Data & Policy (2024), 6: e7
doi:10.1017/dap.2023.36

RESEARCH ARTICLE

An assessment of the legal and regulatory framework supporting the implementation of the National Integrated Identity Management System (NIIMS) in Kenya

Victor Kabata

Records and Archival Science History Department, Sorbonne University, Abu Dhabi, UAE
Email: Victor.kabata@sorbonne.ae

Received: 20 December 2021; **Revised:** 18 October 2023; **Accepted:** 20 October 2023

Keywords: digital identity system; Kenya; legal; regulatory framework

Abstract

This study sought to establish the elements that constitute comprehensive legal and regulatory landscape for successful digital identity system establishment and implementation. Subsequently, the study sought to assess whether these elements were present in the establishment and implementation of the National Integrated Identity Management System (NIIMS) in Kenya. The study adopted a qualitative approach, data was obtained firstly, through literature review that provided background information to the study. Secondly, semi structured interviews were undertaken on purposively selected key informants. The study established that the elements that constitute a robust legal and regulatory framework for digital identity (ID) establishment and implementation include presence of a constitutional provision on the right to privacy; existence of a digital ID law governing the establishment of the system; amendment of laws relating to the registration of persons; existence of a data protection law; existence of an overarching law governing the digital economy among others. Largely, most of these elements were present in Kenya. However, the legislative approach adopted in crafting digital ID law in Kenya was wanting. This has undermined effective implementation of the NIIM system by among other things eroding public confidence in the system. The study concluded that effective operation of the system hinged on the existence of a robust and comprehensive legal and regulatory framework that will engender users' trust in the system. In this regard, the study recommended review of the existing legal framework to ensure that it underpins both the foundational and functional aspects of the NIIM system.

Policy Significance Statement

This study is significant to policymakers in several ways. First, it outlines the set of laws that countries must enact prior to implementing digital identity systems in their jurisdictions. Further, the study provides best practice cases of successful digital identity systems implementation across the world, which policymakers can use as a benchmark to ensure successful digital identity implementation. Thirdly, the results of this study can be used by policymakers in regional bodies such as European and African Union to develop a digital identity system legal guidebook that guides member states seeking to establish and implement digital identity systems. Overall, the result of this study supports policymakers in establishing a robust, inclusive, legal, and trusted digital identity systems.

1. Introduction

World over, proof of identity is a key requirement for accessing essential services such as education, healthcare, social security benefits as well as exercising rights such as electoral participation and overall contribution toward development. Despite the obvious benefits of proof of identity, it is still not a reality to many. Indeed, according to World Bank's identity for development report, by 2018, an estimated 1 billion people globally faced challenges in proving who they are due to lack of official proof of identity. This undermines their ability to access basic services (World Bank, 2018). There have been several initiatives aimed at addressing this global identity coverage gap. Key among them was the move by the United Nations General Assembly in 2015 that identified the provision of legal identity as one of the agenda for sustainable development. Specifically, target 16.9 of the sustainable development goals requires UN member states to provide legal identity to all by 2030 (United Nations, 2015). Towards this end, many countries have prioritized the provision of legal identity to their citizens by establishing unique digital identity management systems. Whilst implementing digital identity management systems is a useful step toward closing the proof of identity gap, ensuring that the systems are inclusive and trusted to safeguard privacy remains a challenge. Indeed, according to World Bank's Identification for Development Report 2018, identity systems in many developing countries are weak, exclusionary, and expose citizens' personal data to privacy risks (World Bank, 2018).

One way of ensuring that the adopted digital identity management systems are inclusive and trusted is by anchoring them on a robust legal and regulatory framework. Indeed, according to World Bank's report (2018), a comprehensive legal and regulatory framework is a globally recognized prerequisite for successful digital identity systems. A comprehensive legal framework underpins both the foundational and the functional aspects of the digital identity system and provides broad provisions and principles on the collection, storage, and use of personal information, among other aspects. Whilst all previous studies on digital identity systems agree that a successful digital identity system should be anchored on a robust legal and regulatory framework, none of these studies enumerates the set of laws that would constitute a robust legal and regulatory framework for digital ID implementation. This is the research gap that this study seeks to address.

The study sought to establish the following: firstly, the set of laws that constitute a robust legal and regulatory framework for successful digital identity system establishment and operation, and secondly, whether these laws were present to support the establishment and implementation of the NIIM system in Kenya. Lastly, the study will make recommendations on areas of improvement.

1.1. Research problem

Kenya has recently implemented a National Integrated Identity Management System (NIIMS). While the benefits of adopting a centralized identity management system cannot be overemphasized, one persistent challenge associated with their deployment is the aspect of privacy. In particular, centralized identity management systems are susceptible to data security and privacy concerns such as functional creep, where personal information collected for one purpose could be used for other purposes; increased government surveillance, where the data in the identity system may be used to monitor and control citizens; loss of anonymity, especially where personal data in the identity system is used to build behavior profiles, thus aiding surveillance capitalism. One way of engendering trust and safeguarding the privacy of personal data held in digital identity systems is ensuring that the system is anchored on a robust legal and regulatory regime. Granted, there have been recent studies on digital identity systems. Specifically, in 2020, the Centre for Internet and Society (CIS) initiated a study whose aim was to develop an evaluation framework to assess India's digital identity system (Aadhaar) for compliance with international rights and data protection principles. The study sought to assess if India's Aadhaar system complied with the rule of law test, the rights-based test, and the risk-based test of the CIS evaluation framework (Bhandari et al., 2020, p. 2).

In 2021, CIS expanded the context of the evaluation framework by covering 10 countries in the African continent. These were Kenya, Ghana, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe. Whilst these studies have succeeded in outlining the parameters (rule of law,

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

rights-based test, and risks test) for assessing digital identity systems, they did not spell out the set of laws and policy framework that countries intending to deploy digital identity systems should have in place. This study seeks to address this research deficiency by the following methods: first, content analyzing the parameters set out in the CIS evaluation framework to identify the specific laws and policy framework necessary for digital identity system establishment and operation; second, establishing whether the identified laws and policy framework were present in the establishment and implementation of the NIIM system in Kenya; and lastly, making recommendations on areas of improvement.

1.2. Research questions

The aim of the study will be achieved through the following research questions.

1. What set of laws and policy framework constitute a robust legal and regulatory framework for the successful establishment and implementation of a digital identity system?
2. To what extent are the identified set of laws and policy framework present in the establishment and implementation of the NIIMS in Kenya?
3. What recommendations for improvement can be made from the areas of strengths and weaknesses identified?

1.3. Rationale for the study

An analysis of extant literature reveals that successful digital identity programs are underpinned by a supportive legal and regulatory framework. Indeed, privacy advocates across the world contend that the establishment and implementation of a digital identity system should be preceded by a comprehensive legal assessment. This assessment should be underpinned by the CIS evaluation framework and should address the following areas: legal authority of the digital ID system, protection of people's rights, and establishing whether the existing policies promote implementation of the digital ID (Atick et al., 2014). One way of ensuring that countries deploy digital identity systems that adhere to international human rights and data protection principles is clearly articulating the set of laws and policy framework that need to be formulated and enacted.

The need to have a comprehensive legal and regulatory framework for the NIIM system is further underlined by a ruling to a case (Nubian Rights Forum & 2 others v. Attorney-General & 6 others, 2020) challenging the system. In particular, the High Court of Kenya in January 2020 ruled that the government should enact an "appropriate and comprehensive regulatory framework" for digital ID prior to the rollout of the NIIMS program (NIIMS case 2020, para 1047 (111)).

1.4. Conceptual framework

Prior to discussing the conceptual framework for this study, it is equally important to understand Kenya's legal system. An understanding of Kenya's legal structure is crucial to the present study as it enables us to appreciate the principles and protocols that guide legal decisions in the country. Further, it enlightens us on the legal context that the NIIMS is expected to operate in.

Palmer and Palmer (2012) note that the phenomenon of legal pluralism is gaining traction across the world. Essentially, a pluralist legal system is regarded as a mixed legal system where the law is derived from different sources such as the constitution, case law, customary and indigenous law, statutes, and regulations. A detailed analysis of the origin and basis of the mixed legal system though enriching is clearly beyond the scope of this paper.

For purposes of this study, Palmer and Palmer (2012) note that Kenya has adopted a mixed legal system which is a combination of the common law, Islamic law, and customary and indigenous law. As a former British colony, the country subscribes to the "English law" or common law system. This means that legal decisions are based on precedence or simply decisions taken in earlier cases on similar matters (Palmer and Palmer, 2012). An important aspect to note about countries that espouse common law systems is that

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

they develop specific written statutes (laws) to address specific matters. However, these statutes are introduced when the government deems it appropriate to introduce a particular legislation. This is consistent with the central thesis of this paper that argues that countries need to enact certain set of laws prior to implementing digital identity management systems.

