Championing an Inclusive, Trustworthy and, Accountable Approach to Uganda’s ID Infrastructure and the Transition to a New Generation ID

A Position Paper
About Unwanted Witness Uganda

Unwanted Witness Uganda – UW is a civil Society Organisation founded in 2012 to promote online freedoms and protect digital rights in Uganda. UW has become a leading voice in advocating for internet freedoms, and digital rights, particularly the right to privacy, digital identity, digital inclusion, and freedom of expression.

The organization aims to create a safe and secure digital environment for citizens and promote the responsible use of technology. It aims to empower citizens to use technology in a safe, secure, and effective manner while holding public and private entities accountable for digital rights violations.

UW achieves its mission through research, advocacy, and empowerment programs. UW conducts research to identify digital rights violations, trends, and threats and uses this information to advocate for policy and legal reforms. The organization also provides digital security training and support to human rights defenders, journalists, and vulnerable groups to enhance their online safety.

In addition, UW engages in public education and awareness campaigns to promote digital literacy and responsible online behavior.

Acknowledgements

Unwanted Witness Uganda extends heartfelt gratitude to its key partners for their invaluable support, which has played a pivotal role in facilitating the successful implementation of its functions.

Unwanted Witness acknowledges the outstanding commitment of its Research and Advocacy Unit, with special recognition to Ms. Freda Nalumansi-Mugambe and the dedicated Researcher, Mr. Odur Anthony, for their significant contributions to the paper’s development. The paper would not have been possible without the invaluable contributions of the esteemed members of the editorial board, notably Ms. Dorothy Mukasa, the Executive Director, Mr. Allan Sempala Kigozi, the Head of Programmes, and Ms. Freda Nalumansi-Mugambe, the Research and Advocacy Lead.

Moreover, the dedication of the entire Unwanted Witness staff throughout the process has been instrumental. Special thanks are extended to Mr. Bruno Emmanuel Arinaitwe and Price Media for the invaluable work in enhancing the graphics and layout, thereby enhancing the quality of the position paper during its development and review phases.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bn</td>
<td>Billion</td>
</tr>
<tr>
<td>BWP</td>
<td>Botswana Pula</td>
</tr>
<tr>
<td>CSOs</td>
<td>Civil Society Organisations</td>
</tr>
<tr>
<td>DPIA</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td>DPPA</td>
<td>Data Protection and Privacy Act, 2019</td>
</tr>
<tr>
<td>DPPPR</td>
<td>Data Protection and Privacy Regulations, 2021</td>
</tr>
<tr>
<td>FAQs</td>
<td>Frequently Asked Questions</td>
</tr>
<tr>
<td>ICCPR</td>
<td>Covenant on Civil and Political Rights</td>
</tr>
<tr>
<td>ID</td>
<td>National Identification Cards</td>
</tr>
<tr>
<td>NIN</td>
<td>Unique national identification number</td>
</tr>
<tr>
<td>NIRA</td>
<td>National Identification and Registration Authority</td>
</tr>
<tr>
<td>NSIS</td>
<td>National Security Identification System</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>ROPA</td>
<td>Registration of Persons Act, 2015</td>
</tr>
<tr>
<td>SDGs</td>
<td>Sustainable Development Goals</td>
</tr>
<tr>
<td>UGX shs</td>
<td>Uganda Shillings</td>
</tr>
<tr>
<td>ULRC</td>
<td>Uganda Law Reform Commission</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNHCR</td>
<td>United Nations High Commissioner for Refugees</td>
</tr>
<tr>
<td>UDHR</td>
<td>Universal Declaration of Human Rights</td>
</tr>
<tr>
<td>USD</td>
<td>United States Dollars</td>
</tr>
<tr>
<td>USPC</td>
<td>Uganda Security Printing Company Limited</td>
</tr>
<tr>
<td>UV</td>
<td>Ultra Violet Light</td>
</tr>
</tbody>
</table>
# Table Of Contents

About Unwanted Witness Uganda ........................................................................................................... 2  
Acknowledgements ..................................................................................................................................... 2  
Abbreviations ........................................................................................................................................... 3  
Executive Summary ................................................................................................................................. 5  
I. Introduction ........................................................................................................................................... 8  
Background Information on the National ID System in Uganda ................................................................. 8  
Purpose of the Position Paper .................................................................................................................... 8  
Overview of the Paper ............................................................................................................................... 8  
II. Current State of the ID System in Uganda ............................................................................................. 9  
Legal and Regulatory Framework Governing Uganda’s National ID System ............................................ 9  
Significant Milestones Achieved by Existing ID System ......................................................................... 13  
III. Areas of Improvement and challenges Encountered: Implications and Solutions ......................... 15  
Exclusion Concerns and Marginalised Populations ............................................................................... 15  
Analysis of Financial Burden on Citizens ................................................................................................. 16  
Privacy Concerns and Data Protection Issues: Identifying Vulnerabilities and Potential Risks ....... 18  
IV. Introducing the New Generation ID System ....................................................................................... 20  
Overview of the features and benefits of the New ID System ................................................................. 21  
Cost, Inclusion, Privacy and Data Protection Considerations in the New Generation ID ....................... 21  
V. Conclusion ......................................................................................................................................... 24  
VI. Recommendations ........................................................................................................................... 24
Executive Summary

The position paper provides an in-depth analysis of the National ID System in Uganda, focusing on the National Security Identification System and the emerging New Generation National ID Project (Ndaga Muntu). The NSIS project, initiated to address security threats and enhance public services, raised human rights concerns around increased unlawful surveillance and potential privacy violations. Despite efforts to implement data integrity and privacy protection protocols, fears of government overreach persisted.

