Huduma Namba Season 2? Assessing the Adequacy of Kenya's Legal Framework in Protecting Children's Privacy in the Maisha Card Digital Identity System

Submitted in partial fulfilment of the requirements for the Bachelor of Laws Degree, Strathmore University Law School

By

Wambeti Mercy Alice

145801

Prepared under the supervision of

Mr. Moses Antony Odhiambo

Table of Contents

Declaration

I, WAMBETI MERCY ALICE, do hereby declare that this research is my original work and that to the best of my knowledge and belief, it has not been previously, in its entirety or in part, been submitted to any other university for a degree or diploma. Other works cited or referred to are accordingly acknowledged.

Signed:  .....

Date: .....26/03/2025.....

This dissertation has been submitted for examination with my approval as University Supervisor.

Signed:  .....

Moses Antony Odhiambo

Date: .....**26th March, 2025**.....

Acknowledgements

I sincerely thank Mr. Moses Antony, my supervisor, for his crucial advice, encouragement, and helpful criticism during this research process. His advice and support have greatly influenced the direction of this dissertation.

My family's steadfast patience, belief in me, and moral support are also greatly appreciated. Throughout this process, I have found strength and inspiration in their encouragement.

Above all, I give thanks to God Almighty for His grace, wisdom, and strength that have sustained me through every step of this journey. Without His guidance, this work would not have been possible. Great is His faithfulness.

List of cases

Nubian Rights Forum and 2 others v The Attorney General and 6 others (2020) eKLR

R v Joe Mucheru and others exparte Immaculate Kassait DPC (2021) eKLR

Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others (2016) eKLR.

S. and Marper v UK, ECtHR Judgement 4 December 2008.

Justice K.S. Puttaswamy and Another v Union of India (UOI) and Others (2018), The Supreme Court of India.

Robinson, Julian v The Attorney General of Jamaica (2018), The Supreme Court of Judicature Of Jamaica.

Gillick v West Norfolk and Wisbech Area Health Authority and another (1985), The United Kingdom House of Lord.

List of Legal Instruments

African Charter on the Rights and Welfare of the Child, 1990.

Children Act, 2022.

Computer Misuse and Cybercrimes Act, 2018.

Constitution of Kenya, 2010.

Data Protection Act, 2019.

Data Protection (Civil Registration) Regulations, 2020.

General Data Protection Regulation, 2016 (EU).

Registration of Persons (Amendment) Rules, 2024.

The Aadhaar (Enrolment & Update) Regulation, 2016 (India).

United Nations Convention on the Rights of the Child, 1989.

List of Abbreviations and Acronyms

AI	Artificial Intelligence
ACRWC	African Charter on the Rights and Welfare of the Child
BCRs	Binding Corporate Rules
CRC	Convention on the Rights of the Child
CRIA	Child Right Impact Assessment
CJEU	Court of Justice of the European Union
DPC	Data Protection Commissioner
DPIA	Data Protection Impact Assessment
DPA	Data Protection Act
DPA	Data Protection Authorities
DNA	Deoxyribonucleic Acid
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
FRA	European Agency for Fundamental Rights
GDPR	General Data Protection Regulation
ID4D	The Identity for Development
ICT	Information and Communication Technology
NIIMS	National Integrated Identity Management System
OECD	Organization for Economic Cooperation and Development
ODPC	Office of the Data Protection Commissioner
RPA	Registration of Persons Amendment Rules
SCCs	Standard Contractual Clauses
UPI	Unique Personal Identification

Abstract

This study examines the implications of Kenya's digital identity systems, particularly the Maisha Card or Unique Personal Identifier (UPI), on children's right to privacy. It highlights the inadequacy of Kenya's legal framework in addressing risks such as identity theft, profiling, and mission creep. Key research questions include the potential consequences of failing to protect children's privacy, the adequacy of Kenya's legal protections, and lessons from the EU's GDPR.

Using a qualitative approach, this study analysed Kenyan laws, including the Constitution, the Data Protection Act, and the Children's Act, alongside case law and GDPR provisions. The findings reveal that while Kenya's legal framework provides foundational protections, it lacks critical child-specific safeguards, such as Children's Rights Impact Assessments (CRIAs) and detailed provisions for protecting children's biometric data. The study also highlights gaps in institutional coordination between the Office of the Data Protection Commissioner and child protection bodies, which hinder a unified approach to safeguarding children's privacy.

The study recommends legal reforms to align Kenya's framework with international best practices, including child-specific data protection measures and promoting data literacy. These reforms are critical to ensuring digital identity systems uphold children's privacy rights and mitigate risks associated with datafication.

***Keywords**: Digital identity, children's privacy, data protection, GDPR, Kenya.*

Chapter 1: Introduction

1.1 Background

In today's rapidly digitising world, digital identity systems have evolved as an essential component of modern life. These systems play a critical role in defining an individual's identity across multiple platforms. India's Aadhaar system stands out as the world's most extensive biometric identification program.[1] Aadhaar allocates each person a unique 12-digit number that is connected to their biometric and demographic information, allowing them to access a variety of services such as banking, healthcare, and social assistance.[2] The simplicity and efficiency that these technologies provide have made digital identities increasingly important in the modern day.

However, as digital identity systems grow increasingly prevalent, they raise serious issues about privacy and data security, particularly among vulnerable populations such as children. According to the Organization for Economic Cooperation and Development (OECD) gauge, the amount of data globally increased eightfold between 2010 and 2015.[3] It was projected that the number of connected devices and other emerging technologies will increase 40 times by 2020.[4] This quickly evolving picture isn't merely the result of the amount of data; advances in processing methods also play a role, allowing analysts to delve deeper into the data that is already available. Although datafication affects everyone, today's children are among the first to undergo it from birth.[5] Children are travelling down uncharted territory, and they have no idea how this will affect them many years from now.

In the digital age, the concept of identity has evolved significantly, with digital identity systems such as the Maisha Card, also known as the Unique Personal Identifier (UPI), in Kenya becoming increasingly prevalent.[6] These systems, while offering numerous benefits, also raise critical

[1] Bhandari V and Sane R, 'A Critique of The Aadhaar Legal Framework' 13 *National Law School of India Review* 1, 2019, 72.
[2] Council on Foreign Relations, *How India's Controversial Biometric ID System Can Help Women*, 2018, 25.
[3] OECD, *Data Driven Innovation: Big Data for Growth and Well-Being*, 6 October 2015, 2.
[4] OECD, *Data Driven Innovation: Big Data for Growth and Well-Being*, 6 October 2015, 2.
[5] Children's Commissioner for England, *Who knows what about me? A Children's Commissioner report into the collection and sharing of children's data*, November 2018, 3.
[6] Odhiambo R, 'Kenya's Digital Identity Revolution: Balancing Progress and Human Rights' Social Science Research Network, 2023, 4.

questions about privacy, notably for at-risk groups such as children.[7] Privacy is a fundamental right that enables individuals to exercise autonomy, dignity and self-determination.[8] It is also a prerequisite for the realisation of other rights, such as freedom of expression,[9] association[10] and access to information.[11]

The advent of digital identity systems in Kenya, marked by the Introduction of the Huduma Namba and the rollout of the UPI, has been a subject of national interest. The Huduma Namba, a unique identifier for all Kenyan citizens and foreign residents, was initially met with enthusiasm. However, its implementation was fraught with issues, one of them being privacy concerns, culminating in the landmark *Nubian Rights Forum and 2 others v The Attorney General and 6 others (2020)*[12] case. The High Court of Kenya in this case expressed serious concerns with the absence of a thorough data protection framework at the time, while also acknowledging the potential benefits of the Huduma Namba.[13] The court decided that the Data Protection Act had to be strictly followed in the gathering and processing of personal data through the Huduma Namba system.[14]

The Kenyan government's apparent dismissal of privacy risk assessments, as evidenced in the *R v Joe Mucheru and others exparte Immaculate Kassait DPC (2021)* case on Huduma Namba where it was found that a Data Protection Impact Assessment (DPIA) was not conducted, further exacerbates these concerns.[15] This lack of due diligence and oversight could lead to severe infringements on children's privacy rights.[16]

[7] Mutung'u G, 'Digital Identity in Kenya: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa' Research ICT Africa, November 2021, 20 — https://researchictafrica.net/publication/digital-identity-in-kenya-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/ on 21 December 2023.
[8] Privacy International, *What is Privacy?*, 23 October 2017, 1.
[9] Article 33, *Constitution of Kenya* (2010)
[10] Article 36, *Constitution of Kenya* (2010)
[11] Article 35, *Constitution of Kenya* (2010)
[12] *Nubian Rights Forum and 2 others v The Attorney General and 6 others* (2020) eKLR.
[13] (2020) eKLR.
[14] (2020) eKLR.
[15] *R v Joe Mucheru and others exparte Immaculate Kassait (DPC)* (2021) eKLR.
[16] Berkeley Law, *Digital Identity and the legal obligation to conduct a human rights impact assessment in Kenya*, April 2023, 12.

The introduction of the Maisha Card, or UPI, which will be granted at birth, adds another layer of complexity to this issue. While the UPI promises to streamline service delivery and enhance inclusivity, it also raises questions about the state's readiness to protect children's privacy rights in the digital age.[17] This study will provide a comprehensive analysis of these issues, contributing to the discourse on digital identity systems and children's right to privacy in Kenya. It will draw on a range of sources, including legal texts, case law, and empirical data, to provide an informed and nuanced perspective on this critical issue.

1.2 Problem Statement

Digital identity systems, such as the Maisha Card (Unique Personal Identifier) in Kenya, have become critical tools for enhancing accessibility and efficiency in today's rapidly evolving digital environment. However, these systems pose significant privacy concerns, particularly for vulnerable groups like children. Despite Kenya's legislative efforts, the current legal framework, including Sections 31 and 48 of the Data Protection Act, lacks the robustness needed to adequately protect children's data.[18] Assessments specific to children's vulnerabilities are not required by Section 31, which requires Data Protection Impact Assessments (DPIAs) for high-risk processing. Furthermore, Section 48, which governs cross-border data transfers, fails to impose stricter safeguards for international data flows involving children's biometric and personal information.[19]

These regulatory gaps heighten the risks of unauthorized access, identity theft, profiling, and mission creep, with potentially severe consequences for children's privacy, security, and future opportunities. Addressing these shortcomings is imperative to safeguard children's rights in a digital age characterized by the proliferation of data-driven systems. To this end, this study undertakes a comparative analysis of Kenya's legal framework and Europe's General Data Protection Regulation (GDPR) to identify lessons and propose reforms that enhance the protection of children's privacy in Kenya.

[17] Wabulengo J, 'Is The Huduma Namba Back?' KICTANet, 11 July 2023 – <https://www.kictanet.or.ke/is-the-huduma-namba-back/ > on 21 December 2023.
[18] *Data Protection Act* (Act No.24 of 2019).
[19] Section 48, *Data Protection Act* (Act No.24 of 2019).

1.3 Research Objectives

1. To examine the key risks associated with digital identity systems, particularly in relation to children's right to privacy, and to identify strategies and safeguards that can effectively mitigate these risks.

2. To examine the current legal framework and its adequacy in the protection of children's right to privacy in providing for Digital IDs.

3. To analyse the best practice lessons from Europe's data protection legislation (GDPR) with regard to how children's right to privacy is upheld.

4. To suggest possible reforms to the law to address the legal gaps identified in Kenya's legislation in protecting children's right to privacy in the current digital identity era.

1.4 Research Questions

1. What are the key risks associated with digital identity systems, particularly concerning children's right to privacy, and how can these risks be mitigated?

2. Is the current legal framework adequate and comprehensive enough in the protection of children's right to privacy in providing for Digital IDs?

3. What lessons can be learned from Europe's data protection legislation (GDPR) with regard to how children's right to privacy is upheld?

4. Based on the findings, what recommendations can be made on possible legislative reforms that Kenya may undertake to address any identified gaps in Kenya's legislation in protecting children's right to privacy in the current digital identity era?

1.5 Hypothesis

The implementation of digital identity systems in Kenya may influence the protection of children's privacy rights by introducing both potential benefits and risks. This study aims to assess how these systems impact privacy safeguards and identify specific privacy concerns and challenges associated with their adoption.

1.6 Justification/significance of the research

This research is significant because it considers a current and important problem that concerns the rights and lives of millions of children in Kenya. To this end, it explores how digital identity systems, such as the Maisha Card, impact children's right to privacy and, in doing so, informs the debate on how to optimize the positives and minimize the negatives of datafication in the digital world. The research is also justified as it fills the gap in the current academic literature which has not fully explored the views and experiences of children in relation to digital identity systems. In addition, based on a thorough assessment of the legal and regulatory framework, the government's practices, and the risks of digital identity systems, it provides valuable insights and recommendations for improving the protection of children's privacy rights in Kenya. Therefore, this research is useful for policymakers, practitioners, academics, and civil society members who are working to promote children's rights in conjunction with digital technologies.

1.7 Theoretical Framework

Legal Positivism

The legal positivist view, which maintains that laws are rules made by humans and that there is no intrinsic or required relationship between morality and the law, serves as the theoretical foundation for the present study.[20] Prominent academics like John Austin and H.L.A. Hart have espoused legal positivism, which emphasizes that a law's legitimacy is established by its origin rather than its content. Hart makes a distinction between fundamental rules, which dictate conduct and secondary rules that regulate the creation, alteration, and enforcement of primary rules. He contends that legal systems are supported by a rule of recognition, which validates the legitimacy of legal power.[21] In the context of this study, legal positivism provides a framework to assess the adequacy of Kenya's legal framework in safeguarding children's privacy in digital identity systems, without invoking moral arguments about privacy but rather focusing on the sufficiency of the legal provisions themselves.

[20] Kramer M, 'The Legal Positivism of H.L.A Hart' University of Cambridge Faculty of Law, Research Paper No. 11/2019, March 2019, 1 — https://dx.doi.org/10.2139/ssrn.3347611 on 1 March 2019.
[21] Dimock S, *Classic Readings and Cases in Philosophy of Law,* York University, New York, 2007, 53.

However, legal positivism has faced criticisms, most notably from natural law theorists like Lon Fuller and Ronald Dworkin, who argue that law cannot be entirely divorced from moral considerations, particularly in cases where human rights, such as privacy, are at stake.[22] These critics contend that laws should inherently reflect moral principles to ensure justice.[23] In relation to this study, while legal positivism helps in analysing whether Kenya's legal framework complies with statutory requirements, the criticisms emphasise the need to consider broader ethical implications, especially when dealing with vulnerable populations such as children. The theory directly relates to this research by offering a lens through which to examine whether the provisions in Kenya's legal framework are not only legally valid but also sufficient to protect children's privacy rights in an increasingly digitised world.

