrens data by acknowledging that children may have limited awareness of the risks and outcomes related to their personal information being used. Article 8 of the GDPR focuses on the requirements for obtaining a child's consent regarding online services. Additionally, Article 8 highlights the importance of providing safeguards, for childrens personal data especially concerning marketing activities, establishment of user profiles or when services are targeted directly at children.

Our analysis indicates a discrepancy in how these apps track user data compared to the standards set by GDPR regulations. The multitude of trackers and the extensive permissions sought by these apps may not align well with GDPRs core values of fairness and transparency. Additionally, the absence of privacy notices tailored for children and user-friendly consent processes in some apps heightens the likelihood of non-compliance, with GDPR guidelines.

Implications for Policy and Practice

The results highlight the importance of enforcing GDPR strictly in childrens app settings. As such it is crucial, for regulators and app creators to collaborate in ensuring that tracking methods are clear and justified while being kept to a minimum. In apps intended for children. Moreover, this highlights the necessity for app developers to embrace privacy focused design concepts by incorporating data protection measures into the development process from the start.

Ultimately even though GDPR offers a structure for safeguarding childrens privacy the behaviors seen in well liked apps targeted at kids reveal notable shortcomings in adherence to regulations. It is vital to close these gaps to ensure the protection of childrens privacy and rights, in today's era.

## 4.4 Summary

This chapter analyzed data tracking practices in children's mobile apps, revealing significant concerns about privacy and GDPR compliance. Using Exodus Privacy, we found an average of five trackers per app, with some apps containing up to 29 trackers. The permissions requested by these apps averaged 12.3 per app, often extending to sensitive data access.

These discoveries bring up concerns regarding how well these practices adhere to the principles outlined in the GDPR law. Especially around limiting data collection and ensuring transparency. The abundance of trackers and broad permissions indicates a lack of focus on safeguarding childrens privacy rights. Showcases a disparity, between what regulations demand and how apps actually operate in reality.

In conclusion, the chapter emphasizes the need for stricter enforcement of GDPR and more responsible app development to protect children's privacy in the digital age. Addressing these issues is crucial for ensuring a safer online environment for young users.

# Chapter 5 – Discussion

## 5.1 Identification of Compliance Gaps

### 5.1.1 Background

In the digital world safeguarding user privacy is crucial to comply with laws and retain customer confidence. For developers of apps, those aimed at youngsters following rules such as GDPR and COPPA is vital. Detecting any areas where compliance may be lacking is an essential process, in guaranteeing that apps conform to these legal requirements, which helps in avoiding possible legal consequences and protecting a company's image.
Failure to comply may result in repercussions such as penalties, sanctions, and harm to brand credibility—particularly vital for applications targeting at risk demographics such as youngsters. This segment emphasizes the significance of rectifying compliance shortcomings to safeguard user information and uphold the credibility of platforms laying the groundwork for a more thorough examination of non-compliance concerns, in subsequent sections.

### 5.1.2 Analysis of Non-Compliance

This section shows a full analysis of two fully compliant and non-compliant childrens apps.

**Epic - Kids' Books & Reading**
Assessment of Compliance Against GDPR Principles:

1. Lawfulness, Fairness, and Transparency: 3/3
   - Lawfulness: The policy explains the types of data collected (e.g., personal information, usage data, device information) that are necessary for the service provided.
   - Fairness: The policy indicates that data collection is limited to what is necessary for providing and improving services, ensuring fair treatment.
   - Transparency: The policy is detailed and clearly explains the data collection, usage, and sharing practices.
   - Compliance: Fully Compliant.
2. Purpose Limitation: 3/3
   - Purpose Specification: The policy outlines specific purposes for data collection, such as providing services, communication, personalization, and security.
   - Use Limitation: It indicates that data is not used beyond the specified purposes without user consent.
   - Compliance: Fully Compliant.
3. Data Minimization: 3/3
   - Data Necessity: The policy claims to collect only the necessary information, such as basic account details and usage data.
   - Parental Control: Parents have control over their child's data, which aligns with minimizing data collection from children.
   - Compliance: Fully Compliant.
4. Accuracy: 3/3
   - Data Accuracy: Users can edit or delete information in their accounts.
   - Policy Provisions: There is a clear mechanism for users to request corrections, ensuring data accuracy.
   - Compliance: Fully Compliant.
5. Storage Limitation: 3/3
   - Retention Period: The policy states that data is retained only as long as necessary for service provision and will be deleted or de-identified thereafter.
   - Compliance: Fully Compliant.
6. Integrity and Confidentiality: 3/3

- Security Measures: The policy describes reasonable security measures, including encryption and secure transmission protocols.
- Breach Notification: While not explicitly mentioned, GDPR requires breach notifications, which is implied as part of their compliance efforts.
- Compliance: Fully Compliant.