Although Kenya subscribes to Islamic law that is administered through Kadhi courts, Hofman and Katuu (2023) note that Kadhi courts are subordinate to common law courts. As such, it is unlikely that Kadhi courts in Kenya would make a pronouncement relating to digital identity. Furthermore, the constitution of Kenya (2010) restricts the Islamic law to determining questions of Muslim law relating to personal status, marriage, divorce, and inheritance for parties that profess Muslim faith (Hofman and Katuu, 2023).

In terms of the conceptual framework, the study is underpinned by the CIS evaluation framework, which sets out a framework for evaluating digital identity systems. The framework outlines principles for assessing digital identity systems for compliance with international rights and data protection principles (Bhandari et al., 2020, p. 2).

The CIS evaluation framework is anchored on the international necessity and proportionate principles on the application of human rights to communication surveillance, the Organization for Economic Cooperation and Development (OECD) privacy guidelines, and the international scholarship on harm-based approaches (Mutun'gu, 2021).

As mentioned earlier, the centralized nature of digital identity systems means that their implementation exposes citizens or data subjects to ills such as surveillance, mission creep, exclusion, and loss of privacy. The CIS evaluation framework is considered appropriate for evaluating digital ID systems because it embodies international human rights laws and data protection principles. As such, using the framework as a lens to assess digital ID systems ensures that the systems are inclusive, protect citizens' right to privacy, and safeguard personal data.

Further, the CIS framework recognizes that the use of a digital ID system is inseparable from the governance structure and the features of the digital ID system. In this regard, the framework provides a series of tests that allows for the assessment of the legitimacy and governance of the digital ID (Mutun'gu, 2021).

The principles that underlie the CIS evaluation framework are classified broadly under three tests. That is, rule of law test, rights-based test, and risk-based test. These three tests form the framework against which digital ID systems are evaluated.

Below is a brief discussion of the provisions of each of these tests and the elements that constitute them.

Within the rule of law test of the CIS evaluation framework, there is the principle of legality. This principle contends that any system that is used to deliver public functions can only be legitimate (legal) if it is anchored on an appropriate legal framework that mandates it to be used for such purposes. Further, the principle of legality provides that any system whose use interferes with human rights must be prescribed in law. Essentially, this principle argues that the state can only deploy or implement a system that interferes with human rights if there is a publicly available legislative act which is clear and precise and which forewarns citizens (Organisation for Economic Co-operation and Development (OECD), 2013). Evidently, this principle is relevant and consistent with this study as it, firstly, reinforces the need to have a law that outlines the legality of the digital ID system and, secondly, buttresses the need for Kenya's NIIM system implementation to be underpinned by an appropriate legal framework. In the present study, this aspect will be addressed by, first, content analyzing the elements of the CIS evaluation framework to identify the law that provides for the legality of the digital ID system and, secondly, establishing the existence of this law in the establishment and operation of the NIIMs system.

There is also the principle of necessity that is captured under the rights-based test of the CIS evaluation framework. This principle prescribes that when a government deploys a particular technology/ system whose use is likely to interfere with citizens' right to privacy, then it must demonstrate that the use of that technology is necessary to achieve certain defined goals. This necessity can be demonstrated through a needs assessment which would be part of a broader data protection impact assessment. In the current study, this aspect is addressed by, first, identifying the right to privacy as a requirement when deploying digital ID systems and, second, assessing whether Kenya has a constitutional provision on the right to

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

privacy and data protection legislation, and whether the NIIM system adheres to data protection principles.

The appropriateness of the CIS evaluation framework as an analytical lens for this study is further reinforced by the fact that the framework is anchored on the OECD principles, which embody data protection principles. Essentially, OECD principles are a set of guidelines on privacy that were developed by OECD member countries as a step toward ensuring harmonized privacy legislations that facilitate safe transborder flow of data across frontiers. The OECD countries include Austria, Canada, Denmark, Germany, France, Norway, and Sweden, among others (Organisation for Economic Co-operation and Development (OECD), 2013).

The OECD principles include collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability (Organisation for Economic Co-operation and Development (OECD), 2013). Essentially, the idea is that although different countries may have disparate privacy legislations, at the very least this legislation should embody the above principles. Notably, European Union (EU) General Data Protection Regulations (GDPR) embodies all the OECD principles.

As mentioned earlier, the CIS evaluation framework assesses digital identity systems' compliance to international rights and data protection principles based on the rights-based test, rule of law test, and risk-based test. Each of these tests comprises a set of elements which seek to establish whether the digital identity system being implemented has legal authority (whether it is anchored in law), whether it protects citizens' rights, and the risks or harms that implementation of the system may expose citizens to.

For purposes of this study, the rule of law tests and the rights-based tests are most relevant in achieving the objective of the study as they outline the elements that assist us in identifying specific legislations that are key to the successful establishment and implementation of a digital identity system. In essence, a content analysis of the text of the elements assessed by the rule of law and rights-based tests gives us a clear picture of the set of laws that need to be in place for the NIIM system to operate within the required legal framework.

On the other hand, the risk-based test, though useful in the overall evaluation of a digital identity system, may not be applicable to this study. This is because it focuses on identifying the specific harms that implementation of a digital identity system may expose citizens to, and the measures to mitigate those harms. This is clearly beyond the scope of this study whose only focus is to identify the set of laws and policy framework that would facilitate digital identity systems establishment and implementation and whether these set of laws were available in the Kenyan context.

In this regard, this paper will restrict itself to the rule of law test and the rights-based test in answering research questions one and two of the study. Below is a brief discussion of the elements that constitute these tests and their relevance to the present study.

As mentioned earlier, the NIIM system, just like other digital ID systems, seeks to collect large amounts of citizens' personal information. As such, during the operation of the system, there is a risk of infringing on citizens privacy rights.

To address this concern, the rule of law test of the CIS evaluation framework recommends that if the operation of a digital identity system will entail the collection of citizens' personal information, then that act of collecting personal data must be legal, have a legitimate aim, be accounted for, and prevent the misuse of that data for other purposes that are different from the original purpose (Bhandari et al., 2020, p. 3). Evidently, one of the legislations that would address the issues raised in a rule of law test is the digital ID system law that will define the scope and purpose and actors of the system and clearly articulate its legitimacy. Further, the legislation on registration of persons is also relevant as identity registration involves collection of data on personal attributes. Other legal provisions that would address these concerns include having a constitutional provision on the right to privacy and a data protection regime.

On the other hand, the rights-based test advocates a series of rights-based principles that assess the extent to which the implementation of a digital identity system infringes on the rights of individuals. These principles address aspects related to necessity and proportionality, data minimization, access control, exclusion, and mandatory use (Bhandari et al., 2020, p. 13).

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Notably, the aspect of necessity and proportionality has already been discussed earlier when explaining the principles that underlie the CIS evaluation framework. However, it is important to note that the issues related to this principle will largely be addressed in the digital ID law. As for data minimization, this is one of the data protection principles that is usually provided for in data protection legislation.

On the other hand, the access control element under the rights-based test normally relates to how access to personal data by the state and private entities is regulated. Ordinarily, access to information in many jurisdictions is controlled through the data protection law as well as the access/freedom of information legislation.

Still on the rights-based test, there is the element of exclusion which is concerned with ensuring that the implementation of a digital ID system does not exclude citizens or restrict their access to services. Primarily, issues related to exclusion are normally provided for in the Bill of Rights. Specifically, the Bill of Rights outlines fundamental human rights and freedoms that citizens are entitled to. As such, the right to equality and freedom from discrimination within the Bill of Rights addresses the aspect of exclusion.

The Bill of Rights, which entails safeguarding citizens' fundamental rights and freedoms, is also underpinned by Amartya Sen's capability approach that emphasizes that in social evaluations and policy design, the focus should always be on what people can do and their freedom to do so and removing constraints that allows them to live the kind of life they desire (Sen, 1999).

As such, Sen's capability theory is particularly relevant to this study since it recommends that countries should not implement digital identity systems that are discriminatory and violate the fundamental rights and freedoms of citizens. Instead, the set of laws on which the digital ID system is anchored on should perpetuate inclusiveness and safeguard citizens' fundamental rights and freedoms.

In particular, Sen's capability theory addresses the aspect of exclusion and discrimination of citizens which would undermine their ability to access certain electronic services. In this regard, Sen's argument is consistent with this study's central argument that a digital identity system should not perpetuate discrimination or exclusion of a section of citizens.

Similarly, the enactment of a law governing the digital economy would ensure that citizens have a digital ID that enables them to enjoy access to digital services without being exposed to digital ills such as identity theft, electronic fraud, and other cybercrimes. This is consistent with Sen's capability approach that seeks to remove constraints that would hinder citizens from living the kind of life they value.

In this regard, enactment of a law regulating the digital economy would ensure that citizens can engage in electronic transactions (buy goods and access services in the digital economy) without the fear of their privacy being violated or their digital identity being compromised.

From the above discussion, it is evident that the CIS evaluation framework (rule of law and rights-based tests) and Amartya Sen's capability approach (fundamental rights) provide an elaborate understanding of the building blocks of a robust legal and regulatory framework for digital identity system implementation.