1.8 Literature Review

The collection and protection of children's data in digital identity systems have sparked significant scholarly debate, with a consensus emerging on the need for less invasive means of data collection to safeguard their privacy. Stoilova et al. emphasise that privacy risks for children are exacerbated by the extensive collection of personal data, advocating for systems that prioritise data minimisation and transparency.[24] Similarly, Bondre et al. critique centralised data systems like India's Aadhaar, proposing decentralised systems that collect biometric data only when absolutely necessary.[25] These approaches highlight the potential for achieving the objectives of digital identity systems while reducing privacy intrusions, particularly for vulnerable groups like children.

1.8.1 Conceptualizing Privacy and Children's Rights in Digital Contexts

Privacy has long been recognised as a fundamental human right, with Warren and Brandeis famously defining it as "the right to be let alone."[26] Modern interpretations, such as those by Solove, expand this definition to encompass control over personal information, particularly in the

[22] Priel D, 'Reconstructing Fuller's Argument Against Legal Positivism' 26 *Canadian Journal of Law & Jurisprudence* 2, 2013, 399-413.
[23] Priel D, 'Reconstructing Fuller's Argument Against Legal Positivism', 399.
[24] Stoilova M, Nandagiri R and Livingstone S, 'Children's understanding of personal data and privacy online – a systematic evidence mapping' 24(4) *Information Communication & Society*, 2019, 557-575.
[25] Bondre A, Pathare S and Naslund J, 'Protecting Mental Health Data Privacy in India: The Case of Data Linkage With Aadhaar' 9 *Global Health: Science and Practice* 3, 2021, 467-480.
[26] Warren S. D and Brandeis L. D, 'The Right to Privacy' 4(5) *Harvard Law Review,* 1890, 193–220.

context of digital data.[27] Children's privacy, however, presents unique challenges, as minors often lack the capacity to fully comprehend the implications of data collection and processing. Livingstone and Third emphasise the importance of framing children's privacy within the broader context of their evolving capacities and best interests,[28] as articulated in the United Nations Convention on the Rights of the Child (UNCRC).[29]

Scholars such as Bygrave argue that privacy frameworks must evolve to address the complexities of the digital age, particularly for children.[30] The collection of personal data at birth, as seen in systems like Kenya's Maisha Card, raises ethical questions about autonomy, and the lifelong implications of digital footprints. Goggin and Hjorth further highlight the tension between the benefits of digital identity systems and the risks they pose to individual rights, particularly when sensitive data is involved.[31] These discussions underscore the need for child-centric legal and procedural safeguards in digital identity systems to address these unique challenges.

1.8.2 Risks of Data Centralisation

Centralised data systems, a hallmark of many digital identity frameworks, are frequently criticized for their inherent vulnerabilities. Solove identifies centralized repositories as prime targets for breaches, where a single point of failure can expose the personal data of millions.[32] For children, such breaches can have profound and lifelong implications, including identity theft, profiling, and unauthorized access.

Beyond security risks, centralized systems create power asymmetries by granting governments and corporations unprecedented control over personal information.[33] For children, the long-term risks are particularly acute, as their digital footprints, collected from birth, can shape their identities and

[27] Solove D. J, *Understanding Privacy*, Harvard University Press, Cambridge, 2008.
[28] Livingstone S and Third A, 'Children and young people's rights in the digital age: an emerging agenda' New Media and Society, 2017, 8.
[29] Article 3, *United Nations Convention on the Rights of the Child*, 20 November 1989, General Assembly resolution 44/25.
[30] Bygrave A, *Data Privacy Law: An International Perspective*, Oxford Unity Press, London, 2014.
[31] Goggin G and Hjorth L, *The Routledge Companion to Mobile Media*, 1st ed, Routledge, New York, 2014.
[32] Solove D. J, 'The Digital Person: Technology and Privacy in the Information Age' NYU Press, GWU Law School Public Law Research Paper 5, 2004, 48 – https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications – on 25 December 2024.
[33] Mordini and Tzovaras, *Second Generation Biometrics: The Ethical, Legal and Social Context*, 81.

opportunities in ways beyond their control.[34] Lyon terms this dynamic as "surveillance creep," where incremental expansions of data-use normalize invasive practices, raising profound ethical concerns about the boundaries of data collection.[35]

1.8.3 Legal Frameworks and Gaps in Protecting Children's Privacy

Legal frameworks addressing children's privacy in digital identity systems have evolved to respond to the increasing risks associated with data collection and biometric registration.[36] The UNCRC recognizes the right to privacy under Article 16,[37] while General Comment No. 25 highlights the need for stronger protections in digital environments, emphasizing the importance of safeguards against data misuse and exploitation.[38] Scholars have argued that while international legal instruments provide a foundation for children's privacy rights, many national legal frameworks lack explicit child-specific protections, particularly in areas such as biometric data collection, data minimization, and oversight of centralized identity databases.[39]

Studies highlight that many jurisdictions fail to provide comprehensive legal standards for biometric data processing, exposing children to risks such as profiling, identity theft, and long-term surveillance.[40] Scholars have further critiqued the absence of robust oversight mechanisms, noting that fragmented regulatory approaches often lead to inconsistencies in data protection measures.[41] The lack of clear data minimisation requirements and purpose limitation principles in

[34] UNICEF, *Children in a Digital World*, 2017, 41.
[35] Lyon D, *Surveillance Studies: An Overview*, Polity Press, United Kingdom, 2007.
[36] Anand N and Brass I, 'Responsible Innovation for Digital Identity Systems' 35 *Cambridge University Press* 3, 2021, 5.
[37] Article 16, *United Nations Convention on the Rights of the Child*, 20 November 1989, General Assembly resolution 44/25.
[38] *General Comment No. 25 on Children's Rights in the Digital Environment,* 2 March 2021, CRC/C/GC/25.
[39] Livingstone S, Stoilova M and Nandagiri R, 'Children's Data and Privacy Online: Growing Up in a Digital Age' London School of Economics and Political Science, 2019, 28.
[40] Carmona M, 'Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection' Extension of Social Security, Working Paper No. 59, 2018, 37 — https://www.researchgate.net/profile/Magdalena-Sepulveda/publication/325909014_Is_biometric_technology_in_social_protection_programmes_illegal_or_arbitrary_An_analysis_of_privacy_and_data_protection/links/5b76eae24585151fd119b29e/Is-biometric-technology-in-social-protection-programmes-illegal-or-arbitrary-An-analysis-of-privacy-and-data-protection.pdf on 30 January 2025.
[41] Carly Nyst, 'Privacy, Protection Of Personal Information And Reputation' United Nations Children's Fund, Discussion Paper Series: Children's Rights and Business in a Digital World, 2017, 13 – https://www.unicef.org/childrightsandbusiness/media/281/file/UNICEF-CRB-Digital-World-Series-Privacy.pdf on 23 December 2024.

many legal systems exacerbates concerns over the storage and retention of children's data in digital identity systems.[42] These gaps underscore the need for legislative reforms that incorporate stronger child-specific privacy protections and ensure digital identity systems prioritize children's best interests.

1.8.4 Ethical Implications of Data Collection in Digital Identity Systems

The ethical implications of biometric data collection in digital identity systems are extensively explored in the literature. Mordini and Tzovaras underscore the sensitivity of biometric identifiers, which are both permanent and difficult to secure.[43] Unlike passwords, biometric data cannot be altered once compromised, creating lifelong vulnerabilities for children.

Zuboff critiques the commodification of personal data in "surveillance capitalism," where children's information is used for economic and political gain.[44] Similarly, Eubanks warns that algorithmic profiling in public systems perpetuates systemic inequalities, disproportionately impacting marginalized groups.[45] For Kenya, these concerns are particularly relevant given the integration of biometric data into centralized databases under the Maisha Card system, where insufficient safeguards increase the risk of misuse and discrimination.

1.8.5 Emerging Best Practices and Technological Safeguards

Despite the risks, the literature offers solutions that prioritize privacy and security. Pasquale advocates for transparency and accountability in data processing, emphasizing privacy by design and default as standard requirements.[46] UNICEF recommends the adoption of Child Rights Impact Assessments (CRIAs) as a critical tool for evaluating how data processing activities affect

[42] Hildebrandt M and Koops B, 'The Challenges of Ambient Law and Legal Protection in the Profling Era' 73 *The Modern Law Review* 3, 2010, 442.
[43] Mordini E and Tzovaras D, *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer Science & Business Media, London, 2012, 16.
[44] Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.
[45] Eubanks V, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor,* St. Martin's Press, New York, 2018.
[46] Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

children, ensuring that their rights and best interests are prioritized and upheld in all decisions involving their personal data.[47]

Technological safeguards also feature prominently in best practices. Schneier highlights encryption and pseudonymization as essential tools for mitigating risks and reducing the likelihood of unauthorized access to sensitive data.[48] Livingstone and Third underscore the necessity of involving children and their guardians in data protection decisions, advocating for transparency and simplicity in privacy policies.[49]

The GDPR serves as a model for integrating these best practices into legal frameworks. Its emphasis on data minimisation, purpose limitation, and accountability provides a roadmap for jurisdictions like Kenya.[50] By adopting GDPR-inspired measures, Kenya can address critical gaps in its framework, ensuring that digital identity systems align with the principles of child protection and privacy.

1.8.6 Research Gap

The literature reveals a clear need for less invasive methods of collecting and processing children's data in digital identity systems. While centralized systems offer efficiency and interoperability, they also create significant risks, particularly for children, whose data is more vulnerable to misuse and long-term harm.[51] Comparative analyses of frameworks like the GDPR demonstrate the importance of incorporating child-specific safeguards, such as tailored DPIAs. This dissertation builds on these insights, proposing a legal and procedural framework for Kenya that prioritizes children's privacy while leveraging the benefits of digital identity systems.

[47] UNICEF, *Developing Global Guidance for Child Rights Impact Assessments in Relation to the Digital Environment*, April 2024, 6.
[48] Schneier B, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W, Norton & Company, New York, 2016.
[49] Livingstone S and Third A, 'Children and young people's rights in the digital age: an emerging agenda' New Media and Society, 2017, 8.
[50] Article 5, *General Data Protection Regulation* (EU) (2016/679).
[51] Goodell G and Aste T, 'A Decentralized Digital Identity Architecture', 7.

1.9 Research Methodology

This research adopts a doctrinal legal research method, involving a systematic and critical analysis of legal texts, principles, and concepts to address the research objectives. The primary sources of data include the Constitution of Kenya, the Children's Act, the Data Protection Act, and relevant case law from Kenyan courts. These legal instruments are examined to evaluate their adequacy in protecting children's right to privacy in the context of digital identity systems. Secondary sources of data include academic articles, books, reports, and policy documents on digital identity systems and children's privacy rights in Kenya and other jurisdictions. These materials provide insights into international best practices, legal frameworks, and scholarly critiques. The study also incorporates a comparative analysis of Europe's GDPR. The GDPR is selected for its comprehensive data protection framework and explicit provisions for safeguarding children's privacy.

1.10 Limitations

This research has some limitations that may affect the validity and generalizability of the findings. The literature on digital identity systems and children's right to privacy in Kenya is scarce and mostly dated, which may hinder the comprehensiveness and currency of the analysis. The research may be subject to bias due to the researcher's personal views and experiences, which may influence the interpretation and presentation of the data. These limitations should be considered when evaluating the results and implications of the study.

1.11 Chapter Breakdown

Chapter 1: The Maisha Card system and its effects on Kenyan children's right to privacy are the subject and scope of the research, which is introduced in this chapter. The study's backdrop and issue statement are presented in this chapter. It describes the study's objective, questions, hypothesis, and rationale. It is essentially an overview of the research.

Chapter 2: This chapter delves into the history, design, and intended purpose of the Maisha Card, emphasizing its role in Kenya's digital identity ecosystem. It examines the system's features, including data collection, storage, and use, with a focus on children as data subjects. The chapter also explores risks such as unauthorised access, identity theft, mission creep, and profiling,

contextualizing them within the broader challenges of implementing digital identity systems in Kenya.

Chapter 3: The Adequacy and Compliance of Kenya's Laws and Policies on the Maisha Card System and Children's Right to Privacy. This chapter will analyse the legal and regulatory framework that governs the Maisha Card system and its impact on children's right to privacy in Kenya.

Chapter 4: This chapter compares Kenya's Data Protection Act to the GDPR, focusing on key provisions such as data minimization, cross-border data flows and special protections for children. It explores how the GDPR's child-centric safeguards, such as explicit rights for children and robust oversight mechanisms, address challenges faced in Kenya. The chapter identifies best practices from the GDPR that could inform improvements to Kenya's legal framework.

Chapter 5: This chapter proposes actionable recommendations to enhance Kenya's legal framework for protecting children's privacy in the Maisha Card system. Drawing from the GDPR and international best practices, it suggests measures such as stricter oversight, child-specific provisions, and mechanisms to address risks like cross-border data flows and indefinite data retention. The chapter concludes by reflecting on the study's findings, emphasizing the importance of aligning Kenya's digital identity initiatives with global standards for children's data protection.

Chapter 2:

Privacy Risks and Consequences for Children in Digital Identity Ecosystems

2.1 Introduction

This chapter sets out to identify the potential implications of failing to uphold children's right to privacy in digital identity systems. It explores the vulnerabilities and risks associated with digital identity systems, particularly for children, whose personal and sensitive data is increasingly subjected to datafication without adequate safeguards. The chapter begins by establishing a foundational understanding of digital identity systems, focusing on the concepts of personal and sensitive data and their significance in these systems. It then delves into key risks such as unauthorised access, identity theft, profiling, and mission creep, analysing how these risks arise and their potential implications. To provide a nuanced perspective, the chapter examines specific sources of risk, including inherent vulnerabilities in data collection processes, storage and access weaknesses, and risks associated with data sharing with third parties or cross-sector integration. Following this, it discusses the role of privacy by design and data minimization principles in mitigating these risks, highlighting their relevance in safeguarding children's data.

The chapter also addresses the tension between consent and legal necessity in the context of children's data, recognizing the unique challenges posed by their evolving capacity to make informed decisions. It further examines broader concerns around surveillance, misuse, and lack of accountability in digital identity systems. By examining these aspects, the chapter provides a comprehensive roadmap of the risks and implications of digital identity systems while laying the groundwork for proposing solutions in subsequent chapters.

2.2 Understanding Personal and Sensitive Personal Data in Digital Identity Systems

Any data that can distinguish or trace an individual, either explicitly or implicitly, is classified as personal data.[52] Some instances are names, identification codes, address-related data, and web-based identifiers.[53] Sensitive personal data, conversely, encompasses information that reveals

[52] Article 4(1), *General Data Protection Regulation* (EU) (2016/679).
[53] Article 4(1), *General Data Protection Regulation* (EU) (2016/679).

more intimate aspects of an individual's identity, like ethnic or racial heritage, political beliefs, religious affiliation, health records, sexual orientation, and biometric markers used for identification.[54] The processing of sensitive data is subject to stricter legal requirements due to its potential to cause significant harm if misused.