7. Accountability: 3/3
   - Compliance Accountability: The policy provides contact information for privacy inquiries and complaints, showing accountability.
   - Detailed Information: It thoroughly describes data practices, which is a key part of demonstrating accountability.
   - Compliance: Fully Compliant.

Epic's Privacy Policy is comprehensive and appears to fully adhere to all GDPR principles. It clearly outlines the collection, use, and protection of personal information, provides transparency, and offers mechanisms for user control and correction of data. The policy is rated as fully compliant with all seven GDPR requirements.

**Fulldrive VR - Virtual Reality**

To evaluate the Fulldive VR privacy policy against the GDPR's seven key principles, I'll assess each principle and provide a compliance score based on the provided scoring system.

1. Lawfulness, Fairness, and Transparency
   - Assessment: The privacy policy explains what types of data are collected, how they are used, and how they are shared with third parties. However, the policy lacks specific legal bases for data processing, particularly under GDPR, and does not clearly state how transparency is ensured for all users, including children.
   - Score: 2 points (Partial compliance)

2. Purpose Limitation
   - Assessment: The policy outlines various purposes for which data is collected (e.g., personalization, ads, safety). While these purposes are generally clear, they are quite broad, and there is no mention of ensuring that data is not used beyond these purposes. The policy should specify more explicitly that data is not processed in ways incompatible with these purposes.
   - Score: 2 points (Partial compliance)

3. Data Minimization
   - Assessment: The policy does not provide enough detail on data minimization practices. It lists extensive types of data collected, but it doesn't demonstrate that only the data necessary for the stated purposes is collected.
   - Score: 0 points (Non-compliance)

4. Accuracy
   - Assessment: There is no specific mention in the privacy policy about how the company ensures the accuracy of the data it collects and processes. GDPR requires that reasonable steps be taken to ensure that inaccurate data is corrected or deleted.
   - Score: 0 points (Non-compliance)

5. Storage Limitation
   - Assessment: The policy mentions that data is stored until it is no longer necessary to provide services or until the user deletes their account. However, it does not provide

specific retention periods or criteria for determining the length of time personal data will be retained.
- Score: 2 points (Partial compliance)

6. Integrity and Confidentiality (Security)
   - Assessment: The policy does not explicitly detail the security measures taken to protect personal data. It mentions using data to promote safety and prevent unauthorized use but lacks a clear explanation of the specific technical and organizational security measures in place.
   - Score: 0 points (Non-compliance)

7. Accountability
   - Assessment: The policy does not demonstrate how the company ensures accountability for GDPR compliance. There is no mention of Data Protection Officers (DPOs), GDPR audits, or other mechanisms to ensure ongoing compliance with GDPR principles.
   - Score: 0 points (Non-compliance)

Final Compliance Score
- Total Score: 6 out of 21

The Fulldive VR privacy policy achieves partial compliance with some of the GDPR principles, but it falls short in critical areas like accuracy, storage limitation, integrity, confidentiality, and accountability. Significant improvements are needed to meet full GDPR compliance, especially considering this is an app available to children.

### 5.1.3 Case Studies of Non-Compliant Apps

Epic's Compliance Review: Epic's privacy policy stands out as a model of GDPR compliance, scoring a perfect 21/21. It excels in areas such as lawfulness, fairness, and transparency by providing clear explanations of data collection, use, and protection. The policy effectively addresses purpose limitation and data minimization by specifying the data collected is strictly necessary and within the defined purposes. Additionally, Epic demonstrates strong adherence to data accuracy, storage limitation, and security measures, ensuring that user data is protected and used appropriately. Their commitment to accountability is evident, with clear provisions for user inquiries and complaints, reflecting a high standard of GDPR compliance.

Fulldive's Compliance Review: On the other hand, Fulldive VR's privacy policy reveals significant compliance gaps, achieving only 6 out of 21 possible points. The policy partially complies with principles such as lawfulness and purpose limitation but lacks detailed legal bases for processing data under GDPR. Data minimization is a critical area where Fulldive falls short, as the policy does not sufficiently demonstrate that only necessary data is collected. The absence of provisions ensuring data accuracy and clarity on data retention further highlights its non-compliance. Additionally, the policy does not adequately address security measures, nor does it ensure accountability, such as appointing a Data Protection Officer or conducting GDPR audits, leading to a failure to meet key GDPR requirements.

Conclusion
The comparison between Epic and Fulldive VR highlights the significance of privacy measures when developing apps aimed at children use. Through a GDPR compliance strategy, Epic sets a high standard for other applications to follow. On the hand, Fulldive's policy is in need of substantial enhancements in areas such as data precision and security. To safeguard user privacy and adhere to GDPR regulations fully it is imperative for apps like Fulldive to update their privacy

policies making sure they align with all aspects of GDPR requirements—especially when it comes to protecting groups, like children.