These building blocks are the set of laws and policy framework that constitute a supportive legal and regulatory framework for digital identity establishment and implementation. They include the following:

- A constitutional provision that guarantees the right to privacy;
- An enabling law governing the establishment and operation of the digital ID system;
- Existence of law governing the collection, storage, and processing of personal information;
- Law governing access to information, that is, data protection law and freedom of information law;
- Existence of regulations to operationalize the data protection law;
- Law that establishes an authority to oversee and enforce the protection of personal data;
- An overarching law regulating the digital economy.
- Fundamental rights—Right to equality and freedom from discrimination

Table 1 outlines the set of laws identified after analyzing the elements of the rule of law and rights-based test of the CIS digital identity system evaluation framework.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Table 1. *Fundamental Laws for Digital ID implementation*

		Elements	Set of laws
CIS framework	Rule of Law Test	Legitimate mandate	Digital ID law
		Legitimate aim	Digital ID law
		Actors and purpose	Digital ID law
		Grievance redress	Data Protection law
		Accountability	Data Protection law
		Mission creep	Data Protection law
CIS framework	Rights-Based Test	Necessity and Proportionality	Digital ID law
		Data minimization	Data Protection law
			Data Protection Regulations
			Data Protection Policy
		Access control	Data Protection law
			Freedom of Information
		Exclusion	Bill of rights- Fundamental rights
		Mandatory use	Digital ID law
Amartya Sen's capability approach		Cybercrimes	Bill of rights- Fundamental rights and freedoms
		Identity Theft	
		Electronic fraud	Law governing the digital economy

Notably, the aspect of fundamental rights and freedoms as well as the law regulating the digital economy are underpinned by Amartya Sen's capability approach that advocates for creation of a conducive environment that enables citizens to embrace digital ID and participate in the digital economy.

2. Literature Review

There is growing consensus among privacy scholars that robust digital identity systems should be underpinned by a comprehensive legal and regulatory regime that promotes trust in the system and safeguards data privacy and users' rights (Atick et al., 2014; World Bank, 2018). Indeed, a trusted and inclusive digital identity system safeguards personal data privacy and security, minimizes abuse such as unauthorized surveillance, and ensures that identity system providers are accountable.

As earlier mentioned, with more countries undertaking digital identity management projects, efforts are being made to ensure that these digital identity systems do not perpetuate exclusion, mass surveillance, and other ills associated with centralized systems. This is achieved by ensuring that countries enact the aforementioned set of laws that will ensure that their digital identity systems are anchored on international rights and data protection principles.

Internationally, in 2020, the CIS made important strides toward this end by developing an evaluation framework for assessing digital identity systems. Although the CIS framework was initially used to evaluate India's Aadhaar system, it provides a useful benchmark for assessing digital identity system implementation, particularly in large population contexts.

Another useful benchmark is Estonia's approach to digital identity establishment and implementation which is regarded as a global model of excellence (Trikanad, 2020).

In Africa, Mutun'gu (2021) noted that the CIS digital identity evaluation project of 10 African countries (Kenya, Ghana, Lesotho, Mozambique, Nigeria, Rwanda, South Africa, Tanzania, Uganda, and Zimbabwe) provides a useful benchmark for implementing digital identity systems in the unique African context where countries have diverse governance and technological realities.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Granted, the aforementioned past studies on digital identity systems have been useful in two ways: first, facilitating the development of an evaluation tool to guide the assessment of digital identity systems' adherence to international rights and data protection norms; second, testing the application of the evaluation tool in different contexts, thereby providing a best practice framework. However, none of these studies has elaborately enumerated the set of laws and policy framework that constitute a robust legal and regulatory framework for successful digital identity system establishment and implementation.

This paper addresses this literature gap by providing a set of laws and policy framework that are key to the establishment and operation of an inclusive, trusted, and secure digital identity system. These laws have been identified through content analysis of the texts of the elements of the rule of law and rights-based test of the CIS evaluation framework a well as a review of literature on policy documents relating to digital identity systems implementation.

The paper also highlights the efforts made by various countries in creating a supportive legal and regulatory framework for the effective implementation of digital identity systems. Further, it discusses the specific elements of the rule of law and rights-based test that a specific legislation seeks to address.

The literature is organized based on the set of laws and policy tools outlined earlier that constitute a comprehensive legal and regulatory framework for the successful establishment and implementation of an inclusive, trusted, and secure digital ID.

2.1 A constitutional provision that guarantees the right to privacy

Any country that wishes to successfully implement a digital ID system should have the right to privacy recognized in the constitution. Indeed, the existence of a constitutional provision guaranteeing the right to privacy is an indication that the aspect of privacy has been prioritized in a given jurisdiction.

Although the rights-based test of the CIS framework does not make a direct reference to the right to privacy, the aspects that are assessed during the test all seek to protect the privacy of citizens from being violated. For instance, the requirement that digital identity systems should adhere to data minimization is intended to ensure that there is a restriction to the volume of citizens' personal information that is collected by the digital ID system. In this case, a digital ID system should only collect personal data that is relevant to serve its purpose.

As such, for purposes of this study, the existence of the right to privacy in any country that wishes to establish and implement a digital identity system is consistent with the rights-based test. First, a right to privacy law protects citizens' private information from being unnecessarily revealed or demanded by state agents. Secondly, it compels the state to safeguard citizens' privacy rights.

An analysis of the literature revealed that several countries around the world have explicit constitutional provisions on the right to privacy. These include Chile, China, Cuba, Finland, Germany, and Ghana, among others (Privacy International, 2021). Additionally, having constitutional privacy protections is important as it provides a foundation for the formulation and enactment of specific laws on data protection.

In contrast, in some countries such as the USA and Ireland, there is no specific reference to the right to privacy in the constitution. Instead, courts have developed these rights from the language of other constitutional provisions (World Bank, 2017).

Beyond having a constitutional provision, countries' commitment to protecting the right to privacy is also demonstrated through the ratification of international instruments relating to the protection of privacy. These include the following:

- Article 12 of the Universal Declaration of Human Rights 1948;
- Article 17 of the International Convention on Civil and Political Rights (ICCPR) (United Nations (UN), 1966).

Below is a brief discussion of each of the aforementioned international instruments and how they relate to the right to privacy.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

At the international level, the right to privacy has its origin in the "Universal Declaration of Human Rights (UDHR)" that was adopted by the United Nations on December 10, 1948. The UDHR states in Article 12 that

> [n]o one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks (UNGA) (1948: 74).

In the context of this paper, this means that the right to privacy as enshrined in the UDHR limits who can access our bodies, spaces, things, and more importantly our communications as well as our information [UDHR] (1948, p. 74).

This is particularly relevant for digital ID systems that act as a gateway to certain government services. In most cases, digital IDs require citizens to share personal data to access services. Rightfully, there is a concern that shared personal information may be misused by government agents to monitor citizens against their will. However, a government that has ratified the UDHR will be obliged to respect the right to privacy even when rolling out a digital identity system.

The right to privacy is also recognized in the ICCPR, which was adopted by the "United Nations (UN) General Assembly" as resolution 2200A in 1966. Article 17 of the ICCPR adopted the same language as the UDHR by stating,

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation (International Covenant on Civil and People's Rights (ICCPR) (United Nations (UN), 1966, p. 178).

In sum, in terms of the right to privacy, this paper will establish, firstly, if Kenya has a constitutional provision on the right to privacy and, secondly, whether the country has ratified and adheres to international instruments on the right to privacy.

2.2 An enabling law governing the establishment and implementation of the digital identity system

Robust identification systems are anchored on a comprehensive digital identity law that stipulates the purpose of the digital ID system, among other issues relating to its operation.

The element of legislative mandate under the rule of law test of the CIS evaluation framework requires that countries intending to implement digital identity systems must ensure that there is a digital ID law that will govern the use and operation of the digital ID system. Further, the state is obliged to ensure public participation before implementing a digital ID system.

In essence, the digital ID project should be founded on a validly enacted law which should, among other things, outline the legitimate aim of the digital ID, specify the actors of the system; outline the grievance redress mechanism against the administrators of the system, and provide for an oversight mechanism to address any cases of misuse of the digital ID.

Indeed, World Bank (2017) contends that an ideal digital ID law should reflect the purpose of an ID system, the data it must collect, and the ends to which it is established to meet. Additionally, the digital ID law will outline mechanisms for monitoring and ensuring compliance with the purpose limitations (World Bank, 2017).

For example, Article 15 of the Nigerian National Identity Management Commission Act 2007 sets out specific objectives of the national identity database. These include providing a medium for the identification, verification, and authentication of citizens, among others (World Bank, 2017).

Additionally, the digital identity law also specifies the body that is mandated with the implementation of the digital identity system. For example, in Austria, the Source PIN register Authority regulation enacted in 2009 sets out the responsibilities of the Authority which is responsible for citizen IDs and cooperation with service providers (World Bank, 2018).

Ironically, some countries have attempted to implement digital identity systems without an enabling digital ID law in place. This has resulted in the ID systems facing litigation headwinds and a lack of trust in

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

the system by the citizens. For example, India's Aadhaar system was initially introduced before an enabling law had been enacted. This led to legal challenges particularly on the constitutionality of the system, with the case ending up in the Indian Supreme Court (World Bank, 2018).