In the context of digital identity systems, these distinctions are crucial because the collection of sensitive data often involves greater risks. Biometric identifiers such as fingerprints or facial recognition data are particularly vulnerable, as they are immutable and can serve as lifelong markers for individuals.[55] There is emphasis on the need for heightened protections for such data, given its unique role in linking individuals to their digital and physical identities.[56]

2.3 Key Risks in Digital Identity Systems

Digital identity systems are transformative tools for managing identities in the digital age. However, their implementation often carries inherent risks that, if unaddressed, could undermine the right to privacy and other fundamental freedoms. This section examines four critical risks; unauthorised access, identity theft, profiling, and mission creep, highlighting their mechanisms, vulnerabilities, and implications.

2.3.1 Unauthorised Access

Unauthorised access is one of the most significant risks associated with digital identity systems, particularly when processing children's data. These systems often store sensitive information, including biometric identifiers and personal details, which, if accessed by unauthorized parties, can lead to serious consequences.[57] Children are especially vulnerable due to their limited awareness of privacy risks and their inability to recognize or respond to breaches.[58] According to

[54] Article 9, *General Data Protection Regulation* (EU) (2016/679).
[55] Mordini E and Tzovaras D, *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer Science & Business Media, London, 2012, 16.
[56] World Bank, *Principles on Identification for Sustainable Development: Toward The Digital Age*, February 2021, 6.
[57] Omotunde H and Ahmed M, 'A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond' 2023 *Mesopotamian Journal of Cybersecurity,* 2023, 115.
[58] Livingstone S and Third A, 'Children and young people's rights in the digital age: An emerging agenda' 19 *New Media & Society* 5*,* 2017, 660.

Solove, unauthorized access to children's data can have long-term impacts, including identity fraud, exploitation, and reputational harm, with effects extending into adulthood.[59]

Digital identity systems are frequently structured around centralized databases, which are attractive targets for malicious actors.[60] The high volume and sensitive nature of the data stored make these systems especially prone to large-scale breaches. Unauthorised access to such databases exposes children's immutable biometric data, such as fingerprints or facial images, which cannot be replaced once compromised.[61]

Unlike passwords or other credentials, these identifiers remain permanently tied to the individual, amplifying the risks and potential consequences of unauthorized access.[62] Another major concern is the adequacy of cybersecurity measures in digital identity systems. Inadequate technical safeguards, such as weak encryption standards, insufficient authentication protocols, and a lack of routine security audits, exacerbate vulnerabilities to unauthorized access.[63]

Unauthorised access also raises concerns about mission creep, where data collected for one purpose is repurposed for others without appropriate oversight or consent.[64] This risk is heightened when third parties gain unauthorized access to children's data for unintended uses, such as targeted advertising or profiling. To mitigate these risks, scholars advocate for privacy-by-design principles and regular security audits as essential tools to enhance protections for children's data in digital identity systems.[65] Moreover, advanced multi-layered access controls tailored to the sensitivity of children's data are increasingly recognized as critical in addressing the risks posed by unauthorized access.[66]

---

[59] Solove D, 'The end of privacy?' 299 *Scientific American* 3, 2008, 100.
[60] Omotunde H and Ahmed M, 'A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond', 115.
[61] Alen E, 'Biometric Data Collection and Use in The Age of Social Media: The Increasing Need for Coppa Updates Given The Decreasing Age Of Internet Users' 49 *Rutgers Computer & Technology Law Journal* 2, 2023, 374.
[62] Rao U and Nair V, 'Aadhaar: Governing with Biometrics' 42 *Journal of South Asian Studies* 3, 2019, 469.
[63] Sharif U, 'The Effects of Security Breaches on Data Integrity' Published LLM Thesis, University of the Cumberlands, Kentucky, 2024, 17.
[64] Hyesun C, Prabu D, Tsai-Wei Ling, 'Acceptance of AI-Powered Facial Recognition Technology in Surveillance Scenarios: Role Of Trust, Security, And Privacy Perceptions' 79 *Technology in Society*, 2024.
[65] Thomas I, Ramesh H, Wilson C and Alloul E, 'Protecting Privacy Rights in the Digital Age' Max Bell School of Public Policy, 2023, 20.
[66] Odudu Q, 'Technological Solutions for Protecting Children from Online Predators: Current Trends and Future Directions' Social Science Research Network, 2024, 34.

2.3.2 Identity Theft

Identity theft happens when someone's private information is illegally obtained and utilized to pretend to be someone else, often for deceptive purposes such as financial fraud, unauthorized access to services, or criminal activities.[67] Identity theft extends beyond mere data breaches to encompass acts of impersonation, where the perpetrator deliberately misrepresents themselves as the victim to gain benefits or evade liability.[68] This phenomenon often results in profound harm, including financial losses, reputational damage, psychological distress, and a loss of personal autonomy.[69]

Scholars have highlighted that the rise of digital identity systems exacerbates the risk of identity theft by centralizing vast amounts of sensitive personal and biometric data in highly attractive targets for cybercriminals.[70] These centralized repositories, often described as "honeypots", are vulnerable to breaches that provide malicious actors with the information required to engage in identity fraud.[71] Furthermore, biometric data poses unique challenges; unlike passwords or PINs, biometric identifiers such as fingerprints and facial scans cannot be changed once compromised, making the consequences of theft particularly severe and enduring.[72]

A notable example of identity theft risks is India's Aadhaar system, which is one of the largest biometric identity systems globally.[73] Several data breaches associated with Aadhaar have been reported, including unauthorized access to the personal information of millions of citizens.[74] Research underscores the need for robust safeguards, including stringent encryption standards, decentralized storage solutions, and multifactor authentication protocols, to mitigate the risks of

[67] Solove D. J, 'The Digital Person: Technology and Privacy in the Information Age' NYU Press, GWU Law School Public Law Research Paper 5, 2004, 109 – https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications – on 25 December 2024.
[68] Keaney A and Remenyi D, 'Identity Theft the Next Generation of Fraud–How well are the Irish Protecting Themselves?' 7(1) *Journal of Information Warfare*, 2008, 45.
[69] Cohen J. E, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press, New Haven, 2012.
[70] Khatchatourov A, Laurent M and Levallois-Barth C, 'Privacy in Digital Identity Systems: Models, Assessment and User Adoption' ResearchGate, 2.
[71] Mordini and Tzovaras, *Second Generation Biometrics: The Ethical, Legal and Social Context*, 81.
[72] Rao U and Nair V, 'Aadhaar: Governing with Biometrics', 469.
[73] World Bank Group, *Aadhaar: Digital Inclusion and Public Services in India*, 2016, 1.
[74] Rao U and Nair V, 'Aadhaar: Governing with Biometrics' 42(3) *Journal of South Asian Studies*, 2019, 469.

identity theft.[75] Legal frameworks must also evolve to address the complexities of digital identity theft, ensuring accountability for data controllers and offering victims mechanisms for redress and recovery. By adopting a multidisciplinary approach that combines technical innovations with legal and policy interventions, the risks posed by identity theft in digital identity systems can be significantly reduced.

2.3.2 Profiling

Profiling involves the analysis of individual data to predict or categorize behaviour, preferences, or characteristics.[76] In the context of digital identity systems, profiling is often facilitated by the aggregation of large datasets, which can lead to discriminatory practices and exacerbate existing inequalities. Zarsky notes that while profiling can improve service delivery efficiency, it also poses a significant threat to fairness and non-discrimination, particularly when applied to marginalized groups.[77]

Children are particularly vulnerable to the risks of profiling, as their data can be used to shape their access to opportunities or entrench stereotypes.[78] For instance, automated profiling tools have been criticized for reinforcing biases in areas such as education and law enforcement.[79] This brings up significant moral dilemmas regarding how to strike a balance between the protection of individual rights and the usefulness of data analytics. Furthermore, scholars have highlighted the "opacity" of profiling systems, where individuals often remain unaware of how their data is being used and how decisions about them are made.[80] This lack of transparency compounds the risk of harm, as it denies individuals the ability to contest or understand the outcomes of profiling.

---

[75] Goodell G and Aste T, 'A Decentralized Digital Identity Architecture', 7.
[76] Ferraris V, Francesca C, D'Angelo E and Suloyeva Y, 'Defining Profiling' Social Science Research Network, 2013, 3.
[77] Zarsky T, 'The trouble with algorithmic decisions' 3 *Law, Innovation and Technology* 1, 2011, 103-128.
[78] Prof. Normann W and Prof. Moira P, 'Privacy risks and harms for children and other vulnerable groups in the online environment' Office of the Australian Information Commissioner (OAIC), 18 December 2020, 36 – https://www.oaic.gov.au/__data/assets/pdf_file/0012/11136/Report-Privacy-risks-and-harms-for-children-and-other-vulnerable-groups-online.pdf on 24 December 2024.
[79] Eubanks V, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor,* St. Martin's Press, New York, 2018.
[80] Hildebrandt M, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology,* Edward Elgar Publishing, United Kingdom, 2016.

2.3.3 Mission Creep

Mission creep, also referred to as function creep, manifests when data obtained for one purpose is repurposed for another, sometimes unrelated, objectives.[81] This practice undermines the principle of purpose limitation, a cornerstone of data protection frameworks.[82] Digital identity systems are particularly prone to mission creep due to the wide range of potential applications for the data they collect. For example, biometric data initially collected for identity verification may later be used for surveillance purposes without the consent of the individuals concerned.

Scholars such as Lyon have argued that such practices not only erode public trust but also infringe upon civil liberties, transforming digital identity systems into tools of surveillance rather than empowerment.[83] The lack of clear legal and ethical boundaries exacerbates the problem of mission creep. In some cases, governments have expanded the scope of digital identity programs to include uses that were not initially disclosed to the public, thereby violating principles of transparency and accountability.[84] This underscores the need for robust governance frameworks that explicitly limit the use of personal data to its original purpose.

2.4 Sources of Risk in Digital Identity Systems

The implementation of digital identity systems introduces various risks that can compromise privacy, security, and individual autonomy. These risks arise at multiple stages, including data collection, storage, access, and sharing with third parties or across sectors.[85] Given the sensitive nature of personal data, especially biometric and children's information, any weaknesses in these systems can be exploited.[86] This section examines key sources of risk in digital identity frameworks, focusing on inherent risks in data collection, vulnerabilities in storage and access, and the challenges posed by data sharing and cross-sector integration.

---

[81] Koops B, 'The Concept of Function Creep' 13 Law, *Innovation and Technology* 1, 2021, 37.
[82] Bygrave A, *Data Privacy Law: An International Perspective*, Oxford Unity Press, London, 2014.
[83] Lyon D, *Surveillance Studies: An Overview*, Polity Press, United Kingdom, 2007.
[84] Koops B, 'The Concept of Function Creep', 15.
[85] Bygrave A, *Data Privacy Law: An International Perspective*, Oxford Unity Press, London, 2014.
[86] Schneier B, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W, Norton & Company, New York, 2016.

2.4.1 Inherent Risks in Data Collection Processes

The process of collecting data for digital identity systems is often marked by over-collection, where more information is gathered than is strictly necessary for the stated purpose. This practice contravenes the principle of data minimization, a fundamental tenet of data protection frameworks like the GDPR.[87] Bygrave highlights that over-collection amplifies the potential for misuse, as the accumulation of excessive data increases the stakes of a breach and the scope for unauthorized use.[88]

Children are particularly vulnerable in this context, since they may not fully understand the implications of sharing personal information. Systems designed to collect their data must account for their lack of informed consent.[89] Biometric data, for instance, is often gathered indiscriminately, despite its heightened sensitivity and the irreversible consequences of its compromise. As Tene and Polonetsky argue, such practices reflect a lack of proportionality and necessity, undermining privacy rights and exposing individuals to long-term risks.[90]

2.4.2 Storage and Access Vulnerabilities

The storage of data in centralized systems creates a 'single point of failure', where a breach can expose vast amounts of sensitive information to unauthorized access, misuse, identity theft, financial fraud, or other malicious activities, significantly compromising the privacy and security of affected individuals.[91] Studies have shown that even systems with advanced security protocols are not immune to cyberattacks, insider threats, or human error.[92] For instance, centralized

[87] Article 5(1)(c), *General Data Protection Regulation* (EU) (2016/679).
[88] Bygrave A, *Data Privacy Law: An International Perspective*, Oxford Unity Press, London, 2014.
[89] Livingstone S, Stoilova M and Nandagiri R, 'Children's data and privacy online: Growing up in a digital age: An Evidence Review' London School of Economics and Political Science, 2019, 4.
[90] Tene O and Polonetsky J, 'Big data for all: Privacy and user control in the age of analytics' 11 *Northwestern Journal of Technology and Intellectual Property* 5, 2013, 239-273.
[91] Gourishetty R and Nimmakayala V, 'Blockchain Applications in Cybersecurity: Strengthening Data Integrity and Authentication' 44 *Library Progress International* 3, 2024, 16627.
[92] Ogugua C , Onyinyechi V , Onimisi D, Chigozie A , Onwusinkwue S , and Ibrahim Ahmad, 'Comprehensive Review On Cybersecurity: Modern Threats And Advanced Defense Strategies' 5(2) *Computer Science & IT Research Journal*, 2024, 296.

biometric databases are particularly attractive to malicious actors, given the high value of the stored data and the difficulty of revoking or altering biometric identifiers after a breach.[93]

Access vulnerabilities further compound these risks. Sensitive information may be accessed by unauthorized parties due to badly constructed access controls or insufficient authentication procedures. Scholars such as Schneier emphasize the importance of adopting layered security mechanisms, such as frequent security audits, multi-factor authentication and encryption.[94] However, these technical solutions must be accompanied by strict legal regulations to ensure accountability and compliance with privacy standards.

2.4.3 Risks Arising from Data Sharing with Third Parties or Cross-Sector Integration

Digital identity systems often facilitate cross-border data transfers, particularly in contexts involving multinational service providers, regional integrations, or global transactions.[95] For instance, e-government systems may collaborate with international organizations or rely on foreign cloud service providers for data storage and processing.[96] In such cases, sensitive personal data, including children's biometric information, can cross jurisdictional boundaries, raising significant privacy and security concerns.[97] The lack of harmonized data protection standards across countries exacerbates these risks, potentially leaving children's data vulnerable to misuse in jurisdictions with weaker legal frameworks.