## 5.2 Recommendations and Awareness

### 5.2.1 Recommendations for App Developers and Policymakers

App developers and policymakers should take steps to ensure GDPR compliance and safeguard children's privacy effectively by incorporating privacy protection, into app development from the beginning stages itself. Focusing on collecting only essential data to maintain accuracy and implementing strong security measures to protect children's personal information securely.

Those in charge of making policies should think about updating the rules to deal with privacy issues in online spaces that are commonly accessed by kids these days. Giving specific directions on how to inform children about privacy concerns based on their age group and handling kid's data more carefully along with strict punishments for not following the rules will encourage developers to prioritize privacy protection. Moreover, creating rules on how long data should be stored and the legal reasons, for processing data will help developers adhere to regulations effectively.

### 5.2.2 Strategies for Raising Awareness

It's really important to make sure parents and teachers are well informed about protecting childrens privacy by raising awareness among them through educational campaigns and campaigns that highlight the significance of reading and comprehending privacy policies – especially the ones related to apps designed for kids. Furthermore, schools can make a difference by including digital literacy in their teaching plans to educate children about the potential dangers of sharing data and how to keep their personal information safe, on the internet.

In addition to that partnerships among government agencies, charitable organizations and tech firms could result in the creation of user materials like manuals training sessions and engaging web applications that clarify privacy entitlements in an easy-to-understand manner suitable for children. Through educating individuals with information these programs encourage a mindset of being mindful of privacy ultimately playing a role in making online spaces safer, for kids.

# Chapter 6 – Conclusions

## 6.1 Summary of Objectives and Findings

This study aimed to assess the compliance of children's apps with the General Data Protection Regulation (GDPR) principles to identify potential compliance gaps and areas of improvement. The primary objective was to evaluate how well these apps adhere to the seven key GDPR principles: Lawfulness, Fairness, and Transparency; Purpose Limitation; Data Minimization; Accuracy; Storage Limitation; Integrity and Confidentiality; and Accountability. After reviewing the privacy policies of 30 popular childrens apps, in detail each app received a rating to assess its adherence level with scores allocated to establish if they fully complied partially complied or did not comply.

The results showed a pattern of apps not fully complying with rules in areas like Data Minimization and Accountability; many apps didn't take enough steps to collect only essential data and lacked clarity, on data accuracy and how incorrect data is fixed or removed. Apps that excel in performance such as Epic have shown adherence to all GDPR principles by presenting explicit and thorough privacy policies that are easy to understand and suitable for childrens use. On the other hand, apps like Fulldive VR have exposed significant non-compliance issues by falling short in important areas emphasizing the necessity, of stricter regulatory supervision and enforcement measures.

## 6.2 Limitations of the Study

While this study took an approach, to examine the subject matter at hand and highlighted various aspects of concern to consider carefully mentioned limitations that should be taken into account. Firstly, it focused on evaluating the accessible privacy policies of apps has its drawbacks as they might not paint an accurate picture of how these companies handle data or comply with regulations effectively. It could be challenging to assess their true level of adherence without insight into their internal data management practices and security protocols which may differ from what is outlined in their policies.

This research primarily centered on the principles outlined in GDPR; however, it's important to note that these standards may not cover all privacy regulations worldwide. There could be legal expectations for apps operating across various jurisdictions that might impact how they approach compliance strategies differently. Furthermore, the changing landscape of app updates and policy modifications implies that the study captures a moment in time and may not take into consideration continuous enhancements or declines, in compliance standards.

Privacy policies often do not accurately mirror how apps actually operate in real-life situations. They may include procedures and safeguards that are not consistently enforced or fully put into action by some companies. This discrepancy highlights the importance of conducting audits and verification checks to ensure that the data handling practices promised in privacy policies match up with the way data is actually managed.

Finally, this research did not take into account the opinions of users like how parents perceive privacy policies or how well children can navigate spaces securely. Integrating these viewpoints in studies could offer a more comprehensive outlook, on the practicality of privacy safeguards.

# Reference


Alhossen, M., Himi, R.Z. and Hasan, Z. 2021. *Child Safe Browser Extension: A Browser Extension to Detect Adultery and Violent Content to Make Safer Web for Children* (Doctoral dissertation, Brac University).

Allana, S. and Chawla, S. 2021. ChildShield: A rating system for assessing privacy and security of internet of toys. *Telematics and Informatics*, 56, p.101477.

Amâncio, F.M.P., Souza, A.P., Fantinato, M., Peres, S.M., Hung, P.C., do Rêgo, L.G.C. and Roa, J. 2023. Parental perception of children's privacy in smart toys in countries of different economic levels. *Technology in Society, 72*, p.102180.