Beyond enacting a digital identity system law, it is equally important to appreciate that there are other laws that are closely related to the aspect of digital identification. A case in point is the law on the registration of persons.

Notably, the process of civil registration entails the collection of citizens' personal attributes which can be used for identification purposes. As such, civil registration contributes to the development of identification systems. As a matter of fact, the establishment and implementation of foundational identity systems is influenced by the existing civil registration system of a particular jurisdiction.

Further, the management of civil registration systems raises similar legal and regulatory issues as those of foundational identification systems (World Bank, 2017). As such, seamless implementation of a digital identity system requires that the law governing the establishment and operation of the identity system be aligned with the law relating to registration of persons.

In Kenya's context, the concern of this paper is to establish if the law relating to the registrations of persons has been amended to reflect the establishment and operation of the NIIM system.

2.3 Existence of laws governing the collection, storage, and processing of personal identifiable information (Data Protection Law)

As mentioned earlier, identity systems collect and retain a lot of personally identifiable information relating to citizens. This data-centric nature of digital identity systems predisposes their users to risks associated with data breaches. These risks include identity theft and discrimination, among other ills.

The rights-based test of the CIS evaluation framework requires that countries implementing digital identity systems have a law that addresses the aspects of necessity and proportionality, data minimization, access control, exclusion, and mandatory use. Notably, all these aspects relate to the collection, storage, and processing of personal data, and are therefore addressed by enacting a data protection law. In essence, a data protection law stipulates data protection principles that will guide the management of personal data within the ID system.

For example, on the aspect of data minimization, the data protection law should outline mechanisms that ensure that the digital identity system adheres to the principle of data minimization. That is, it should propose privacy design features that ensure the collection of personal data is limited to only what is necessary to serve the purpose of the digital ID system.

In terms of the enactment of the Data Protection law, internationally, according to the United Nations Conference on Trade and Development (UNCTAD), out of the 194 countries in the world, at least 132 have some sort of regulation on the acquisition, use, and safety of data (United Nations Conference on Trade and Development (UNCTAD), 2016). At the continental level, in Africa, extant literature reviewed revealed that 25 out of 55 countries have passed data protection laws (Kadengye and Owoko, 2019).

According to Banisar and Davies (1999), there are two major models of data privacy protection. The first model comprises a country adopting an omnibus or general data protection law that seeks to safeguard all categories of personal data. This is the preferred model for most European countries. It provides for a public official, an ombudsman or privacy commissioner, to enforce the provisions of the data protection law.

In contrast, some countries, such as the United States, have avoided a general data protection law in favor of sectoral laws governing specific categories of information such as police files and consumer credit records. However, the drawback of this model is that it requires legislations to be introduced for each new technology and thus may delay protections (Banisar and Davies, 1999, p. 13). Further, the sectoral approach means enacting multiple legislations which may be time-consuming, thus delaying the implementation of the digital ID system.

In many African countries, having a general law that covers all categories of personal data would be more appropriate. This would ensure leverage of the limited resources since lawmaking entails a

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

prolonged process that involves drafting, seeking public views, and presentation to parliament for debate and approval.

In the Kenyan context, this paper is concerned with establishing the model of data privacy protection adopted to facilitate the establishment and implementation of the NIIM system.

There is also the aspect of ensuring that the provisions of the data protection law are reflected in the design of the identity system. Indeed, the European Union's GDPR introduced new obligations requiring organizations to adhere to the principle of privacy-by-design so that data protection issues are considered at the outset of the design phase of an identity system (World Bank, 2017).

The rights-based test of the CIS framework that underpins this study requires countries implementing digital identity systems to adhere to the principle of data minimization. Notably, one way of achieving data minimization within a digital identity system is by embedding features that allow the system to collect as minimal data as possible.

This means developing a privacy-preserving ID system by incorporating data protection principles in the architecture of the identity system. For example, in India, the Aadhaar system has inbuilt privacy-enhancing features that ensure that the Aadhaar number generated by the system does not disclose the identity of the user. This privacy-by-design feature is consistent with the principle of data minimization that is pronounced in the Aadhaar's system enabling legislation, the Aadhaar Act 2016 (World Bank, 2018).

In the Kenyan context, the concern of this paper is whether there are any privacy-by-design features pronounced in Kenya's Data Protection law and if so, how these features are incorporated in the design of the NIIM system to achieve data minimization.

There is also the question of accountability. Specifically, the rule of law test requires a digital identity system law to provide a mechanism for holding both private and public users of the digital ID accountable. In essence, the law should ensure the effective enforcement of the various provisions relating to data protection. Indeed, under the European Union's GDPR, member states are expected to have an oversight authority to monitor the enforcement and implementation of the law (European Union (EU), 2016).

Extant literature reviewed revealed that different countries have adopted different models of oversight mechanisms depending on the governance structure. For instance, some countries have two distinct agencies overseeing the implementation of the Data Protection Act and the Freedom of Information Act. In contrast, some countries have a single agency overseeing the implementation of both Acts.

For example, in the UK, all laws relating to access to information and data protection are coordinated by a single authority. In particular, the UK information commissioner is the point of contact for public authorities and the public for both the Data Protection Act and the Freedom of Information Act (Amos and Holsen, 2004). Further, the Access to Information clearing house is charged with ensuring consistent application of the Data Protection Act, the FOIA. and the environmental regulations (Dokeniya, 2013, p. 18).

In the Kenyan context, the paper is concerned with establishing whether the Data Protection Act 2019 provides for an oversight mechanism to oversee the deployment of digital ID systems such as NIIMs.

2.4 Law governing access to Information—Data Protection law and the Freedom/ Access to Information legislation

The rights-based test of the CIS framework that underpins this study requires that countries implementing digital identity management systems have a law that governs access to citizens' information by the state as well as private actors. Notably, in many jurisdictions, access to personal information is governed by the data protection legislation.

However, it is important to appreciate that the Data Protection law does not operate in a vacuum but interfaces with other legislations governing access to information. In particular, for a Data Protection law to be implemented effectively, its provisions must be consistent with the laws relating to freedom/access to information.

In essence, the provisions of the freedom/access to information legislation should complement certain aspects of the data protection law, particularly in relation to privacy of personal data. For example, in the UK, the Freedom of Information (FOI) Act 2000 is harmonized with the UK Data Protection Act of 1998.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Specifically, the UK FOI Act 2000 clearly states that requests for information about third parties are covered by the Freedom of Information Act 2000, but data protection principles apply (Amos and Holsen, 2004).

In contrast, an analysis of literature revealed that in countries where the data protection law is not harmonized with the freedom/access to information legislation, there is confusion among public officials leading them to unjustifiably refuse requests for information. For example, in New Zealand, citizens complained of being unjustifiably denied access to information on account of the Privacy Act (Rodrigues, 2008).

While most countries have distinct legislations for data protection and access to information, it is worth noting that in some countries, such as Canada and Ireland, the aspects of data protection and freedom of information are integrated into a single legislation (World Bank, 2016 ID4D Country Diagnostic, Kenya).

In the Kenyan context, this paper is concerned with establishing the extent to which the Data Protection Act 2019 in Kenya is harmonized with the Freedom/Access to Information Act 2016 to fulfil the access control element of the rights-based test and, by extension, create a conducive environment for the operation of the NIIM system.

2.5 Existence of policy and regulations to operationalize both the Digital ID law and the Data Protection law

The elements articulated in both the rule of law test and the rights-based test cannot be actualized by only enacting the set of laws mentioned above. As such, it is important to appreciate that laws are operationalized by enacting regulations and a policy framework that elaborates the methodology of enforcing the provisions set out in the law.

In view of the above, for a digital identity law to operate effectively, it has to be supplemented by regulations specifying how the various components of the identity system will operate.

Similarly, there is a need for data protection regulations to operationalize the data protection legislation. Indeed, some of the legal requirements of the rights-based test such as the aspect of data minimization are operationalized through policy tools that provide guidelines to data controllers on adhering to the data minimization principle.

Further, effective enforcement of the digital identity law requires the formulation of a policy that outlines the various guidelines to be followed in the implementation of the digital ID law The guidelines will outline among other aspects the roles and responsibilities of various actors in the operation of the digital identity system. Similarly, there is a need to formulate a data protection policy that spells out the mechanism for actualizing the implementation of the Data Protection Act.

In the Kenyan context, the concern of this study was to establish whether Kenya's digital ID law and the Data Protection Act 2019 were complemented by policy and regulations to facilitate their operationalization.

2.6 Existence of a law governing the digital economy

Digital identity systems do not operate in isolation; rather they are part of a broader digital economy. Advances in information and communication technologies in the last decade have led to increased global internet connectivity. This has resulted in a digital economy where essential services are offered through digital technologies. In essence, in a digital economy, consumers once connected to the Internet can access goods and services from the digital market from any part of the world (Gillani et al., 2022, p. 1). Ordinarily, financial transactions are founded on trust, and electronic transactions are no exception. As such, digital IDs are necessary to ensure that electronic transactions in the digital market are secure and reliable. Through a digital ID, sellers can verify and authenticate the identity of the buyers in the digital market.