Instances of cross-border data transfers in identity systems are increasingly prevalent in today's interconnected world. For example, interoperability of e-government systems within regional blocs such as the European Union has highlighted both the opportunities and risks associated with

[93] Omotunde H and Ahmed M, 'A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond' 2023 *Mesopotamian Journal of Cybersecurity*, 2023, 115.
[94] Schneier B, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W, Norton & Company, New York, 2016.
[95] Ibor A, Hooper M, Maple C, Crowcroft J and Epiphaniou G 'Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries' AI & Society, 2024, 5.
[96] Otjacques B, Hitzelberger P and Feltz F, 'Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing' 23 *Journal of Management Information Systems* 4, 2007, 30.
[97] Daley M, 'Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure & Data Privacy' 12 *In Sedona Conf. J*, 2011.

such transfers.[98] Similarly, national identity programs that integrate with international financial systems or educational platforms may require data transfers to external jurisdictions.[99]

Data sharing, whether with third parties or across government and private sectors, introduces significant risks related to transparency, consent, and accountability.[100] The integration of data for purposes such as predictive analytics or service optimization often blurs the boundaries of data ownership and control. As Zarsky notes, this practice can lead to function creep, where data initially collected for a specific purpose is repurposed in ways that may infringe on individual rights.[101]

In the context of children's data, the risks are particularly pronounced. For example, sharing educational or health data with private entities for commercial purposes can result in profiling and discrimination, as well as the commodification of children's identities.[102] The lack of robust contractual and legal safeguards often leaves individuals with little recourse against such practices. Moreover, the interoperability of data systems raises questions about the adequacy of consent mechanisms. Most individuals, and particularly children, are unlikely to fully understand the implications of consenting to the sharing of their data across multiple platforms or entities.[103]

2.5 The Role of Privacy by Design and Data Minimisation in Mitigating Risks

Privacy by design is a proactive and preventive approach to ensuring data protection, emphasising that privacy considerations must be embedded into the architecture of systems from their inception. One of the fundamental tenets of privacy by design, according to Tyagi et al., is data minimization, which calls for the collection and retention of only the information that is absolutely required for

[98] Otjacques B, Hitzelberger P and Feltz F, 'Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing', 29.
[99] Grech A, Sood I and Ariño L, 'Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education' Frontiers in Blockchain, 2021, 3.
[100] Marijin J and Jeroen H, 'Big and Open Linked Data (BOLD) in government: A challenge to transparency and privacy?' 32(4) *Government Information Quarterly*, 2015, 365.
[101] Zarsky T, 'The trouble with algorithmic decisions' 3 *Law, Innovation and Technology* 1, 2011, 103-128.
[102] Livingstone S and Third A, 'Children and young people's rights in the digital age: an emerging agenda' New Media and Society, 2017, 8.
[103] Hildebrandt M, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Amsterdam, 2016.

a given purpose.[104] This approach directly challenges practices that result in the collection and retention of excessive personal data, particularly in the context of digital identity systems.

Data minimisation is particularly relevant here. Instead of collecting comprehensive biometric data from children, only the minimal information necessary for identity verification should be collected. Goodell et al argue that decentralised digital identity systems, which allow individuals to control their own data and share it only, when necessary, offer a more privacy-respecting alternative.[105] This model would limit the data collected for services like healthcare or education to only what is essential, reducing both the scope and duration of data storage.

International case law serves to bolster these ideas. According to the European Court of Human Rights (ECtHR) in *S. and Marper v. United Kingdom*, the indiscriminate and widespread retention of personal information, such as fingerprints and DNA profiles of people who are suspected of committing crimes but have not been found guilty, violates Article 8 of the European Convention on Human Rights, which protects the right to privacy.[106] The Court emphasised the importance of safeguards where the automatic processing of personal data is concerned, particularly when that data is used for police or other state purposes.[107]

The Court in *S. and Marper* underscored that domestic laws must ensure that data collection is not excessive, and that the data is retained only for as long as necessary to fulfil its original purpose.[108] In addition, sufficient assurances must be in place to guard against abuse and misuse of the data that is kept. This criterion is particularly important for sensitive data categories like DNA, which contains extremely private genetic information that affects the individual as well as their family members.[109]

[104] Tyagi A, Rekha G and Sreenath N, 'Is your Privacy Safe with Aadhaar? An Open Discussion' Distributed and Grid (PDGC), 2018, 318-323.
[105] Goodell G and Aste T, 'A Decentralized Digital Identity Architecture' 2(17) *Frontiers Blockchain*, 2019, 7.
[106] *S and Marper v United Kingdom*, ECtHR Judgement 4 December 2008.
[107] *S and Marper*, ECtHR, 1581.
[108] *S and Marper*, ECtHR, 1581.
[109] Dixon P, 'A Failure to "Do No Harm" — India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S' 7 *Health and Technology*, 2017, 546.

Privacy by design, coupled with data minimisation, would require the state to explore less invasive alternatives to biometric data collection.[110] For example, pseudonymisation or encryption techniques could be employed to ensure that even if personal data is collected, it cannot be easily linked to the individual child.[111] Methods such as zero-knowledge proofs, allow identity verification without the need to store sensitive, directly identifiable information.[112] This would substantially reduce the risk of data breaches and privacy violations, offering a more secure framework for managing children's digital identities.

Moreover, the introduction of privacy by design mechanisms would necessitate a re-evaluation of the justification for collecting children's biometric data in the first place. The state must demonstrate that such data collection is truly essential, exploring alternatives like tokenized identities or decentralised data-sharing platforms, which allow individuals to share minimal information without revealing unnecessary personal details. The principle of data minimisation is also crucial in mitigating long-term privacy risks. For instance, the storage of biometric data raises concerns about data retention periods. Following the guidance of the ECtHR in *S. and Marper*, any data retained must be relevant, not excessive, and stored for no longer than necessary.[113]

2.6 Consent vs. Legal Necessity: Addressing the Unique Challenges in Children's Data

The child's ability to offer consent depends on their maturity level; can they think clearly enough to comprehend their situation and, thus, give consent?[114] The UK House of Lords defined the ability to consent in the landmark Gillick case as "a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision."[115] One key tenet of the data

[110] World Bank Group, *Privacy by Design: Current Practices in Estonia, India, and Austria*, 2018, 4.
[111] World Bank Group, *Privacy by Design: Current Practices in Estonia, India, and Austria*, 2018, 3.
[112] Yin W, 'Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age' 37 *Applied Artificial Intelligence* 1, 2023, 5.
[113] *S and Marper*, ECtHR, 1581.
[114] Simone Van Der Hof, 'I Agree. . . Or Do I? — A Rights-Based Analysis of The Law On Children's Consent In The Digital World' 4(4) *Wisconsin International Law Journal*, 2017, 421.
[115] *Gillick v West Norfolk and Wisbech Area Health Authority and another* (1985), The United Kingdom House of Lords.

protection principle is consent, which guarantees that people have control over the collection, use, and sharing of their personal data.[116]

As Bondre highlights, the concept of legal necessity can sometimes override the requirement for consent, especially when the collection of data is considered essential for public services or is in the public interest.[117] However, this reliance on legal necessity raises significant concerns. Murray and Fusey critique the overuse of legal necessity, arguing that it should only be invoked when data collection is truly indispensable, and only after less invasive alternatives have been thoroughly explored.[118]

Prof. Laura M. Bingham, in her affidavit in the ongoing constitution petition against the Maisha Card at the High Court, further highlights the tension between consent-based and necessity-based data collection.[119] Governments frequently bypass consent requirements by invoking legal necessity, often arguing that certain data is indispensable for delivering basic needs like health or education. While access to such services is crucial, necessity-based data collection should not be a default solution, particularly when it concerns vulnerable populations like children.

The dissent in the Aadhaar judgment makes a compelling argument against the broad invocation of legal necessity. It critiques the "bread vs. freedom" justification, where individual rights, such as the right to privacy, are derogated in the name of improving access to basic needs.[120] The dissent argues that the state's failure to demonstrate why the Aadhaar system's benefits in welfare schemes required such profound infringements on privacy reveals a dangerous precedent.[121] It emphasises that economic rights and privacy rights are not mutually exclusive. The state has a duty to protect both, without allowing one to be compromised for the other. This argument is particularly relevant

[116] Simone Van Der Hof, 'I Agree. . . Or Do I? — A Rights-Based Analysis of The Law On Children's Consent In The Digital World', 421.
[117] Bondre A, Pathare S and Naslund J, 'Protecting Mental Health Data Privacy in India: The Case of Data Linkage with Aadhaar', 469.
[118] Murray D and Fussey P, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' 52 *Israel Law Review* 1, 2019, 55.
[119] *Haki na Sheria Initiative v The Honourable Attorney General and 4 others* (2023) eKLR.
[120] Upendra B, 'From Human Rights to the Right to Be Human: Some Heresies' 13 *International Centre Quarterly* 3/4, 1986, 186.
[121] *Justice K.S. Puttaswamy and Another v Union of India (UOI) and Others* (2018), The Supreme Court of India.

to the Maisha Namba system, where concerns about privacy infringement are often overshadowed by the state's promise of improved service delivery.

One potential safeguard is enhancing parental consent mechanisms or establishing independent oversight to ensure decisions regarding children's data are made with the child's best interests in mind. However, as Stoilova, Livingstone, and Nandagiri argue, relying solely on parental consent may be insufficient due to the complexity of digital environments and the technical nature of data processing.[122] While parents are considered competent to provide or withhold consent for their own personal and sensitive data, they may not always have access to the necessary information or expertise to fully comprehend the long-term privacy implications of decisions affecting their children's data.[123]

To address this, the law can incorporate measures to supplement parental consent, such as mandating transparency from data processors, requiring child-specific data impact assessments, and embedding privacy-by-design principles into digital identity systems. By shifting some of the responsibility to organizations handling children's data and ensuring robust accountability mechanisms, the legal framework can help mitigate the limitations of relying solely on parental consent without undermining parents' capacity to act in their children's best interests.

2.7 Concerns Around Surveillance, Misuse, and Lack of Accountability

One of the most significant concerns associated with government-led digital identity systems is the potential for surveillance. Zuboff warns of the creeping normalcy of surveillance practices, where governments collect, monitor, and analyse citizens' data under the guise of national security or administrative convenience.[124] This surveillance can create a chilling effect, stifling individual freedoms and eroding public trust in state institutions.

The risk of data misuse by governments is another pressing issue. Historical examples, such as the misuse of identity systems during apartheid in South Africa or the Holocaust, demonstrate how

[122] Livingstone S, Stoilova M and Nandagiri R, 'Children's data and privacy online: Growing up in a digital age: An Evidence Review' London School of Economics and Political Science, 2019, 4.
[123] Livingstone S, Stoilova M and Nandagiri R, 'Children's data and privacy online: Growing up in a digital age: An Evidence Review' London School of Economics and Political Science, 2019, 4.
[124] Zuboff S, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York, 2019.

data can be weaponized to target vulnerable populations.[125] While modern legal frameworks aim to prevent such misuse, gaps in oversight and accountability persist. For instance, data collected for one purpose, such as social service delivery, may be repurposed for law enforcement or political profiling, violating the principles of purpose limitation and consent.

Lack of accountability compounds these risks, as governments often operate with significant discretion in managing sensitive data. Pasquale describes the opacity of decision-making processes in government systems as a black box, making it difficult for individuals to challenge errors or abuses.[126] Without robust oversight mechanisms, individuals, especially children, are left vulnerable to exploitation and harm.

2.8 Conclusion

This chapter conducted an inquiry of the potential implications of failing to uphold children's right to privacy in digital identity systems. It examined the risks posed by digital identity systems, such as unauthorized access, identity theft, profiling, and mission creep, highlighting how centralized storage and data-sharing practices exacerbate these vulnerabilities. It also explored the unique challenges of protecting children's privacy particularly the tension between consent and legal necessity. To mitigate these risks, the chapter emphasized the need for privacy-by-design principles, data minimization, and robust legal safeguards that extend beyond reliance on consent. By analysing these aspects, the chapter sets the stage for evaluating Kenya's legal framework and proposing reforms to better protect children's privacy in digital identity systems.

[125] Seltzer W and Anderson M, 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses' 68 *Social Research* 2, 481–513.
[126] Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

Chapter 3:

The Role of Kenya's Legal Framework in Protecting Children's Rights within Digital Identity Systems

3.1 Introduction

The objective of this chapter is to examine the adequacy of Kenya's legal framework in protecting children's right to privacy within digital identity systems, particularly focusing on the Maisha Card system. In answering this objective, the chapter first provides an overview of Kenya's current legal framework governing digital identity systems, focusing on the Constitution of Kenya, the Data Protection Act, the Children's Act, and related policies. It then critically analyses these laws to determine their adequacy in safeguarding children's privacy, emphasizing key principles such as data minimization and accountability. The chapter further examines case law and judicial interpretations to assess how Kenya's courts have addressed issues surrounding children's data privacy, identifying significant legislative and enforcement gaps.

3.2 Overview of the Legal Framework Governing Digital Identity and Privacy in Kenya

This section examines the key laws and regulations that form the legal framework governing digital identity and privacy in Kenya. The focus is on assessing their provisions in safeguarding children's right to privacy within the Maisha Card system and other digital identity initiatives. The discussion begins with the Constitution of Kenya, 2010, which provides the foundational principles for the right to privacy and the protection of personal data. It then explores the Data Protection Act and Regulations, 2019, Kenya's primary legislation on data protection, analysing its relevance to children's privacy.

The Children Act, 2022, which provides specific protections for children's rights, including their right to privacy, is also discussed. Additional regulatory instruments, such as the Registration of Persons (Amendment) Regulations and Births and Deaths (Amendment) Regulations, are examined for their role in managing children's personal data in identity systems. Finally, the section reviews the Computer Misuse and Cybercrimes Act, 2018, focusing on its provisions for addressing misuse, fraud, and unauthorized access related to digital identity systems. By analysing

these legal instruments, this section seeks to determine the adequacy of Kenya's legal framework in protecting children's privacy and identify areas requiring reform to strengthen safeguards against risks inherent in digital identity systems.

3.2.1 Constitution of Kenya, 2010

Kenya's 2010 Constitution establishes a robust framework for the protection of fundamental rights, including the right to be registered at birth and provided with identification documents. Article 12 affirms the right of every citizen to acquire and possess registration and identification documents, emphasizing that these are entitlements, not privileges.[127] This ensures equal access to services and recognition under the law. Additionally, the Constitution upholds values such as dignity, privacy,[128] access to information,[129] and the best interests of the child.[130] These provisions collectively underscore the state's obligations to safeguard both identity and privacy rights.

The right to privacy, enshrined in Article 31, is particularly significant in the context of digital identity systems.[131] It guarantees protection against the unauthorized collection, use, or disclosure of personal data and protects individuals from unwarranted searches and seizures.[132] However, this right intersects with the state's obligation to maintain accurate and secure records, which is critical for ensuring access to services and effective governance.

This raises the question of how the state reconciles the right to privacy with the operational requirements of maintaining registration systems. While the state has a legitimate interest in collecting and storing personal data for governance and service delivery, it must do so in a manner that minimizes risks to individual privacy. For instance, safeguarding sensitive data from unauthorized access, ensuring its use is proportional to its purpose, and adopting privacy-by-design principles are essential mechanisms to balance these rights.