Bélanger, F., Crossler, R.E., Hiller, J.S., Park, J.M. and Hsiao, M.S. 2013. POCKET: A tool for protecting children's privacy online. *Decision Support Systems*, 54(2), pp.1161-1173.

Bennett, C.J., 2018. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? *Information Polity*, 23(2), pp.239-246.

Buckley, G., Caulfield, T. and Becker, I., 2024. GDPR: Is it worth it? Perceptions of workers who have experienced its implementation. *arXiv preprint arXiv:2405.10225*.

*Child online safety: Data protection and privacy (2021) GOV.UK*. Available at: https://www.gov.uk/guidance/child-online-safety-data-protection-and-privacy (Accessed: 14 August 2024).

Crepax, T., Muntés-Mulero, V., Martinez, J. and Ruiz, A. 2022. Information technologies exposing children to privacy risks: domains and children-specific technical controls. *Computer Standards & Interfaces, 82*, p.103624.

Dempsey, J., Sim, G., Cassidy, B. and Ta, V.T. 2022. Children designing privacy warnings: Informing a set of design guidelines. *International Journal of Child-Computer Interaction, 31*, p.100446.

Desimpelaere, L., Hudders, L. and Van de Sompel, D. 2021. Children's perceptions of fairness in a data disclosure context: The effect of a reward on the relationship between privacy literacy and disclosure behaviour. *Telematics and Informatics, 61*, p.101602.

Ekambaranathan, A., Zhao, J. and Chalhoub, G., 2023. 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), pp.1-24.

Frey, S. (2021, May 6). New safety section in Google Play will give transparency into how apps use data. *Android Developers Blog*. https://android-developers.googleblog.com/2021/05/new-safety-section-in-google-play-will.html

Hossain, M.S. and Haberfeld, C. 2020, September. Touch behaviour based age estimation toward enhancing child safety. *In 2020 IEEE International Joint Conference on Biometrics (IJCB)* (pp. 1-8). IEEE.

Iwata, M., Arase, Y., Hara, T. and Nishio, S. 2010. Web browser for children using bubble metaphor. *International Journal of Web Information Systems, 6*(1), pp.55-73.

Jibb, L., Amoako, E., Heisey, M., Ren, L. and Grundy, Q., 2022. Data handling practices and commercial features of Apps related to children: A Scoping review of content analyses. *Archives of disease in childhood, 107*(7), pp.665-673.

Kaaniche, N., Laurent, M. and Belguith, S. 2020. Privacy enhancing technologies for solving the privacy-personalization paradox: Taxonomy and survey. *Journal of Network and Computer Applications, 171*, p.102807.

Kollnig, K., 2021. Tracking in apps' privacy policies*. arXiv preprint arXiv:2111.07860.*

Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C. and Shadbolt, N., 2021. Before and after GDPR: tracking in mobile apps. *arXiv preprint arXiv:2112.11117.*

Krämer, J., 2024. The death of privacy policies: How app stores shape GDPR compliance of apps. *Krämer, J. (2024). The death of privacy policies: How app stores shape GDPR compliance of apps. Internet Policy Review,* 13(2).

*Lex - 02016R0679-20160504 - en - EUR-lex (2016) EUR*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 (Accessed: 14 August 2024).

Li, H., Yu, L. and He, W., 2019. The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, 22(1), pp.1-6.

Liu, M., Wang, H., Guo, Y. and Hong, J., 2016, February. Identifying and analyzing the privacy of apps for kids. In *Proceedings of the 17th international workshop on mobile computing systems and applications* (pp. 105-110).

Medjkoune, T., Goga, O. and Senechal, J. 2023, November. Marketing to children through online targeted advertising: Targeting mechanisms and legal aspects. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (pp. 180-194).

Mehrnezhad, M. 2020, September. A cross-platform evaluation of privacy notices and tracking practices. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 97-106). IEEE.

O'Hara, K., 2022. Privacy, privacy-enhancing technologies & the individual.

Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C. and Gill, P., 2018, February. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In *The 25th annual network and distributed system security symposium (NDSS 2018).*

Xu, H., Crossler, R.E. and BéLanger, F., 2012. A value sensitive design investigation of privacy enhancing tools in web browsers. *Decision support systems, 54*(1), pp.424-433.ijk
Zhang-Kennedy, L., Abdelaziz, Y. and Chiasson, S., 2017. Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction*, 13, pp.10-18.

Zhao, J., Duron, B. and Wang, G., 2022, June. KOALA hero: Inform children of privacy risks of mobile apps. In *Proceedings of the 21st Annual ACM Interaction Design and Children Conference* (pp. 523-528).

Zimmerle, J.C. and Wall, A.S., 2019. What's in a policy? evaluating the privacy policies of children's apps and websites. *Computers in the Schools, 36*(1), pp.38-47.