Granted, the digital economy has revolutionized access to goods and services. However, it is also fraught with challenges. Key among them is its susceptibility to cybercrimes such as identity theft and electronic fraud. To address these ills, there is need for an overarching legislation that covers the broader digital economy to guarantee trusted communication.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Internationally, in 2001, the Council of Europe formulated an international treaty (Budapest Convention) that came into effect in 2004. The treaty identifies crimes committed on the Internet and other computer networks such as infringement on copyright, child pornography, and violations of network security (Council of Europe, 2004). As such, countries are expected to demonstrate their commitment to combat cybercrime and internet fraud by ratifying or aligning their domestic laws with the Budapest Convention.

The Budapest Convention is cognizant of the fact that electronic systems, including digital identity systems, are susceptible to manipulation, and as such, there is a need to have a law addressing the criminal conduct directed against the confidentiality, integrity, and availability of computer systems and networks as well as data processed on them (World Bank, 2017).

Amartya Sen's capability approach, that partly underpins this study, advocates for the removal of constraints that may hinder citizens from living a meaningful life (Sen, 1999). In the context of this study, the challenges facing the digital economy such as identity theft and electronic fraud, among others, undermine the ability of citizens to enjoy their fundamental rights and freedoms within the digital space. In this regard, having a law on the digital economy will ensure that there is a set of rules and mechanisms for dealing with cybercrimes, thereby enabling citizens to fully achieve their capabilities in the digital space.

The concern of this study is to establish the existence of an overarching law governing the digital economy in Kenya.

2.7 Fundamental Rights and Duties

Any country across the world that is founded on democratic ideals is expected to guarantee certain rights to its citizens. These are termed as fundamental rights which every citizen is entitled to and are outlined in the Bill of Rights. In the same vein, these fundamental rights oblige citizens to perform certain duties toward other individuals, society, nation, or humanity.

In essence, any legal system has certain social and ethical principles that outline what is allowed of people (freedom) and what is owed to people (duties). These rights and duties facilitate the existence and development of individuals in a society (India, 1950).

Democratic societies safeguard fundamental rights by enshrining them in the Constitution, thereby guaranteeing them. Further, fundamental rights are justiciable, that is, they can be enforced through the courts (India, 1950). This means that in the event of a violation of any of these rights, an individual can petition the court seeking their protection.

These fundamental rights are universal and outlined in the Bill of Rights. They include the right to life, right to equality, freedom from discrimination, freedom of conscience, religion, belief, and opinion, among others (India, 1950; Kenya, 2010).

As such, governments across the world should always endeavor to safeguard fundamental rights. This means that any law enacted by the state must be consistent to the fundamental rights of the citizens. In view of this, the enactment and implementation of the digital ID law must be consistent with citizens' fundamental rights.

In particular, the rights-based test of the CIS evaluation framework that underpins this study requires countries that are implementing digital identity systems to ensure that those systems do not perpetuate exclusion. In this case, the use of the digital ID system should not occasion a situation where a certain category of citizens is excluded or discriminated against from accessing certain government services.

Similarly, Amartya's Sen's capability approach, that partly underpins this study, requires that human beings be afforded an environment that enables them to fully achieve their capabilities. In this regard, granting citizens their fundamental rights and freedoms ensures that they fulfil their capabilities (Sen, 1999).

At the international level, governments are expected to demonstrate respect for their citizens' fundamental freedoms by ratifying international instruments such as the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD).

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

In December 1965, the UN General Assembly adopted Resolution 2106, which established the ICERD. In essence, this convention seeks to adopt measures to eliminate racial discrimination in all its forms and manifestations (United Nations General Assembly (UNGA), 1965).

This convention is relevant to the aspect of digital identity systems, especially given that most digital ID systems are programmed in Western countries and may have an embedded bias that may not be compatible with African contexts. In this regard, it is important for countries intending to implement digital ID systems to ratify this convention to ensure that they implement digital ID systems that do not discriminate against citizens based on their race or color.

3. Research Methodology

The study adopted a qualitative research approach and case study research design where the NIIM system was the main case. The case study design is appropriate for this study since the assessment of the legal and regulatory framework is context specific, the context being the NIIM system. Yin (2009) describes a case study as an empirical enquiry that investigates a contemporary problem within its real-life context. As such, use of the case study design will provide insights into the set of laws that would ensure adherence to all the elements of the rule of law and rights-based test as well as fundamental rights and freedoms in the context of the NIIM system.

Data was collected through content analysis, document review, and interviews. First, the researcher content analyzed the elements outlined in the CIS evaluation framework for digital identity systems. The analysis focused on the rule of law and rights-based test elements of the framework. For each of the elements, the researcher was able to identify specific texts that gave an indication of the relevant legislation that would ensure that the test in question was achieved. This analysis enabled the researcher to answer research question #1 of the study.

Secondly, the researcher reviewed literature (laws and policy documents) on digital identity systems, the NIIM system, and the legal and policy framework relating to privacy and data protection internationally, in Africa and Kenya. This review was useful in answering research question #2 of the study, which focused on establishing which of the identified sets of laws and policy tools were present in the implementation of the NIIM system in Kenya. Further, this enabled the researcher to identify other laws that may be crucial to successful digital ID implementation (for instance, the law on the digital economy).

Subsequently, semi-structured interviews were conducted on two purposively sampled respondents. First was the legal officer in the Ministry of Interior and Coordination of National Government, which is the ministry tasked with the implementation of the NIIM system. The legal officer provided information on the efforts made by the ministry to ensure that the NIIM system adhered to international rights and data protection norms.

Secondly, the researcher interviewed a representative at the Office of the Data Protection Commissioner (ODPC), who is charged with the responsibility of overseeing the implementation of Kenya's Data Protection Act 2019. The officer was able to shed light on the measures that the Commission had taken to ensure that the NIIM system operated within the requirements of the Data Protection Act 2019.

As such, information obtained from the interviews was used to corroborate the data collected through the literature review. Further, the literature review was useful in answering research question # 3 of the study, which sought to make recommendations on the measures that can be undertaken to ensure that the NIIM systems adhere to international rights and data protection norms.

4. Findings

The presentation of the findings of this study will be based on the research questions that were outlined earlier.

An analysis of the elements that constitute the CIS evaluation framework for digital identity systems enabled the researcher to answer research question # 1 of the study. The various set of laws that are key to implementing a digital identity system that complies with international rights and data protection norms are listed in Table 1 of Section 1.4 and informed the review of literature for this study.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

On the other hand, the findings for research question #2 are discussed below and are organized based on the set of laws identified in the first research question.

4.1 Constitutional provision guaranteeing privacy—Right to Privacy

The study revealed that Kenya's constitution explicitly provides for the right to privacy. Specifically, Article 31 of the Constitution of Kenya (2010) recognizes and guarantees citizens the right to privacy. In particular, Article 31 of the Constitution of Kenya (2010) provides the following:

> Every person has the right to privacy, which includes the right not to have-
>
> a) their person, home or property searched;
> b) their possessions seized;
> c) information relating to their family or private affairs unnecessarily required or revealed; or
> d) the privacy of their communications infringed (Kenya, 2010).

Constitutional guarantee on privacy is important as it lays the legal foundation for the enactment and implementation of laws relating to privacy and protection of personal data. Indeed, in Kenya's case, Article 31 of the Constitution of Kenya (2010) laid the foundation for the enactment of the Data Protection Act in 2019.

In terms of the impact on the implementation of the NIIM system, the presence of a constitutional guarantee on the right to privacy means that the system is being implemented in an environment where the privacy of citizens is well safeguarded. This engenders trust in the system among the citizenry by providing an assurance that their personal data is safe.

Additionally, the study revealed that Kenya adheres to several international legal instruments aimed at enhancing privacy and protection of personal data. Specifically, Kenya has ratified international instruments relating to the right to privacy, thus committing itself to fulfilling the requirements stipulated in these instruments. These include the following:

- Universal Declaration of Human Rights (UDHR) and specifically Article 19;
- International Convention on Civil and Political Rights (ICCPR);
- International Convention on the Elimination of All Forms of Racial Discrimination (IECRD).

There are also regional treaties that seek to promote data protection and privacy. For instance, in Africa, the study revealed that only 14 out of 55 African Union (AU) member states have ratified the African Union Convention on Cyber Security and Data Protection (Malabo Convention). Indeed, enforcement of the African Union Convention on data privacy has been undermined by the delay by some African Union member states to ratify the convention. Notably, some scholars have argued that this delay is attributed to the inclusion of the aspect of cybersecurity as part of the convention as well as lack of resources by the African Union to lobby its members to ratify (Greenleaf and Bertil, 2020).

Regrettably, Kenya is among the countries that are yet to ratify the African Union Convention on Cyber Security and Data Protection (Malabo Convention). The delay in ratification of the Malabo Convention by Kenya sends the wrong signal as it puts into doubt the country's commitment toward complying with regional standards on cybersecurity and data protection.