[127] Article 12, *Constitution of Kenya* (2010).
[128] Article 31, *Constitution of Kenya* (2010).
[129] Article 35, *Constitution of Kenya* (2010).
[130] Article 53(2), *Constitution of Kenya* (2010).
[131] Article 31, *Constitution of Kenya* (2010).
[132] Article 31, *Constitution of Kenya* (2010).

Furthermore, Article 24 of the Constitution also establishes the legal basis for limiting rights, including privacy.[133] It specifies that such limitations must be rational and defensible in a democratic and open society rooted in human dignity, equality, and freedom.[134] In the case of digital identity systems, the state can limit privacy rights by collecting and processing personal data, but only to the extent necessary to achieve legitimate objectives such as national security, public administration, or service delivery.[135] However, these limitations must be accompanied by safeguards that prevent abuse, including strict data minimization practices, transparency, accountability, and robust legal protections for vulnerable groups like children.

While the Constitution provides a strong foundation for the protection of privacy and identity rights, significant challenges remain in striking a balance between the state's obligations to maintain identification systems and the right to privacy. Addressing these challenges requires not only adherence to constitutional principles but also the implementation of child-specific protections to mitigate risks associated with digital identity systems.

3.2.2 Data Protection Act

The Data Protection Act (DPA) operationalizes the constitutional right to privacy under Article 31 of the Constitution.[136] It establishes a thorough legislative basis for Kenya's safeguarding of personal data, including principles of transparency, accountability, fairness, lawfulness, and data minimization.[137] Additionally, it creates the Office of the Data Protection Commissioner (ODPC) to oversee enforcement and compliance with the Act.[138] A data subject is defined under Section 2 of the Act as an individual whose personal data is being processed, a definition broad enough to include children.[139] Importantly, as stated in Article 53(2) of the Constitution, the DPA stresses that the principle of furthering the child's best interests must serve as the basis for processing children's personal data.[140]

---

[133] Article 24, *Constitution of Kenya* (2010).
[134] Article 12, *Constitution of Kenya* (2010).
[135] Amnesty International, *Digital ID in Kenya (An Advisory Policy Paper providing a roadmap to the implementation of a Rights Respecting Digital ID Regime in Kenya)*, 2023, 21.
[136] Article 31, *Constitution of Kenya* (2010).
[137] Section 25, *Data Protection Act* (Act No. 24 of 2019).
[138] Section 5, *Data Protection Act* (Act No. 24 of 2019).
[139] Section 2, *Data Protection Act* (Act No. 24 of 2019).
[140] Section 33(1)(b), *Data Protection Act* (Act No. 24 of 2019).

The DPA mandates DPIAs for high-risk processing activities, including those involving sensitive personal data.[141] A DPIA is a methodical procedure used to assess and reduce the risks related to processing personal data, especially for undertakings that could pose serious threats to people's rights and liberties. DPIAs are intended to encourage responsibility in data processing procedures and guarantee adherence to data protection regulations. However, the Act does not explicitly require child-specific DPIAs, which are crucial for assessing privacy risks unique to children. In international best practices, CRIAs are used to evaluate how policies and systems affect children's privacy and rights.[142] The lack of such assessments under the DPA leaves children vulnerable to risks such as profiling, unauthorized data use, and long-term surveillance.

The principle of data minimisation under Section 25 of the DPA mandates that only data strictly necessary for the stated purpose should be collected.[143] However, the Act does not specify heightened standards for children or provide safeguards for invasive data types such as biometric data. Biometric data, which includes facial recognition, fingerprints, and other sensitive identifiers, is immutable and can expose children to heightened risks of identity theft and surveillance. While some may argue that the general principle of data minimisation suffices, international frameworks suggest the need for child-specific provisions given the unique vulnerabilities of children.[144]

Section 48 of the DPA regulates cross-border data transfers, requiring that personal data may only be transferred to countries with laws that adequately secure data or with the explicit consent of the data subject.[145] However, the Act lacks a clear mechanism for determining adequacy and does not require enforceable safeguards, such as binding corporate rules or contractual clauses, to protect data in jurisdictions with weaker privacy protections. This gap becomes significant in the context of digital identity systems like the Maisha Card, where data backups or cloud storage may involve

[141] Section 31, *Data Protection Act* (Act No. 24 of 2019).
[142] UNICEF, *Developing Global Guidance for Child Rights Impact Assessments in Relation to the Digital Environment*, April 2024, 4.
[143] Section 25, *Data Protection Act* (Act No. 24 of 2019).
[144] UNICEF, *Developing Global Guidance for Child Rights Impact Assessments in Relation to the Digital Environment*, April 2024, 10.
[145] Section 48, *Data Protection Act* (Act No. 24 of 2019).

international transfers. The potential for misuse or breaches increases in such scenarios, especially if data is stored in countries with lower privacy standards.[146]

The enforcement framework under the DPA relies on the ODPC to investigate complaints, issue penalties, and ensure compliance. However, the framework does not explicitly address children's unique vulnerabilities, nor does it include proactive measures to monitor systems like the Maisha Card, which involve large-scale processing of minors' data.[147] For example, the Act does not require annual audits or independent reviews of child-specific systems. This oversight gap weakens protections against risks such as data breaches, profiling and mission creep.[148]

The ODPC's dependence on the mandatory participation of the Cabinet Secretary for ICT and national security organs further precludes it from having guaranteed independence.[149] Potential conflicts of interest are introduced by this dependency, which also compromises the ODPC's independence. Such reliance raises concerns about the ability of the ODPC to act impartially, particularly when enforcing data protection laws against state agencies or politically sensitive entities. Without robust independence, the ODPC's effectiveness and credibility in ensuring accountability in data handling practices are compromised.[150] This limitation is especially significant in the context of children's data, where impartial enforcement is critical to safeguarding their privacy rights against potential misuse.

[146] Aishat O and Ridwan O, 'Digital Identity, Surveillance, and Data Protection in Africa' ResearchGate, 2024, 128.
[147] Amnesty International, *Digital ID in Kenya (An Advisory Policy Paper providing a roadmap to the implementation of a Rights Respecting Digital ID Regime in Kenya)*, 2023, 27.
[148] Carly Nyst, 'Privacy, Protection Of Personal Information And Reputation', 13.
[149] Kageni M and Odhiambo Y, 'Strengthening Data Protection in Kenya: Opportunities and the Way Forward' KIPRA, 30 June 2024 – <https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/#:~:text=The%20office%20of%20the%20Data,of%20the%20Data%20Protection%20Commissioner.> on 13 January 2025.
[150] Amnesty International Kenya, *Amnesty International Kenya Data Protection Report*, November 2021, 27.

3.2.3 Children Act

In order to bring Kenya's legislative framework on children's rights into compliance with the 2010 Kenyan Constitution and international agreements like the African Charter on the Rights and Welfare of the Child (ACRWC) and the United Nations Convention on the Rights of the Child (UNCRC), the Children Act was enacted.[151] The Act guarantees children fundamental rights as stipulated in Article 53 of the Constitution, including the right to parental care, protection, education, and immediate birth registration under the Births and Deaths Registration Act.[152] It also enshrines the principle of the best interests of the child as paramount in all matters pertaining to children.[153]

Crucially, Section 27 of the Children Act affirms the right to privacy, asserting that each and every child is protected against unlawful or arbitrary interference with their private, family, or correspondence.[154] The Act requires the processing of children's personal data in compliance with the Data Protection Act.[155] This reflects the legislature's acknowledgment of the growing role of digital systems, such as the Maisha Card, in collecting and managing children's personal data from birth.

However, the Act falls short of providing specific guidelines or a comprehensive framework for institutional oversight and coordination in managing children's personal data.[156] This gap is particularly concerning given the reliance on multiple state institutions, such as the ODPC and children's services departments, to ensure the privacy and protection of sensitive data.[157] In the context of digital identity systems, these oversight and coordination challenges expose children to

[151] World Organisation Against Torture, *Rights of the Child in Kenya; An alternative report to the UN Committee on the Rights of the Child on the implementation of the Convention on the Rights of the Child in Kenya*, January 2007, 11.
[152] Article 53, *Constitution of Kenya* (2010).
[153] Section 8, *Children Act* (Cap. 141).
[154] Section 27(1), *Children Act* (Cap. 141).
[155] Section 27(3), *Children Act* (Cap. 141).
[156] Chege N and Ucembe S, 'Kenya's Over-Reliance on Institutionalization as a Child Care and Child Protection Model: A Root-Cause Approach' Social Sciences, 2020, 8.
[157] Eke D, Ochang P, Adimula A, Borokini F, Akintoye S, Oloyede R, Sorborikor L, Adeyeye M, Wale-Oshinowo B, Ogundele T, 'Responsible Data Governance in Africa: Institutional Gaps and Capacity Needs' Centre for the Study of African Economies, 2022, 20.

potential risks, including data breaches, unauthorized access, and inadequate enforcement of data protection standards.

The absence of detailed coordination mechanisms between child protection bodies and the ODPC introduces several risks.[158] First, it creates ambiguity regarding which institution bears primary responsibility for ensuring that children's data is processed in line with privacy principles.[159] This lack of clarity can lead to accountability gaps, where breaches of children's data privacy may not be adequately investigated or remedied. For example, if data collected by the Director of Children's Services is mishandled or improperly accessed, it is unclear whether the ODPC or the NCCS should take the lead in enforcing compliance or addressing the breach.

Second, the gap in oversight coordination undermines the effectiveness of both the Children Act and the DPA. Ogonjo and Achieng emphasize the complexities surrounding the rights of children in the digital era to privacy and data protection. They highlight the necessity for clear policies and coordination among institutions to effectively safeguard children's data.[160] Without such coordination, the enforcement of data privacy frameworks becomes fragmented, diminishing their overall effectiveness.

Further, the lack of explicit institutional coordination provisions hampers the development of a unified strategy for protecting children's data. For instance, international best practices, such as the creation of joint task forces between child welfare institutions and data protection regulators, have been recommended by UNICEF to enhance oversight in digital identity systems.[161] Without similar mechanisms, Kenya risks leaving children's data exposed to misuse, particularly in high-risk contexts such as centralized databases.[162]

---

[158] Laibuta M, 'The Evolution of Privacy and Data Protection in Kenya' 30 *A Journal of Legal History* 1, 2024.

[159] Otele O, 'Kenya's Data Protection Regime: Challenges And Future Prospects' 1 Journal Of African Politics, 2021, 81.

[160] Ogonjo F and Achieng R, 'Children's Rights to Data Protection and Privacy in the Digital Age: Existing Laws and Policies' Centre for Intellectual Property and Information Technology Law, 4 October 2022 – <https://cipit.strathmore.edu/childrens-rights-to-data-protection-and-privacy-in-the-digital-age-existing-laws-and-policies >on 21 January 2025.

[161] *General comment No. 25 (2021) on children's rights in relation to the digital environment*, CRC/C/GC/25, 2 March 2021, 5.

[162] World Bank, *Principles On Identification For Sustainable Development: Toward The Digital Age*, February 2021, 16.

The phenomenon of "policy silos," where individual agencies operate without considering the broader implications of their actions on children's welfare, has been discussed in various scholarly works. For instance, the Social Policy Report by the Society for Research in Child Development highlights that fragmented policy approaches can lead to inefficiencies and gaps in addressing child poverty and welfare.[163] Additionally, the report Leave No Youth Behind by the Centre for Law and Social Policy emphasizes that disconnected services and lack of coordination among agencies can hinder effective support for at-risk youth.[164] In the Kenyan context, the establishment of the ODPC offers an opportunity to strengthen oversight of children's data through collaboration with the NCCS and DCS. However, the lack of legislative provisions requiring such collaboration limits the potential for these institutions to work effectively together.

3.2.4 Registration of Persons (Amendment) Regulations and Birth and Deaths (Amendment) Regulations

The Registration of Persons (Amendment) Regulations (RPA Rules), and the Births and Deaths Registration (Amendment) Rules, aim to digitize Kenya's civil registration and identity systems. However, several provisions in these regulations raise significant concerns about privacy, transparency, and accountability, particularly regarding children's data protection in systems like the Maisha Card.

Regulation 8(2) of the Births and Deaths Registration (Amendment) Rules mandates that every child be assigned a Unique Personal Identifier (UPI) at birth to ensure continuity and accuracy in record-keeping.[165] While this enhances the management of personal records, the regulation fails to provide safeguards for the generation, storage, and access to UPIs. It does not specify whether secure technologies, such as encryption, will be employed or if third-party entities will be involved in the UPI generation process.[166] These omissions create risks of unauthorized access, data

[163] Aber L, Morris P and Raver C, 'Children, Families and Poverty Definitions, Trends, Emerging Science and Implications for Policy' 26 *Society for Research in Child Development* 3, 2012, 14.
[164] Epstein J and Greenberg M, 'Leave No Youth Behind: Opportunities for Congress to Reach Disconnected Youth' Center for Enter for Enter for Law and Social Policy, 2003, 12.
[165] Regulation 8(2), *The Births and Deaths Registration (Amendment) Rules* (2024).
[166] Kenya ICT Action Network (KICTANet) and Amnesty International Kenya, *Joint Memorandum on the Births and Deaths Registration (Amendment) Rules 2024 and the Registration of Persons (Amendment) Rules 2024*, 26 September 2024, 2.

breaches, and misuse of sensitive personal data. Given the importance of UPIs in identity systems, the regulation should establish data protection guidelines, require regular audits, and ensure compliance with the Data Protection Act.

Regulation 10(2) further requires that a UPI be assigned and linked to an individual's record at birth.[167] However, it does not address how registrars will manage data securely, especially in regions with low digital literacy.[168] Without mandatory training for registrars on data security practices, this provision risks exposing children's data to human error and inadequate protection. Strengthening this regulation to include registrar training and the adoption of standardized data protection practices is critical to safeguard children's privacy.

Regulation 5(1) of the RPA Rules mandates the collection of biometric data for registration purposes, including facial recognition, fingerprints, and thumbprints.[169] While this expands the scope of identity verification, it raises concerns about data minimization and the risks associated with collecting multiple biometric identifiers. The regulation does not address how biometric data will be stored or managed securely, nor does it consider potential issues such as AI bias in facial recognition technologies. Additionally, the absence of a centralized biometric repository for verification purposes increases the risk of inconsistencies and breaches.[170] To comply with the DPA, the regulation should mandate stringent safeguards for biometric data storage, including encryption, secure access controls, and detailed policies for managing and auditing biometric records.

Regulation 7 of the RPA Rules allows for either the adoption of UPIs or new index numbers for identity cards.[171] While this flexibility aims to ease implementation, it risks creating inconsistencies in record-keeping and undermines the coherence of a unified identification system.

---

[167] Regulation 10(2), *The Births and Deaths Registration (Amendment) Rules* (2024).
[168] Kenya ICT Action Network (KICTANet) and Amnesty International Kenya, *Joint Memorandum on the Births and Deaths Registration (Amendment) Rules 2024 and the Registration of Persons (Amendment) Rules 2024*, 26 September 2024, 4.
[169] Regulation 5(1), *Registration of Persons (Amendment) Rules* (2024).
[170] Kenya ICT Action Network (KICTANet) and Amnesty International Kenya, *Joint Memorandum on the Births and Deaths Registration (Amendment) Rules 2024 and the Registration of Persons (Amendment) Rules 2024*, 26 September 2024, 11.
[171] Regulation 7, *Registration of Persons (Amendment) Rules* (2024).

Such inconsistencies could have long-term implications for children's records, including difficulties in accessing services tied to identity documentation. A unified approach is necessary to ensure continuity and reduce confusion in identity management.

Regulation 8(2) further allows for issuing both physical and digital certificates for identity registration.[172] However, it does not address the security and authenticity of digital certificates, which are susceptible to forgery and unauthorized access.[173] Without safeguards, such as digital signatures or verification mechanisms, the authenticity of these certificates cannot be guaranteed, potentially compromising the reliability of children's identity records.

A further concern lies in the proposal to consolidate data from the Maisha Namba, Maisha Card, and Maisha Digital ID into a centralised Maisha Integrated Database, for which no legal framework exists.[174] This creates serious vulnerabilities, as highlighted by the *Nubian Rights Forum v. Attorney General (2020)* case, which flagged the risks of misuse and insufficient safeguards in data gathered via the National Integrated Identity Management System (NIIMS).[175]

Muriithi J. and Lenaola J. in *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v. Cabinet Secretary Ministry of Health & 4 Others (2016)* eKLR observed that even when the State's goals are legitimate, the methods of data collection could infringe on the right to privacy.[176] The government's plan to reuse this contested data for the Maisha Card compounds the potential for breaches of children's privacy, as compliance issues from NIIMS remain unresolved.[177]

[172] Regulation 8(2), *Registration of Persons (Amendment) Rules* (2024).
[173] Kenya ICT Action Network (KICTANet) and Amnesty International Kenya, *Joint Memorandum on the Births and Deaths Registration (Amendment) Rules 2024 and the Registration of Persons (Amendment) Rules 2024*, 26 September 2024, 12.
[174] Al Kags, 'Maisha Namba: Thoughts about Kenya's evolution of identity' Open Institute, 2 September 2024 — <https://alkags.me/maisha-namba/ > on 21 November 2024.
[175] (2020) eKLR.
[176] *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others* (2016) eKLR.
[177] Kenya Human Rights Commission, *Government shouldn't force flawed digital ID system in Kenya*, 27 February 2024.

These regulatory gaps significantly impact children's right to privacy, as enshrined in Article 31 of the Constitution and the Children Act.[178] By failing to provide adequate safeguards for the generation, storage, and management of UPIs and biometric data, the regulations expose children to risks such as identity theft, unauthorized profiling, and breaches of personal data. Furthermore, the lack of training for registrars and the absence of clear frameworks for centralized databases exacerbate these vulnerabilities, leaving children's data unprotected in an increasingly digital environment.

3.2.5 The Computer Misuse and Cybercrimes Act

The Computer Misuse and Cybercrimes Act, 2018 establishes penalties for offenses such as unauthorized access, data interception, and the misuse of information systems.[179] These provisions are crucial for addressing breaches in digital systems, including those storing children's biometric data in centralized systems like the Maisha Card.[180] However, the Act does not explicitly cover the unique risks posed by biometric data, such as profiling or misuse of immutable identifiers, which require more specific safeguards.

The lack of explicit provisions raises concerns about whether misconduct and misuse specific to biometric data stored in centralized systems fall comprehensively under the offenses prescribed in the Act. While unauthorized access or hacking of such data could lead to prosecution, the Act does not address nuanced issues such as inappropriate internal use, third-party misuse, or vulnerabilities stemming from algorithmic processing in facial recognition systems.[181]

Furthermore, the Act's broad focus on cybercrimes means it primarily addresses reactive measures, penalizing breaches after they occur, rather than preventive mechanisms specific to biometric data.[182] In contrast, frameworks like the Data Protection Act are better suited to establish preventive measures, such as encryption, purpose limitation, and privacy-by-design principles.[183]

---

[178] Article 31, *Constitution of Kenya* (2010).
[179] Part III, *Computer Misuse and Cybercrimes* (Act No 5 of 2018).
[180] Bowmans, *The Computer Misuse and Cybercrimes Act,* 6 March 2020, 1.
[181] Abdirahman I, 'Exploring Co-Regulation as a Solution to Automated Disinformation in Kenya' 3 *Journal of Intellectual Property and Information Technology Law (JIPIT)* 1, 2023, 227.
[182] Walumoli B, 'A Critical Analysis of the Challenges Facing Counter-Cybercrime in 21st Century Africa: A Focused Comparison of Kenya and Rwanda' Unpublished LLM Thesis, University of Nairobi, Nairobi, 2021, 8.
[183] Section 41, *Data Protection Act* (Act No. 24 of 2019).

This leaves a gap in addressing misconduct or misuse that may not constitute a direct cybercrime but nonetheless violates the integrity and privacy of biometric data in centralized systems.

In systems like the Maisha Card, where children's data is collected and stored from birth, this gap underscores the need for comprehensive oversight that combines the reactive measures of the Cybercrimes Act with the preventive safeguards outlined in the Data Protection Act.[184] The absence of explicit protections for biometric data in the Cybercrimes Act limits its capacity to address all potential forms of misuse in digital identity systems comprehensively.

3.3 Judicial Interpretations on Children's Right to Privacy

a) Nubian Rights Forum Case (2020)

In *Nubian Rights Forum & 2 others v Attorney-General & 6 others*, the High Court examined the constitutionality of the NIIMS program, particularly its implications for privacy under Article 31 of the Kenyan Constitution.[185] The petitioners raised concerns about the intrusive nature of the data collection process, including the mandatory submission of sensitive biometric information such as facial features and fingerprints.[186] It was argued that the statutory framework lacked clarity on safeguards to prevent misuse of personal information and that there were no provisions to regulate data access or ensure accountability in its use.[187] These omissions posed a threat to the right to privacy, particularly for children, whose personal information would be included in the centralized database.

The petitioners further highlighted that the amendments to the Registration of Persons Act lacked clarity on access controls and safeguards for collected data, exposing individuals, including children, to potential risks.[188] The court underscored the necessity of having data protection legislation in place to address privacy concerns before the rollout of such a system, aligning with

[184] Privacy International, *The Right to Privacy in Kenya: Stakeholder Report Universal Periodic Review 35th Session - Kenya*, July 2019, 14.
[185] (2020) eKLR.
[186] (2020) eKLR.
[187] (2020) eKLR.
[188] (2020) eKLR.

the broader constitutional requirement to ensure the protection of fundamental rights, including children's best interests as enshrined in Article 53.[189]

b) R v Joe Mucheru Ex Parte Immaculate Kassait (2021)

In *Republic v Joe Mucheru & 2 others; Katiba Institute & another (Ex Parte)*, the High Court addressed the rollout of the Huduma Card and emphasized the necessity of compliance with the Data Protection Act, 2019, particularly Section 31, which mandates a DPIA for operations likely to pose high risks to the rights of data subjects.[190] The court found that implementing such systems without a DPIA violated statutory obligations and constitutional privacy protections under Article 31 of the Constitution.[191] While children were not specifically mentioned, the judgment has significant implications for minors, given their vulnerability and the sensitivity of their data in digital identity systems.

The court's decision underscored the risks posed by the lack of a regulatory framework prior to data collection and processing, highlighting the state's duty to ensure privacy safeguards are in place before implementing large-scale digital systems.[192] This judgment illustrates the broader necessity of addressing risks to personal data, including children's information, by ensuring compliance with legal and constitutional standards, thereby protecting the right to privacy for all citizens.

3.4 Conclusion

This chapter sought to examine whether Kenya's current legal framework is adequate and comprehensive in protecting children's right to privacy within digital identity systems. The findings reveal that while foundational protections are established through the Constitution, Data Protection Act, Children Act, Computer Misuse and Cybercrime Act, and judicial decisions, the framework falls short of addressing the unique vulnerabilities of children. Key gaps include the lack of child-specific provisions, such as tailored data minimisation requirements and safeguards for biometric data. Additionally, the absence of comprehensive oversight and coordination among

[189] (2020) eKLR.
[190] Section 31, *Data Protection Act* (Act No. 24 of 2019).
[191] (2021) eKLR.
[192] (2021) eKLR.

implementing agencies further undermines the protection of children's data in initiatives like the Maisha Card. To fully safeguard children's privacy rights, Kenya must prioritize the inclusion of explicit, child-centric legal protections that reflect the evolving challenges posed by digital identity systems.

Chapter 4:

Comparative Analysis of Digital Identity Systems: Lessons from the European General Data Protection Regulation (GDPR)

4.1 Introduction

The objective of this chapter is to analyse the best practices and identify lessons from the European Union's GDPR regarding the protection of children's privacy and their applicability to Kenya's digital identity framework. It begins by providing an overview of the GDPR, explaining why it was chosen as the comparator, its nature as a regional law, and the distinction between its substantive provisions and recitals. The chapter then undertakes a comparative analysis of Kenya's legal framework against the GDPR, focusing on four key areas: principles governing data protection, safeguards for children's data, institutional oversight, and cross-border data transfers. Each section evaluates the GDPR's provisions, highlights gaps in Kenya's approach, and identifies actionable lessons for improving children's privacy protections within the Maisha Card digital identity system. The chapter concludes by summarizing these best practices and demonstrating how the research objective has been met.

4.2. Overview of GDPR

The GDPR is a regional law applicable across all EU member states, designed to harmonize data protection standards and provide comprehensive protection for personal data.[193] Its extraterritorial breadth guarantees that it can be applied to non-EU entities that handle the personal data of EU citizens, establishing it as a globally recognised data protection standard.[194] The GDPR adopts a rights-based approach, emphasizing transparency, accountability, and privacy by design, with a special focus on protecting at-risk groups such as children.[195] This framework provides valuable insights for jurisdictions like Kenya, where legal safeguards for children's privacy, particularly in digital identity systems like the Maisha Card, remain underdeveloped.

[193] Albrecht J, 'How the GDPR Will Change the World' European Data Protection Law Review, 2016, 1.
[194] Article 3, *General Data Protection Regulation* (EU) (2016/679).
[195] *General Data Protection Regulation* (EU) (2016/679).

Structurally, the GDPR is composed of binding Articles and interpretative Recitals. The Articles outline substantive obligations and rights, forming the regulation's enforceable core, while the Recitals provide contextual guidance to aid in the interpretation and application of these provisions.[196] However, the non-binding nature of Recitals presents a challenge when benchmarking Kenya's legal framework against the GDPR. For research ethics purposes, it is critical to acknowledge that several superior attributes of the GDPR, particularly its progressive stance on children's privacy, are derived from Recitals rather than binding Articles.[197] This limits their direct applicability but still serves as valuable guidance for reforming Kenya's legal and regulatory framework.

The GDPR's principles and provisions offer a practical roadmap for Kenya to strengthen its legal protections for children's privacy. Key areas of relevance include data minimisation, purpose limitation, and the need for independent oversight mechanisms. By integrating these insights, Kenya can address existing gaps and enhance the Maisha Card system to better protect children's privacy.

4.3 Comparative Analysis: Kenya's Legal Framework vs. the GDPR

Kenya's DPA and the GDPR share key similarities but also reveal critical gaps, especially in safeguarding children's privacy. This analysis examines their alignment in data protection principles, child-specific safeguards, cross-border data transfers, and institutional oversight, highlighting areas where Kenya can enhance its framework, particularly in the Maisha Card system.

4.3.1 Principles Governing Data Protection

The GDPR outlines key tenets of data protection, such as purpose limitation, data minimisation, lawfulness, fairness, and transparency.[198] These principles strive to guarantee the processing of personal data responsibly, with particular emphasis on protecting vulnerable groups such as

[196] University of Oslo, *The Data Breach Notification Obligation in the GDPR*, 2020, 2.
[197] Nolan K, 'The Individual in EU Data Protection Law' Unpublished LLM Thesis, The London School of Economics and Political Science, London, 2023, 9.
[198] Article 5(1), *General Data Protection Regulation* (EU) (2016/679).

children.[199] These principles have set a high standard globally and are integral to GDPR's rights-based approach to data protection.

Kenya's DPA aligns well with many of these principles. For instance, both the GDPR and DPA emphasize data minimisation, which calls for the collection and processing of only the information required for the intended purpose.[200] This alignment demonstrates Kenya's commitment to embedding efficiency and responsibility in data processing activities. Similarly, both frameworks echo the notion of purpose limitation. According to the GDPR, personal data must only be collected for legitimate and explicit purposes and cannot be processed in a manner that is incompatible with those purposes.[201] The DPA's Section 25(a) incorporates similar language, ensuring that data controllers in Kenya adhere to this principle.[202]

Transparency is another principle where the DPA aligns commendably with the GDPR. Both laws mandate that individuals who provide data are aware of the methods used to gather, handle and use their data.[203] While the GDPR emphasizes child-friendly communication in Recital 58, the DPA does not explicitly outline similar requirements for children.[204] Nevertheless, the general transparency obligations under the DPA provide a solid foundation, and any additional focus on child-specific measures would enhance Kenya's framework rather than address a deficiency. In terms of fairness, the GDPR mandates that data be processed in a way that respects the rights and freedoms of individuals.[205] Kenya's DPA incorporates this principle implicitly, emphasizing lawful and ethical data processing.[206] This similarity reflects a strong alignment between the two frameworks in their legal provisions.

[199] Recital 38, *General Data Protection Regulation* (EU GDPR) (2016).
[200] Section 25(b), *Data Protection Act*, Cap 411C (2022).
[201] Article 5(1)(b), *General Data Protection Regulation* (EU) (2016/679).
[202] Section 25(a), *Data Protection Act*, Cap 411C (2022).
[203] Article 12, *General Data Protection Regulation* (EU) (2016/679) and Section 29, *Data Protection Act*, Cap 411C (2022).
[204] Recital 58, *General Data Protection Regulation* (EU GDPR) (2016).
[205] Article 5(1)(a), *General Data Protection Regulation* (EU) (2016/679).
[206] Section 25, *Data Protection Act*, Cap 411C (2022).