4.2. An enabling law governing the establishment and operation of the digital ID system

As mentioned earlier, the rule of law test of the CIS evaluation framework that underpins this study demands that a digital identity system should be founded on an enabling law governing its establishment and operation. Specifically, a digital identity system that adheres to data protection norms should draw its legitimacy from an elaborate stand-alone Act that outlines the legitimate aim of the digital identity system and outlines its functions and purpose.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

However, in Kenya's case, NIIMS was not established through a stand-alone Act of parliament. Instead, the government introduced an omnibus bill seeking to amend provisions of the Registration of Persons Act Cap 107. Section 9A (1) of the Act establishes the NIIMS (Mutung'u and Rutenberg, 2020). The fact that the NIIM system is anchored on an executive order instead of a stand-alone digital ID law means that the system does not meet the requirements of the CIS framework rule of law test, thereby undermining its legitimacy.

Further, this narrow legislative approach adopted in establishing the system undermined public participation and scrutiny of the proposed amendments. Indeed, this anomaly was highlighted by civil society organizations who noted that regulations cannot be used to regulate and create substantive systems which have implications on the effective and proper functioning of government, and which directly affect an individual's identity (Article 19 Eastern Africa, 2020).

Further, the digital ID law is expected to specify the purpose of the digital ID. Indeed, according to the World Bank (2017), the law establishing the digital ID system should, among other aspects, outline the purposes for which data will be collected and used. This is meant to adhere to the rights-based test that requires that the data collected be proportionate to the purpose of the ID system. Regrettably, in Kenya's case, the amendment to the Registration of Persons Act, on which NIIMS is anchored, is not elaborate on the contemplated purpose of the data collected by the system. This has prompted some civil society activists to describe the NIIM system as "purpose-free" (Mutung'u and Rutenberg, 2020).

As such, the legal basis of the NIIM system in Kenya was through an executive order no.1 of 2018. Specifically, the president directed the development of NIIMs to create and manage a central master population database, to be the "single source of truth" on all Kenyan citizens and foreign nationals residing in Kenya (Mutung'u and Rutenberg, 2020).

Section 9A (1) of the Act establishes the NIIMS. The Registration of Persons Act cap 107 section 14 (1) (k) (1) and (m) prohibits anyone from publishing or communicating any data that is acquired in the course of employment other than for allowed official purposes. It also prohibits any third party from possessing any personal data derived from registration processes (Kenya, 1947).

Beyond enacting a digital ID enabling law, it is also important to align it to the legislation relating to the registration of persons. This action stems from the fact that the digital identity system is directly linked to the registration of persons. Indeed, World Bank (2017) noted that civil registries record a lot of personal attributes which are sometimes used for identification purposes. As such, foundational identity systems are founded on existing civil registration systems. Notably, for a digital ID system to function well, it requires the mandate for civil registration and, at some point, it should provide citizens with incentives for voluntary registration (Asian Development Bank, 2016).

In Kenya's case, the digital identity system was established through an amendment to the primary identity law, the Registrations of Persons Act. The amendment expanded the range of data collected during the registration of persons and created NIIMS as a central link to government services and some private services (Mutung'u and Rutenberg, 2020).

According to Section 9A (2)(a) and (b) of the amended Act, NIIMS was introduced to

- create, manage, maintain, and operate a national population register as a single source of personal information of all Kenyan citizens and registered foreigners resident in Kenya;
- assign a unique national identification number to every person registered in the register (Kenya, 2018).

As such, in Kenya's case, there is no stand-alone digit ID law, and thus no harmonization with the Registration of Persons Act. Instead, the government amended provisions of the Registration of Persons Act as outlined above. The absence of a stand-alone digital ID law means that the establishment and operation of the NIIM system does fully meet the rule of law test of the CIS evaluation framework.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

4.3. Law governing the collection, storage, and processing of personal information (Data Protection Law)

The data-centric nature of digital identity systems means that they collect large volumes of personally identifiable information belonging to citizens. Having a digital identity system that is in the form of a centralized database exposes it to data breaches such as identity theft, mass surveillance, and other privacy concerns.

The rights-based test of the CIS evaluation framework identifies the principles of necessity and proportionate as well as data minimization as important elements that should be embedded in a digital identity system for it to be deemed to be complying with data protection norms.

In this case, a digital identity system that is founded on the principle of necessity and proportion will only collect personal data that is necessary for the fulfilment of the legitimate aim of the system. Further, the data collected is proportional to the use and purpose of the digital ID system.

In Kenya's context, the government enacted the Data Protection Law 2019 which outlines data protection principles that all data-centric systems implemented within Kenyan borders are expected to adhere to. Notably, Kenya's Data Protection Act 2019 adopts the form and substance of the European Union's GDPR and therefore, by extension, embodies the OECD principles of collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.

On the question of privacy-by-design, the rights-based system of the CIS evaluation framework requires digital identity systems to collect personal data that is adequate, relevant, and limited to what is necessary in relation to the purpose of the digital ID. This means protecting the privacy of citizens through embedding the principle of data minimization in the design of the digital ID.

In Kenya's case, the Data Protection Act 2019 does not stipulate privacy design features that are supposed to be adhered to when designing data-centric systems. Indeed, there are no specific privacy-by-design features embedded in the NIIM system.

In sum, the NIIM system does not adhere to some of the data protection principles. This is problematic as it means that its implementation may undermine citizens' right to privacy by, for instance, collecting more personal data than is necessary for the fulfilment of its purpose.

4.3.1. Law establishing an institutional body to oversee the enforcement of the legal provisions on digital ID and Data Protection

The rule of law test of the CIS evaluation framework that underpins this study requires countries implementing digital identity systems to put into place an accountability mechanism. In particular, the accountability element in the rule of law test assesses whether a country has established mechanisms for holding the actors and users (public and private) of the digital ID system accountable.

One way of holding users and actors of the digital ID system accountable is establishing an independent institution to undertake oversight duties. Indeed, successful digital identity systems require an environment with an institutional oversight mechanism. This means the existence of an institutional body that ensures effective enforcement of the data protection principles. As such, the oversight body ensures that identity system providers comply with the laid-out data protection principles. Notably, an institutional oversight mechanism can only effectively discharge its mandate if it is anchored in law.

In Kenya's case, the NIIMS implementing body is the executive through the Ministry of Interior and Coordination of National Government with technical assistance provided by the Ministry of Information and Communication Technology (MoICT). Accordingly, any complaints regarding the NIIM system have to be directed to the executive. This has undermined oversight of NIIMS operation as it would mean the executive holding itself accountable.

However, an interview with the legal officer at the Ministry of Interior and Coordination of Government expressed the willingness of the ministry to be held accountable over the operations of the NIIM system. He explained,

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

> "We are implementing the system within the confines of the Data Protection Act 2019; indeed, we have been engaging the ODPC to ensure that the system fulfils international data protection requirements" (Kihara, 2021).

Indeed, the only oversight initiative in Kenya's digital identity landscape is the provision for the establishment of the ODPC under the Data Protection Law 2019. Specifically. Part 11, Section 8 (a) of the Data Protection Act 2019 empowers the Commission to oversee the implementation and enforcement of the Act (Kenya, 2019a). As such, it is evident that Kenya has fulfilled this requirement of the rule of law test.

In terms of the independence of the oversight institution, World Bank (2017) noted the oversight authority has to be independent if it is to undertake its oversight roles effectively. Some of the structural factors that can be used to measure independence include composition of the oversight body, the method of appointment of members, power and time frame of exercising oversight functions, allocation of sufficient resources, and ability to make decisions without interference (World Bank, 2017).

In Kenya's case, ideally, the ODPC is meant to be an independent commission; however, this is not the case. Firstly, although the Data Protection Commissioner was appointed by the president on the recommendation of the National Assembly, the process was highly influenced by the executive. Secondly, its funding and other administrative operations are dependent on its parent Ministry of Information and Communication. This has undermined its oversight ability.

4.4. Law governing access to Information—Data Protection law and the Freedom/ Access to Information legislation

The rights-based test of the of the CIS evaluation framework also obliges countries implementing digital identity systems to adhere to data protection norms by having elaborate laws that govern access to information by state and private actors. In this case, the framework stipulates that the country needs to enact a data protection law as well as the freedom/access to information law.

Further, an analysis of extant literature revealed that digital identity systems are successful in an environment where the data protection law is harmonized with the law relating to freedom/access to information.

As such, this study sought to establish whether Kenya's Data Protection Law 2019 was harmonized with the Access to Information Act 2016 to facilitate the seamless operation of the NIIM system.

The study revealed that the Access to Information Act (ATI) 2016 that governs access to information held by public entities by citizens is to a large extent harmonized with the Data Protection Law 2019. Specifically, the ATI Act 2016 is relevant to the privacy of identity systems, in that Section 6 (1) of the Act provides for limitation of the right to information thus safeguarding the privacy of personal data. Subsection 1 (d) prohibits disclosure of information that is likely to "involve the unwarranted invasion of the privacy of an individual." Further, Section 28 of the Act provides for a heavy fine of Kenya shillings 1 million or an imprisonment as defined in Section 6 (Kenya, 2016).