4.3.2 Safeguards for Children's Data

Kenya's Data Protection Act, aligns with the GDPR in several key areas, including provisions for DPIAs, pseudonymization, and privacy-by-design principles. Section 31 of the DPA mandates DPIAs for high-risk processing activities,[207] like Article 35 of the GDPR, ensuring that risks to data subjects are assessed and mitigated before data processing begins.[208] Additionally, Section 41 recognizes pseudonymization and encryption as critical technical measures to secure sensitive personal data,[209] aligning with the GDPR's emphasis on robust data security mechanisms.[210]

Privacy-by-design principles, which are a cornerstone of GDPR Article 25, are also addressed in Kenya's DPA.[211] Section 41(3) requires data controllers and processors to put in place organisational measures that integrate data protection principles into their processing activities.[212] This reflects a commitment to embedding privacy safeguards throughout the data lifecycle, particularly in systems like the Maisha Card, which handle sensitive biometric data of children. Despite these provisions, both frameworks lack explicit requirements for conducting CRIAs, which could ensure that the unique risks posed to children's data in systems like Maisha Card are specifically addressed. CRIAs differ from DPIAs in that they focus on assessing how proposed policies, laws, or systems may affect privacy rights of children, among other rights.

According to Livingstone and Third, children are uniquely vulnerable in digital environments due to their evolving capacities and limited ability to comprehend the long-term implications of data collection.[213] CRIAs are specialized methodologies designed to evaluate the potential impacts of data processing activities on children's rights, including privacy, development, and freedom of expression.[214] Unlike DPIAs, which focus broadly on risks to data subjects, CRIAs emphasize

[207] Section 31, *Data Protection Act*, Cap 411C (2022).
[208] Article 35, *General Data Protection Regulation* (EU) (2016/679).
[209] Section 25, *Data Protection Act*, Cap 411C (2022).
[210] Article 32(1), *General Data Protection Regulation* (EU) (2016/679).
[211] Article 25, *General Data Protection Regulation* (EU) (2016/679).
[212] Section 41(3), *Data Protection Act*, Cap 411C (2022).
[213] Livingstone S and Third A, 'Children and young people's rights in the digital age: An emerging agenda', 660.
[214] Digital Futures Commission, *Child Rights Impact Assessment: A tool to realise children's rights in the digital environment*, March 2021, 8.

children's best interests as a primary consideration, drawing on principles from international frameworks like the UNCRC.[215]

A CRIA could be used to pinpoint specific weaknesses in digital identity systems like Maisha Card, like the dangers of gathering and storing biometric data. These assessments would consider how the system impacts children's privacy, their authority over their personal data, and the potential for harm in cases of data breaches or misuse. UNICEF's Child Rights and Business Principles emphasize that businesses and governments alike have a duty to assess their impact on children's rights, further underscoring the need for CRIAs in the development and implementation of data-driven systems.[216]

Using instruments like CRIAs, the European Data Protection Board (EDPB) has acknowledged the vital necessity of incorporating children's rights into data protection frameworks. Guidelines for processing personal data under GDPR Article 6(1)(f) issued by the EDPB in 2024 highlight the importance of assessing children's best interests when balancing legitimate interests with data subjects' fundamental rights and freedoms.[217] These guidelines propose CRIAs as a procedural tool to ensure that the best interests principle is adequately considered in cases involving children.[218] This development signals a significant step toward operationalizing children's rights in data protection practices under the GDPR, aligning with the UNCRC's recommendation that children's best interests serve as both a substantive right and a procedural rule.[219]

Kenya's DPA provides for DPIAs under Section 31, requiring assessments for high-risk processing activities to identify and mitigate potential harm to data subjects.[220] While this provision aligns with GDPR Article 35, the DPA does not explicitly require CRIAs or similar child-specific impact assessments.[221] Given the unique risks associated with the Maisha Card system, which processes

[215] UN Committee on the Rights of the Child, *General Comment No. 14: On the Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration,* 29 May 2013, CRC/C/GC/14.
[216] UNICEF, *Child Rights and Business Principles,* 2013, 5.
[217] Article 6(1)(f), *General Data Protection Regulation* (EU) (2016/679).
[218] Fernandes E, Sas M, Dewitte P, and Verdoodt V, *Points of Attention Regarding the Processing of Children's Data in EDPB Guidelines 1/2024.*
[219] Article 3(1), *Convention on the Rights of the Child*, 20 November 1989, General Assembly resolution 44/25.
[220] Section 31, *Data Protection Act*, Cap 411C (2022).
[221] Article 35, *General Data Protection Regulation* (EU) (2016/679).

children's biometric data, CRIAs could play a vital role in ensuring that children's rights are not inadvertently compromised.

The absence of CRIAs within the Kenyan framework represents an opportunity for improvement rather than a deficiency in the current legal structure. By adopting CRIAs, Kenya could enhance its safeguards for children's data, ensuring that systems like the Maisha Card prioritize children's best interests and anticipate potential long-term impacts. This approach would align Kenya's framework with the progressive steps being taken under the GDPR and reinforce its commitment to international best practices.

While both the GDPR and Kenya's DPA provide strong foundations for safeguarding children's data, the integration of CRIAs into these frameworks would mark a significant advancement in protecting children's rights. The EDPB's guidelines demonstrate the GDPR's commitment to evolving its approach to children's data protection, offering a valuable model for Kenya to follow.[222] By incorporating CRIAs, Kenya could ensure that its digital identity systems, such as the Maisha Card, fully address the unique vulnerabilities and rights of children.

4.3.3 Cross-Border Data Transfers

Cross-border data transfers encompass the movement of personal data across jurisdictions and are a critical consideration in data protection frameworks.[223] Such transfers carry significant risks, particularly for children's privacy, due to variations in the strength of data protection laws between countries. While the GDPR establishes stringent safeguards for cross-border data transfers, Kenya's framework under the DPA provides fewer comprehensive protections, exposing children's sensitive data to heightened vulnerabilities.

The GDPR sets a high standard for cross-border data transfers, ensuring that personal data leaving the European Economic Area (EEA) remains protected at a level equivalent to that within the

[222] Fernandes E, Sas M, Dewitte P, and Verdoodt V, *Points of Attention Regarding the Processing of Children's Data in EDPB Guidelines 1/2024.*

[223] Privacy Pillar, 'Cross Border Data Transfer Regulations: What you need to know?' 18 June 2024 – <https://privacypillar.com/cross-border-data-transfer/ > on 25 December 2024.

EU.[224] Article 44 restricts the transfer of data to third countries unless sufficient security measures are in place.[225] The adequacy mechanism, outlined in Article 45, empowers the European Commission to evaluate whether a third country's legal framework provides sufficient data protection, ensuring seamless data flows to jurisdictions deemed equivalent.[226] Where adequacy decisions are unavailable, Articles 46 and 49 provide alternative safeguards, including binding corporate rules (BCRs), standard contractual clauses (SCCs), or, in limited cases, explicit consent from the data subject.[227] These systems provide flexibility while preserving a high standard of safety for personal information, especially for vulnerable populations like children.

In comparison, Kenya's DPA takes a more general approach to cross-border data transfers. Sections 48 and 49 establish conditions for transferring personal and sensitive data to another jurisdiction, requiring proof of appropriate safeguards or the necessity of the transfer for specific purposes, such as public interest or contractual obligations.[228] However, Kenya's framework does not include predefined mechanisms like SCCs or BCRs, relying instead on the discretion of the Data Commissioner to evaluate safeguards on a case-by-case basis.[229] While this approach offers flexibility, the absence of detailed regulatory mechanisms creates uncertainty for data controllers and processors, particularly when managing high-risk data such as children's biometric information.

One key distinction is the role of adequacy decisions. The GDPR's Article 45 provides a systematic process for evaluating third countries' legal frameworks, fostering predictability and trust in international data flows.[230] Kenya's DPA, by contrast, lacks a comparable provision, leaving the determination of "commensurate data protection laws" under Section 48(b) largely undefined.[231]

[224] European Data Protection Board, 'Data Protection Guide for Small Businesses: International Data Transfers, European Union – <https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en#toc-2 > on 25 December 2024.
[225] Article 44, *General Data Protection Regulation* (EU) (2016/679).
[226] Article 45, *General Data Protection Regulation* (EU) (2016/679).
[227] Article 46(2), *General Data Protection Regulation* (EU) (2016/679).
[228] Section 48, *Data Protection Act* (Cap 411C of 2022).
[229] Section 48(b), *Data Protection Act* (Cap 411C of 2022).
[230] Article 45, *General Data Protection Regulation* (EU) (2016/679).
[231] Section 48(b), *Data Protection Act* (Cap 411C of 2022).

This gap increases the risk of subjective or inconsistent assessments, potentially exposing children's data to jurisdictions with weaker privacy standards.

Kenya can draw important lessons from the GDPR in strengthening its framework for cross-border data transfers. Introducing predefined mechanisms like SCCs and BCRs would provide clear and consistent safeguards, ensuring that children's data is adequately protected in global transactions. Additionally, establishing a process for recognizing jurisdictions with equivalent data protection standards, similar to the GDPR's adequacy decisions, would enhance predictability and accountability in international data transfers. By adopting these measures, Kenya can build a more robust framework for securing children's data, aligning its practices with international best standards.

4.3.4 Institutional Oversight

The GDPR establishes a robust institutional oversight framework through independent supervisory authorities, mandated under Article 51.[232] These authorities are tasked with monitoring compliance, investigating complaints, and enforcing data protection laws. Their independence is explicitly safeguarded under Article 52, which ensures that supervisory authorities operate free from external influence, including political or governmental interference.[233]

In addition to independence, the GDPR emphasizes coordination through the EDPB.[234] The EDPB facilitates harmonized enforcement across member states, particularly in cross-border data protection cases.[235] This collaborative structure enhances accountability and ensures that supervisory authorities consistently apply the GDPR's principles. These mechanisms are critical in addressing sensitive contexts, such as the processing of children's data, where impartiality and consistency are essential.

Kenya's DPA establishes the Office of the Data Protection Commissioner as the primary oversight body responsible for enforcing data protection laws.[236] Under part VIII of the DPA, the ODPC is

[232] Article 51, *General Data Protection Regulation* (EU) (2016/679).
[233] Article 52, *General Data Protection Regulation* (EU) (2016/679).
[234] Article 70, *General Data Protection Regulation* (EU) (2016/679).
[235] European Data Protection Board, *Contribution of the EDPB to the report on the application of the GDPR under Article 97*, 12 December 2023, 9.
[236] Section 5, *Data Protection Act*, Cap 411C (2022).

mandated to monitor compliance, investigate complaints, and oversee data controllers and processors.[237] While the establishment of the ODPC demonstrates Kenya's commitment to data protection, challenges persist, particularly regarding its independence and institutional coordination.

The ODPC's independence is not fully guaranteed under the current framework. Section 5(5) of the DPA allows for the Cabinet Secretary for ICT to play a role in operationalizing the ODPC[238], while the ODPC is also subject to potential influence from national security organs.[239] These dependencies introduce risks of external interference, particularly in politically sensitive or high-stakes cases. Scholarly analyses, such as Vermeulen et al., emphasize that supervisory authorities must be entirely independent to effectively protect vulnerable groups like children.[240] Without robust guarantees of autonomy, the ODPC's ability to enforce data protection laws impartially and effectively is undermined.

To address these challenges, Kenya's framework could benefit from strengthening the ODPC's independence by amending the DPA to remove provisions allowing for Cabinet Secretary involvement and ensuring the ODPC operates free from influence by other state organs. Additionally, Kenya could establish formal coordination mechanisms between the ODPC and child protection institutions, drawing lessons from international best practices like the GDPR's EDPB. These measures would foster a more unified and robust oversight framework, ensuring that children's privacy is effectively safeguarded in systems like the Maisha Card.

4.4 Conclusion

This chapter sought to identify lessons that can be learned from Europe's data protection legislation (GDPR) regarding how children's right to privacy is upheld. Following a benchmark analysis, several key lessons emerge. The GDPR underscores the importance of embedding children's rights into data protection frameworks through robust principles like privacy by design, technical safeguards such as encryption and pseudonymization, and procedural tools like DPIAs.

[237] Part VIII, *Data Protection Act*, Cap 411C (2022).
[238] Section 5(5), *Data Protection Act*, Cap 411C (2022).
[239] Section 8(2), *Data Protection Act*, Cap 411C (2022).
[240] Vermeulen G and Lievens E, *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance, and big data*, Maklu Publishers, Antwerp, 2017, 181.

The recent emphasis on CRIAs further highlights the need to address the unique vulnerabilities of children in data processing. Kenya's DPA aligns with the GDPR in many respects but lacks equivalent operational features such as binding corporate rules, adequacy decisions and standardized contractual clauses for cross-border transfers. Strengthening institutional oversight, enhancing legal specificity, and introducing child-specific impact assessments could significantly improve Kenya's framework, ensuring that systems like the Maisha Card uphold children's privacy rights effectively. These lessons from the GDPR provide a roadmap for Kenya to bridge existing gaps and adopt international best practices.

Chapter 5:

Conclusion and Recommendations

5.1 Introduction

This chapter synthesizes the findings of this study, which examined the implications of digital identity systems for children's privacy rights in Kenya. It provides an overview of the findings from each chapter, evaluates the hypothesis, and presents recommendations for strengthening Kenya's legal framework to safeguard children's privacy. The analysis underscores the urgency of addressing gaps in existing legislation to ensure that digital identity systems prioritize the rights and best interests of children.

5.2 Summary of Findings

With respect to the question on the potential implications of failing to uphold children's right to privacy in digital identity systems, the second chapter revealed that such failures expose children to significant risks, including identity theft, profiling, and mission creep. These risks are heightened by the sensitivity and permanence of biometric data, which, once compromised, cannot be replaced. The analysis further demonstrated how inadequate safeguards, such as the absence of robust data protection mechanisms and child-specific privacy provisions, exacerbate these vulnerabilities, potentially resulting in long-term harm to children's autonomy, identity, and future opportunities. The chapter emphasized the critical importance of implementing privacy-by-design principles, minimizing data collection, and ensuring accountability in digital identity systems to mitigate these risks and uphold children's rights.

With respect to the question on whether the current legal framework is adequate and comprehensive enough to protect children's right to privacy in providing for digital identity systems, the third chapter revealed that while Kenya has foundational protections in place through the Constitution, the Data Protection Act, the Children Act and key regulations, significant gaps remain. The legal framework does not adequately address the unique vulnerabilities of children, such as data minimization and safeguards for biometric data. Additionally, the chapter highlighted insufficient coordination among institutions tasked with implementing privacy protections, as well

as the lack of comprehensive oversight mechanisms for digital identity systems like the Maisha Card. These gaps underscore the need for explicit, child-centric legal and policy reforms to ensure children's privacy rights are effectively safeguarded in the digital age.

With respect to the question on the lessons that can be learned from Europe's data protection legislation regarding how children's right to privacy is upheld, the fourth chapter demonstrated that the GDPR provides valuable best practices that Kenya can adopt to strengthen its legal framework. These include embedding privacy-by-design principles and implementing stringent safeguards for cross-border data transfers, which include binding corporate rules and adequacy decisions. Additionally, the chapter highlighted the emerging importance of CRIAs, which focus specifically on evaluating the impact of data processing on children's rights. By incorporating CRIAs and adopting these GDPR-inspired measures, Kenya can ensure that its legal framework effectively addresses the unique privacy risks faced by children in digital identity systems.

5.4 Recommendations

1. Introduce a provision in the Data Protection Act requiring CRIAs to evaluate the impact of data processing on children's rights, particularly in systems like the Maisha Card.
2. Revise Section 48 of the Data Protection Act to establish clearer mechanisms for cross-border data transfers, such as adequacy decisions, binding corporate rules, and standard contractual clauses, with stricter safeguards for transfers involving children's data.
3. Amend the Births and Death Registration Act to mandate data protection guidelines for the generation, storage, and management of Unique Personal Identifiers under Regulation 8 of the Birth and Death Registration (Amendment) Rules, ensuring compliance with privacy safeguards outlined in the Data Protection Act, 2019.
4. Strengthen institutional coordination by amending the Children's Act to establish formal collaboration mechanisms between the ODPC and child welfare institutions, such as the National Council for Children's Services, to ensure a unified approach to protecting children's data.
5. Include provisions under the Registration of Persons (Amendment) Regulations to address data minimization for biometric data collection and introduce clear policies for the management, storage, and secure handling of biometric identifiers.

6. Amend Section 6 of the Data Protection Act to explicitly guarantee the independence of the ODPC, including removing provisions allowing for Cabinet Secretary involvement and ensuring the ODPC is free from interference by other state organs.
7. Establish comprehensive technical and legal policies under the Data Protection Act addressing the collection, storage, and use of biometric data. These policies should specify encryption standards, access controls, and the technical requirements for biometric recording devices.
8. Revise Regulation 10(2) of the Births and Deaths Registration (Amendment) Rules to require training programs for registrars on data security and protection practices, particularly in regions with low digital literacy.
9. Amend Regulation 7 of the Registration of Persons (Amendment) Rules to remove provisions allowing for the use of either UPIs or new index numbers, ensuring a unified and consistent identification system.
10. Enhance data protection education and awareness by incorporating provisions in the Children's Act requiring public education campaigns targeting children, parents, and guardians on the importance of privacy and the risks associated with digital identity systems.

5.5 Conclusion

The hypothesis proposed that the implementation of digital identity systems in Kenya could influence the protection of children's privacy rights by introducing both potential benefits and risks. This study confirms the hypothesis. Digital identity systems offer benefits such as improved service delivery and streamlined governance. However, they also introduce significant risks to children's privacy, particularly in the absence of robust legal protections. Kenya's current legal framework, while foundational, is insufficient to address these risks, highlighting the need for reforms to ensure that digital identity systems uphold children's privacy rights.

Bibliography

Books

Bygrave A, *Data Privacy Law: An International Perspective*, Oxford Unity Press, London, 2014.

Dimock S, *Classic Readings and Cases in Philosophy of Law,* York University, New York, 2007.

Eubanks V, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor,* St. Martin's Press, New York, 2018.

Liu N, *Bio-Privacy: Privacy Regulations and the Challenge of Biometrics*, 1st ed. Routledge, London, 2011.

Lyon D, *Surveillance Studies: An Overview*, Polity Press, United Kingdom, 2007.

Mordini E and Tzovaras D, *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer Science & Business Media, London, 2012

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge, 2015.

Schneier B, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W, Norton & Company, New York, 2016.

Westin A. F, Privacy and Freedom, 25 *Wash. & Lee L. Rev.* 166, 1968.

Zuboff S, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, PublicAffairs, New York, 2019.

Journals

Bhandari V and Sane R, 'A Critique of the Aadhaar Legal Framework' 13 *National Law School of India Review* 1, 2019.

Bondre A, Pathare S and Naslund J, 'Protecting Mental Health Data Privacy in India: The Case of Data Linkage with Aadhaar' 9 *Global Health: Science and Practice* 3, 2021.

Bunn A, 'The Curious Case of the Right to Be Forgotten' 31 *Computer Law & Security Review* 3, 2015.

Caglar C, 'Children's Right to Privacy and Data Protection: Does the Article on Conditions Applicable to Child's Consent Under the GDPR Tackle the Challenges of the Digital Era or Create Further Confusion?' 12 *European Journal of Law and Technology* 2, 2021.

Custers B, Dechesne F, Sears A, Tani T and Hof S, 'A Comparison of Data Protection Legislation and Policies Across the EU' 34 (2) *Computer Law & Security Review*, 2018.

Dixon P, 'A Failure to "Do No Harm" — India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S' 7 *Health and Technology*, 2017.

Goodell G and Aste T, 'A Decentralized Digital Identity Architecture' 2 *Frontiers Blockchain* 17, 2019.

Greenleaf G, 'India's National ID System: Danger Grows in a Privacy Vacuum' 26 *Computer Law & Security Review* 5, 2010.

Jacobsen E, 'Unique Identification: Inclusion and Surveillance in the Indian Biometric Assemblage' 43 *Security Dialogue* 5, 2012.

Kohl U, 'The Right To Be Forgotten In Data Protection Law And Two Western Cultures Of Privacy' 72 *International and Comparative Law Quarterly* 3, 2023.

Koops B, 'The Concept of Function Creep' 13 Law, *Innovation and Technology* 1, 2021.

Laufer R and Wolfe M, 'Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory' 33 *Journal of Social Issues* 3, 1977.

Livingstone S, 'Children: A Special Case for Privacy?' 46 *Intermedia* 2, 2018.

Macenaite M and Kosta E, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?' 26 *Information & Communications Technology Law* 2, 2017.

Macenaite M, 'From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation' 19 *New Media & Society* 5, 2017.

Milkaite L and Lievens E, 'Child-Friendly Transparency of Data Processing in the EU: From Legal Requirements to Platform Policies' 14 *Journal of Children and Media* 1, 2019.

Murray D and Fussey P, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' 52 *Israel Law Review* 1, 2019.

Priel D, 'Reconstructing Fuller's Argument Against Legal Positivism' 26 *Canadian Journal of Law & Jurisprudence* 2, 2013.

Rao U and Nair V, 'Aadhaar: Governing with Biometrics' 42 *Journal of South Asian Studies* 3, 2019.

Ryngaert C and Taylor M, 'The GDPR as Global Data Protection Regulation?' 114 *AJIL Unbound*, 2020.

Sindakis S and Showkat G, 'The Digital Revolution in India: Bridging the Gap in Rural Technology Adoption' 13, *Journal of Innovation and Entrepreneurship* 29, 2024.

Stoilova M, Livingstone S and Nandagiri R, 'Digital by Default: Children's Capacity to Understand and Manage Online Data and Privacy' 8 *Media and Communication* 4, 2020.

Stoilova M, Nandagiri R and Livingstone S, 'Children's Understanding of Personal Data and Privacy Online — A Systematic Evidence Mapping' 24 *Information Communication & Society* 4, 2019.

Taylor M and Paterson J, 'Protecting Privacy in India: The Roles of Consent and Fairness in Data Protection' 16 *Indian Journal of Law and Technology* 1, 2020.

Upendra B, 'From Human Rights to the Right to Be Human: Some Heresies' 13 *International Centre Quarterly* 3/4, 1986.

Van Der Hof S, 'I Agree. . . or Do I? — A Rights-Based Analysis of the Law on Children's Consent in the Digital World' 4 *Wisconsin International Law Journal* 4, 2017.

Velasquez E and Lacey C, 'The Evolution of Identity Crime and its Impacts' 37 *GPSolo* 5, 2020.

Voss W and Hugues B, 'EU General Data Protection Regulation Sanctions in Theory and in Practice' 37 *Santa Clara High Technology Law Journal* 1, 2021.

Yin W, 'Zero-Knowledge Proof Intelligent Recommendation System to Protect Students' Data Privacy in the Digital Age' 37 *Applied Artificial Intelligence* 1, 2023.

Dissertation and Theses

Nolan K, 'The Individual In EU Data Protection Law' Unpublished LLM Thesis, The London School of Economics and Political Science, London, 2023.

Nyakundi, F. N. 'Huduma Namba: Kenya's Transformation into an Informational State' Published LLM Thesis, University of Washington, Washington, 2020.

Sharif U, 'The Effects of Security Breaches on Data Integrity' Published LLM Thesis, University of the Cumberlands, Kentucky, 2024.

Walumoli B, 'A Critical Analysis of the Challenges Facing Counter-Cybercrime in 21st Century Africa: A Focused Comparison of Kenya and Rwanda' Unpublished LLM Thesis, University of Nairobi, Nairobi, 2021.

Reports

Children's Commissioner for England, *Who Knows What About Me? A Children's Commissioner Report into the Collection and Sharing of Children's Data*, November 2018.

European Commission, *Second Report on the Application of the General Data Protection Regulation*, July 25, 2024.

OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, 6 October 2015.

OECD, *Draft Recommendation on the Governance of Digital Identity*, March 17, 2023.

Privacy International, *Biometrics: Friend or Foe of Privacy?* November 2017.

Privacy International, *Data Protection Impact Assessments and ID Systems: The 2021 Kenyan Ruling on Huduma Namba*, January 27, 2022.

Privacy International, *Digital National ID Systems: Ways, Shapes and Forms, Privacy International*, October 26, 2021.

Privacy International, *The Right to Privacy in Kenya: Stakeholder Report Universal Periodic Review 35th Session - Kenya*, July 2019.

Privacy International, *What Is Privacy?* October 23, 2017.

UNICEF, *Faces, Fingerprints & Feet: Guidance on Assessing the Value of Including Biometric Technologies in UNICEF-Supported Programs*, July 2019.

UNICEF, *The Case for Better Governance of Children's Data: A Manifesto*, May 2021.

World Bank Group, *Digital Access: The Future of Financial Inclusion In Africa*, May 2018.

World Bank Group, *Privacy by Design: Current Practices in Estonia, India, and Austria*, 2018.

World Bank Group, *The State of Identification Systems in Africa: A Synthesis of Country Assessments*, 2017.

World Bank Identification for Development (ID4D), *The Role of Digital Identification for Healthcare: The Emerging Use Cases*, 2018.

World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age*, February 2021.

Working Papers

Bajpai N and Biberman J, 'Digital Identification and ICT-Driven Development in Africa' ICT India Working Paper Number 49, Columbia University Centre for Sustainable Development, May 2021.

Bhatnagar S, 'Public Service Delivery: Role of Information and Communication Technology in Improving Governance and Development Impact' ADB Economics Working Paper Series Number 391, Asian Development Bank, March 2014.

Kramer M, 'The Legal Positivism of H.L.A Hart' Research Paper No. 11/2019, University of Cambridge Faculty of Law, March 2019.

OECD Publishing, 'Protecting Children Online an Overview of Recent Developments in Legal Frameworks and Policies' OECD Digital Economy Papers Number 295, OECD, May 2020.

Self-Published Articles

Al Kags, 'Maisha Namba: Thoughts About Kenya's Evolution of Identity' Open Institute, September 2, 2024.

Barnwal P, 'Curbing Leakage in Public Programs with Direct Benefit Transfers Evidence from India's Fuel Subsidies and Black Markets' World Bank, 2016.

Gichohi L, 'Kenya's Digital ID: Balancing Progress with Privacy Concerns' KICTANet, February 22, 2024.

Indeje D, 'New Report Identifies Achievements, Challenges and Recommendations to Enhance Data Protection in Kenya' KICTANet, 8 May 2024.

Khatchatourov A, Laurent M and Levallois-Barth C, 'Privacy in Digital Identity Systems: Models, Assessment and User Adoption' ResearchGate, 2024.

Kipkoech D, 'Navigating the Crossroads: The Challenges of Cross-Border Data Flows Under Domestic Laws in Africa' Centre for Intellectual Property and Information Technology Law, November 23, 2023.

Livingstone S, Stoilova M, and Nandagiri R, 'Children's Data and Privacy Online: Growing Up in a Digital Age: An Evidence Review' London School of Economics and Political Science, 2019.

Mutung'u G, 'Digital Identity in Kenya: Case Study Conducted as Part of a Ten-Country Exploration of Socio-Digital ID Systems in Parts of Africa' Research ICT Africa, November 2021.

OJEN-ROEJ, 'Section 1 of the Charter and the Oakes Test' Ontario Justice Education Network, 2013.

Prof. Kang'ara, S. 'Digital Identification Law in Kenya: The State of Play' Policy Brief No. 5, Kenya ICT Action Network, August 2020.

Tyagi A, Rekha G, and Sreenath N, 'Is Your Privacy Safe with Aadhaar? An Open Discussion' Distributed and Grid (PDGC), 2018.

Wabulengo J, 'Is the Huduma Namba Back?' KICTANet, July 11, 2023.

Internet Resources

< https://www.cookiebot.com/en/kenya-dpa/ > on 11 September 2021.

Al Kags, 'Maisha Namba: Thoughts about Kenya's evolution of identity' Open Institute, 2 September 2024 — <https://alkags.me/maisha-namba/ > on 21 November 2024.

European Data Protection Board, 'Data Protection Guide for Small Businesses: International Data Transfers, European Union – <https://www.edpb.europa.eu/sme-data-protection-guide/international-data-transfers_en#toc-2 > on 25 December 2024.

Privacy Pillar, 'Cross Border Data Transfer Regulations: What you need to know?' 18 June 2024 – <https://privacypillar.com/cross-border-data-transfer/ > on 25 December 2024.

OECD Publishing, 'Protecting Children Online An Overview Of Recent Developments In Legal Frameworks and Policies' OECD, OECD Digital Economy Papers Number 295, May 2020, 34 – https://www.oecd.org/content/dam/oecd/en/publications/reports/2020/06/protecting-children-online_0c385619/9e0e49a9-en.pdf on 8 December 2024.

Institutional Papers

Amnesty International, *Digital ID in Kenya (An Advisory Policy Paper Providing a Roadmap to the Implementation of a Rights Respecting Digital ID Regime in Kenya)*, 2023.

Berkeley Law, *Digital Identity and the Legal Obligation to Conduct a Human Rights Impact Assessment in Kenya,* April 2023.

Child Front and Centre, *Fundamentals for a Child-Oriented Approach to Data Processing*, December 2021.

Council on Foreign Relations, *How India's Controversial Biometric ID System Can Help Women*, 2018.

European Data Protection Board, *Guidelines 05/2020 on Consent*, Regulation 2016/679.

FSD Kenya, *Data Privacy and Protection in Kenya: A Regulatory Review*, January 2022.

Information Commissioner's Office, *Age-Appropriate Design: A Code of Practice for Online Services*, September 2, 2020.

Information Commissioner's Office, *Children and the GDPR*, March 22, 2018.

Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, August 2018.

Kenya Human Rights Commission, *Government Shouldn't Force Flawed Digital ID System in Kenya*, February 27, 2024.

World Bank Group Committee on Payments and Market Infrastructures, *Payment Aspects of Financial Inclusion in the Fintech Era*, April 2020.