As mentioned earlier, the access control element under the rights-based test normally relates to how access to personal data by the state and private entities is regulated. Typically, the aspect of access to information is governed by the freedom/access to information law as well as the Data Protection Act. Regulating access to information is key it ensures citizens' privacy rights are protected. Similarly, having a law that facilitates citizens' access to information is important as it fosters good governance and accountability.

Notably, the management of information in Kenya is also influenced by the Public Archives and Documentation Service Act, Chapter 19 of the Laws of Kenya. Essentially, all records generated by public entities during the transaction of government business are regarded as public records and their management should be guided by this Act. In terms of digital identity, the provisions of Kenya's Public Archives and Documentation Service Act are consistent with the provisions of the Data Protection Act 2019 as well as the Freedom Right to Information Act 2016.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

While Kenya has made great strides toward facilitating access to information by citizens, it is also important to note that the right/freedom to information is not absolute. In this regard, there are certain categories of information whose access is restricted; for instance, information relating to national security matters. These restrictions are outlined in various acts such as the Official Secrets Act, Chapter 187 1970, National Intelligence Service Act 2012, Evidence Act 2012, and Security Laws (Amendment) Act of 2014. In particular, the Security Laws Amendment Act 2014 undermines access to information by inhibiting media freedom. Similarly, the Act compromises citizens' privacy by giving the intelligence agencies surveillance powers.

In Kenya's case, it is evident that the NIIM system is operating in an environment where the access control element of the CIS evaluation framework has been fulfilled by access to information law as well as a data protection act whose provisions are harmonized.

4.5. Policy and regulations to operationalize the Digital Identity system law and the Data Protection Act

A digital identity law can only operate effectively if supplemented by regulations specifying how the various components of the ID system will operate. Further, there is a need for a policy framework that outlines the various guidelines to be followed in the implementation of the digital ID law as well as the roles and responsibilities of the various actors.

In the Kenyan context, the absence of a stand-alone digital identity law means the NIIM system is anchored on Huduma-Namba regulations. Human rights organizations such as Article 19 have criticized this move by noting that regulations cannot be used to regulate and create substantive systems which have implications on the effective and proper functioning of government, and which directly affect an individual's identity (Article 19 Eastern Africa, 2020). Whilst it is commendable to have regulations that elaborate the operations of the NIIM system, they should not be the basis upon which the system is founded.

On the question of policy, the government has formulated a data protection policy to operationalize the Data Protection Act 2019. Further, a staff at the ODPC intimated that the Data Protection Commissioner has already formulated data protection regulations which are currently being debated in parliament.

"*We have already drafted the data protection regulations, as well as received views from the public in adherence to the public participation requirement. We have forwarded the draft regulations to parliament for consideration*" (Nyambura, 2021).

The upshot is that the existence of both the data protection regulations as well as the data protection policy means that there is an adequate policy framework to operationalize and ensure effective enforcement of the Data Protection Act 2019.

4.6. Law regulating the digital economy

Digital identity systems are an integral element of information communication and technologies (ICTs), and thus the need to have policies that aim to promote the modern and effective use of ICTs in the long term (Atick et al., 2014). In this respect, a comprehensive legal and regulatory framework for digital ID establishment and implementation should be broad enough to address legal and policy issues relating to the wider digital economy.

In essence, policies that are geared toward providing more connectivity and online access, improved digital education and training, as well as responsible use of the Internet will go a long way in promoting digital identity systems development (Atick et al., 2014). This is consistent with Sen's capability approach, which advocates for an environment where citizens' capabilities are nurtured by removing constraints that may undermine their freedoms (Sen, 1999).

In Kenya, the government has made efforts to enact laws regulating the digital economy. For example, Kenya enacted a Computer Misuse and Cybercrimes Act in 2018. The Act seeks to regulate the country's cyberspace and largely adopts the form and substance of the Budapest Convention on cybercrime. As

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

such, the Act is aligned with international standards on cybercrime prevention. Further, the Act provides penalties for the misuse of computer systems, such as NIIMS (Kenya, 2018).

Likewise, Part VIA of the Kenya Information Communication Act Amended 2019 provides that the cabinet secretary can declare a system as a "protected system" for purposes of safeguarding the system from unauthorized access. Specifically, section 83Q provides that the cabinet secretary can gazette "protected systems," such as NIIMS. Further, the section provides a fine not exceeding Kenya shillings 10 million or imprisonment for a term of 10 years or both to anyone who secures unauthorized access or attempts to secure unauthorized access to a protected system (Kenya, 2019b).

Notably, there are also other laws that seek to regulate citizens' conduct in the digital space. These include provisions within Kenya's penal code, and the Consumer Protection Act 2012.

In view of the above, arguably, Kenya has an adequate set of laws governing the digital economy. The provisions within the Computer Misuse and Cybercrimes Act 2018 and the amended Kenya Information Communication Act 2019, as well as broad provisions in the penal code and the Consumer Protection Act 2012, provide adequate mechanisms to address any cybercrimes that may arise during the implementation of the NIIM system.

4.7. Fundamental Rights and Duties

The rights-based test of the CIS evaluation framework that underpins this study provides that countries implementing digital ID systems should ensure that the adoption of digital ID systems does not exclude citizens or restrict their access to benefits and services.

Similarly, Amartya Sen's capability approach provides that in policy design, the focus should always be on giving people the freedom to do what they are capable of doing and removing constraints that undermine their capabilities (Sen, 1999). This is particularly relevant for this study as it seeks to ensure that countries do not deploy identity systems that undermine the fundamental rights of their citizens and prevent them from achieving their capabilities.

In Kenya's case, chapter 4 of the constitution of Kenya (2010) provides for the Bill of Rights that guarantees specific fundamental rights and freedoms. In particular, Part Two of the Chapter provides for the following fundamental rights and freedoms:

- The right to life;
- Right to equality and freedom from discrimination;
- Right to freedom and security of the person;
- The prohibition of slavery, servitude and forced labour and
- Freedom of conscience, religion, belief, and opinion (Kenya, 2010).

The right to equality and freedom from discrimination is particularly relevant for this study as it implies that the government is obliged to ensure that digital systems such as the NIIM system do not perpetuate discrimination or exclude citizens from accessing services. In view of the above, it is evident that the NIIM system in Kenya is being implemented in an environment where citizen's fundamental rights and freedoms are clearly articulated and enshrined in the constitution.

5. Discussion of the Results

This study set out to determine the set of laws and policy framework (legal and regulatory framework) that are necessary for the establishment and implementation of a digital identity system. The CIS framework for assessing digital identity systems was used as an analytical lens to illuminate the principles that digital identity systems require to fulfil international data protection norms. The principles included the rule of law test and the rights-based test. The text of the elements that constitute these principles were context analyzed to identify the set of laws and policy that constitute a supportive legal and regulatory framework for digital ID implementation.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

Table 1 outlines the set of laws identified after analyzing the elements of the rule of law and rights-based test of the CIS digital identity system evaluation framework.

The set of laws and policy enumerated in the above table answer research question 1 of this study, which set out to establish the set of laws and policy relevant for establishing and implementing a digital identity system.

Indeed, these results reinforce the argument by privacy advocates across the world, who contend that the establishment and implementation of a digital identity system should be preceded by a comprehensive legal assessment. This assessment should address the following areas: legal authority of the digital ID system, protection of people's rights, and establishing whether the existing policies promote the implementation of digital ID (Atick et al., 2014). Evidently, the set of laws outlined above address all the three areas.

Having identified the set of laws relevant for digital ID operation, research # 2 set out to find out if these laws were present in the establishment and implementation of the NIIM system in Kenya.

It emerged that, to some extent, the establishment and operation of the NIIM system in Kenya adhere to the requirements of the rule of law test and the right based tests. However, there are specific areas that require improvement.

In terms of the system being anchored on a digital ID law, Kenya's NIIM system fell short of this requirement since it was anchored on an executive order. This went against the requirements of the CIS framework that underpins this study, which provides that a digital identity system that adheres to data protection norms should draw its legitimacy from an elaborate stand-alone Act that outlines the legitimate aim of the digital identity system and outlines its functions and purpose. As a result of this anomaly, the legitimacy of the NIIM system has, on a number of occasions, been contested in court. Such a scenario is problematic in that it erodes public confidence in the system by engendering mistrust among the users of the system. This scenario was replicated in India where the Aadhaar system was initially introduced before an enabling law had been enacted. This led to legal challenges particularly on the constitutionality of the system, with the case ending up in the Indian Supreme Court (World Bank, 2018).

Another law that is key to digital ID establishment and operation is the data protection law. In Kenya's case it emerged that Data Protection Act 2019 is already in place. Additionally, Kenya's Data Protection law is aligned with EU GDPR, and thus it embodies all the data protection principles. This means that ideally the NIIM system should largely fulfil the requirements of the rights-based test of the CIS evaluation framework. However, it emerged that there are some elements of the rights-based test that the NIIM system is yet to fulfil. For example, the data minimization principle requires that systems embed privacy-by-design features that limit the amount of personal data collected to only what is adequate. It was established that NIIM lacks privacy-by-design features, and as a result, enforcement of the data minimization principle is undermined. This means that there is a possibility of the system collecting more personal data from citizens than is necessary. Kenya should endeavor to learn from India where the Aadhaar system has inbuilt privacy-enhancing features that ensure that the Aadhaar number generated by the system does not disclose the identity of the user. This privacy-by-design feature is consistent with the principle of data minimization that is pronounced in the Aadhaar's system enabling legislation, the Aadhaar Act 2016 (World Bank, 2018).

6. Conclusion

Overall, the study has demonstrated that the effective establishment and operation of a digital ID system hinges on the existence of a supportive legal and regulatory framework that safeguards users' personal data, thereby engendering their trust in the system. In this regard, the study has advanced scholarship on digital identity by enumerating the set of laws and policy framework that should be in place for a digital identity system to function effectively. Enacting this set of laws will ensure the seamless establishment and implementation of digital ID systems. Additionally, the existence of these laws and policy framework ensures that the digital ID system in any jurisdiction is robust, inclusive, secure, and trusted.

https://doi.org/10.1017/dap.2023.36 Published online by Cambridge University Press

In the Kenyan context, the study has established that the NIIM system is to a large extent supported by the set of laws and policy framework outlined in this study. However, there are still some aspects of Kenya's digital identity legal and regulatory landscape that need to be streamlined. For example, first, the robustness of the NIIMs system can be enhanced by anchoring it on a stand-alone digital identity law. Secondly, the Data Protection Act 2019 needs to be amended to include provisions on privacy-by-design features that should be embedded on the NIIMs as well as other systems that intend to collect and process personal data from Kenyan citizens. This will go a long way in adhering to the international data protection principle of data minimization.

Lastly, the study also provides a glimpse into areas that may require further research. For instance, the study has revealed that Kenya and many other countries have a pluralist legal system. Accordingly, there is a need to undertake a deeper theoretical analysis of the CIS framework to understand its applicability in pluralist legal system contexts.

Funding statement. This work received no specific grant from any funding agency, commercial, or not for profit sectors

Competing interest. The author declares none.

Author contribution. This work was conceptualized and created solely by the author.

Data availability statement. The data that support the findings of this study are available from the references provided. No restrictions exist for the availability of these data.

References

Amos J and Holsen S (2004) *A Practical Guide to the UK Freedom of Information Act 2000. (No. 115). The Constitutional Unit*. London: University College London.

Article 19 Eastern Africa (2020) Joint Memorandum, Public participation on the Registration of Persons (National Integrated Identity Management System) Regulations, 2020. Available at https://www.article19.org/wp-content/uploads/2020/03/ARTICLE-19-EA-KICTANet-Joint-Memorandum-on-the-Registration-of-Persons-NIIMS-Regulations-2020.pdf (accessed 15 October 2022).

Asian Development Bank (2016) *Identity for Development in Asia and the Pacific*. Mandaluyong City, Philippines: Asia Development Bank.

Atick J, **Gelb AH**, **Pahlavooni S**, **Ramos EG and Safdar Z** (2014) Digital Identity Toolkit: A Guide for Stakeholders in Africa. World Bank Group Working Paper.

Banisar D and Davies S (1999) Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *John Marshall Journal of Computer & Information Law 18*(1), 13–14.

Bhandari V, **Sinha A and Saxena P** (2020) Governing ID: India's Unique Identity Programme. Available at https://digitalid.design/docs/CIS_DigitalID_IndiaCaseStudy_2020.02.pdf (accessed 3 September 2022).

Council of Europe (2004) Convention on Cybercrime (Budapest Convention). Available at https://www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 22 September 2022).

Dokeniya A (2013) *Implementing Right to Information: Lessons from Experience*. Washington DC: World Bank Group.

European Union (EU) (2016) General data protection regulations: Art. 5 GDPR - Principles relating to processing of personal data. Proton Technologies AG. Available at https://gdpr.eu/article-5-how-to-process-personal-data/ (accessed 17 December 2021).

Gillani S, **Dermish A and Grossman J** (2022) The role of electronic transactions and national digital ID systems in the digital economy (United Nations Capacity Development Fund (UNCDF), Policy Accelerator Brief). Available at https://static1.squarespace.com/static/5f2d7a54b7f75718fa4d2eef/t/621d4545d668f30b5c35eab3/1646085472035/EN-UNCDF-Brief-ElectronicID-2022.pdf (accessed 10 November 2022).

Greenleaf G and Bertil C (2020) Comparing African Data Privacy Laws: International, African and Regional Commitments (April 22, 2020). University of New South Wales Law Research Series, 2020. Available at https://ssrn.com/abstract=3582478 (accessed 10 October 2022); https://doi.org/10.2139/ssrn.3582478.

Hofman D and Katuu S (2023) Law and record keeping: A tale of four African countries. In *Managing Digital Records in Africa*. London, UK: Routledge, 7–48.

India (1950) *Constitution of India*. New Delhi: Government Printer.

Kadengye D and Owoko H (2019) A Review of Kenya's 2019 Data Protection Act: Insights for Data Controllers in Africa. Available at https://africaevidencenetwork.org/en/learning-space/article/64/ (accessed 22 September 2022).

Kenya (1947) *Registration of Persons Act, Cap 107*. Nairobi: Government Printer.

Kenya (2010) *Constitution of Kenya (COK)*. Nairobi: Government Printer.

Kenya (2016) *Access to Information Act*. Nairobi: Government Printer.

Kenya (2018) *Computer Misuse and Cyber Crimes Act*. Nairobi: Government Printer.

Kenya (2019a) *Data Protection Act*. Nairobi: Government Printer.

Kenya (2019b) *Kenya Information and Communication (KIC)Act*. Nairobi: Government Printer.
Kihara P (2021) Personal communication.
Mutun'gu G (2021) Digital Identity in Kenya- Case study conducted as part of a ten-country exploration of social- digital ID systems in parts of Africa. Available at 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/ (accessed 13 November 2021).
Mutung'u G and Rutenberg I (2020) Digital id and risk of statelessness. *The Statelessness & Citizenship Review 2*(2), 348–354.
Nubian Rights Forum & 2 others v. Attorney-General & 6 others (2020) Child Welfare Society & 8 others (Interested Parties), EKLR (High Court of Kenya, Nairobi).
Nyambura R (2021) Personal Communication.
Organisation for Economic Co-operation and Development (OECD) (2013) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (accessed 12 November 2022).
Palmer VV and Palmer VV (2012) *Mixed Jurisdictions Worldwide: The Third Legal Family*. Cambridge, UK: Cambridge University Press.
Privacy International (2021) Global Surveillance Monitor. Available at https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf (accessed 13 November 2022).
Rodrigues C (2008) *Implementing Access to Information: A Practical Guide for Operationalizing Access to Information Laws*. New Delhi: Commonwealth Human Rights Initiative.
Sen A (1999) *Development as a Freedom*. Oxford, UK: Oxford University Press.
Trikanad S (2020) Governing ID: Estonia's Digital Programme. Available at https://digitalid.design/docs/CIS_DigitalID_EstoniaCaseStudy_2020.04.pdf (accessed 12 November 2022).
United Nations (2015) *Transforming the World: The 2030 Agenda for Sustainable Development (UN 2030 Agenda)*. New York: United Nations.
United Nations (UN) (1966) International Convention on Civil and Political Rights (ICCPR). Available at http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx (accessed 25 October 2022).
United Nations Conference on Trade and Development (UNCTAD) (2016) Data Protection Regulations and International Data Flows: Implications for Trade and Development. Available at https://unctad.org/webflyer/data-protection-regulations-and-international-data-flows-implications-trade-and (accessed 13 November 2022).
United Nations General Assembly (UNGA). (1948) 183rd Plenary Meeting. International Bill of Human Rights: A Universal Declaration of Human Rights. Resolution 217 (III) (10 December 1948). Geneva: United Nations, 1948. 71–9. Available at http://www.un-documents.net/a3r217.htm (accessed 25 October 2022).
United Nations General Assembly (UNGA) (1965) International Convention on the elimination of all forms of Racial Discrimination (ICERD). Available at https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial (accessed 25 October 2022).
World Bank (2017) *ID Enabling Environmental Assessment*. Washington DC: World Bank.
World Bank (2018) *Privacy by Design: Current Practices in Estonia*. India and Australia Washington, DC: World Bank.
World Bank Group (2016) *World Development Report 2016: Digital Dividends*. World Bank Publications.
Yin R (2009). *Case Study Research: Design and Methods*, 4th edn. Thousand Oaks, CA: Sage.

Cite this article: Kabata V (2024). An assessment of the legal and regulatory framework supporting the implementation of the National Integrated Identity Management System (NIIMS) in Kenya. *Data & Policy*, 6: e7. doi:10.1017/dap.2023.36