The paper highlights the purpose of examining human rights concerns related to Uganda’s ID infrastructure and the impending New Generation National ID Project. It critically evaluates NSIS, emphasizing its shortcomings and advocating for a transparent, inclusive, and accountable identification framework. The role of the National Identification and Registration Authority (NIRA) is scrutinized, addressing privacy concerns and security vulnerabilities.

The overview of the paper traces the developmental trajectory of NSIS, its obstacles, and progress. It analyzes the effectiveness of NIRA in citizen registration and data consolidation, expressing concerns about financial strain and potential exclusion of marginalized populations. Privacy issues, legal framework gaps, and the introduction of advanced biometric measures in the New Generation National ID Project are extensively explored.

The paper presents several recommendations to enhance Uganda’s National ID system, acknowledging significant shortcomings in the current system. Overall, the study emphasizes how the deployment of Biometric technologies in a human rights void may raise predictable and serious human rights concerns.

Recommendations for Parliament and Law Reform Commission:

- Review the Registration of Persons Act, 2015 and undertake an amendment of
  - include provisions for alternative forms of identification for accessing essential services to prevent unjust exclusion,
  - reduce replacement and error corrections charges,
  - penalties for non-registration and failure to update information in Section 76(a) and Section 64(5) to more considerate of vulnerable groups,
  - Section 55(1) and Schedule 3 to limit unnecessary collection of personal data during registration to protect privacy and advance data minimization;
  - Section 65 to provide for well-defined specific purposes for which registered data can be used to prevent potential misuse,
  - Section 66 to remove the requirement of ID cards for accessing basic services to avoid exclusion,
  - Schedule 3 to ensure that only necessary sensitive personal information is collected during registration to reduce data management burden and uphold privacy rights;
- Allocate adequate resources to NIRA for making enrollment services more accessible for vulnerable groups and the entire public;

Recommendations for Ministry of Internal Affairs

- Evoke the Minister’s powers under the Registration of Persons Regulations, 2015 and direct for the;
  - modification ID replacement fee structure to be reduced substantially to at least $4 US dollars, as to ease financial strain on marginalized groups, ensuring replacement fees are fair and accessible or a complete removal of the fees;
  - implement provisions allowing for alternative identification, like temporary IDs, for those unable to obtain National IDs to ensure equitable access to essential services and prevent exclusion of vulnerable individuals;
  - invest in modernizing and expanding infrastructure to improve efficiency and access across different regions.
Recommendations for the National Identification and Registration Authority

- Conduct a thorough Data Protection Impact Assessment (DPIA) ahead of the envisaged mass enrollment as mandated by Regulation 12 of the Data Protection and Privacy Regulations, 2021
- Publish a Privacy Policy to ensure alignment with Section 3 (a), (b) (e) and (f) of the Data Protection and Privacy Act, 2015
- Reassess penalties for non-registration and information updates to ensure they are proportionate and do not disproportionately affect marginalized groups.
- Implement automated feedback mechanisms to promptly notify applicants of application errors, reducing processing delays and inaccuracies.
- Develop a comprehensive data migration strategy prioritizing security and compliance with data protection regulations.
- Establish clear guidelines for data sharing with consent mechanisms to empower citizens with control over their data.
- Implement efficient data management practices to prevent the accumulation of uncollected ID cards, safeguarding sensitive data.
- Deploy robust security measures to protect biometric data from unauthorized access, regularly auditing and updating protocols.
- Provide specialized training for personnel handling biometric data, particularly for vulnerable groups.
- Operationalization of the complaints handling mechanism, to receive and investigate complaints.
- Conduct periodic audits and evaluations of the National ID system for continual improvement and compliance.

Recommendations for the Personal Data and Protection Office

- Provide guidance to NIRA about their obligations and responsibilities while collecting data,
- Supervise NIRA and monitor them on all matters in relation to data collection,
- Conduct audits in NIRA’s data collection operations to ensure compliance with the data protection laws of Uganda,
- Partner with NIRA to review the data collection process, focusing on collecting only necessary information to meet identification requirements and reducing the burden on data management and,
- Engage with relevant stakeholders to develop comprehensive data protection regulations outlining the collection, storage, and sharing of citizens’ data, with a strong emphasis on robust security measures.

Recommendations for Civil Society

- Advocate for reducing replacement fees for national IDs by collaborating with authorities and presenting data on the impact of these fees on marginalized groups for policy reforms.
- Push for the enhancement of citizens’ rights, including clarity on consent requirements, data usage limitations, and penalties for data misuse in key legislation like the DPPA and ROPA.
- Monitor compliance with the DPPA and other relevant legislation to ensure accountability.
- Refer and submit complaints to PDPO about data breaches for appropriate resolution.
- Lead public awareness campaigns to educate citizens about their rights regarding personal data and privacy and to hold authorities and tech companies accountable.
- Conduct research with legal and data experts on areas of concern, such as inclusivity and control, and advocate for reforms. Engage policymakers to promote inclusivity and fairness in the ID replacement process.
- Advocate for data collection practices that align with privacy principles and limit the collection of sensitive personal information.

- Collaborate with independent auditors to assess data management practices within NIRA and monitor the implementation of privacy safeguards in the new ID system.
I. Introduction

A. Background information on the National ID System in Uganda

The concept of a legal identification system hinges on its ability to enable individuals to establish their identity using credentials officially recognized by law or regulation as valid proof of legal identity. The initiation of the National Security Identification System (NSIS) Project seemed to have been intended to address emerging security threats and to enhance public services. However, it sparked human rights concerns, including increased unlawful surveillance and control over citizens. The NSIS Project was a convoluted journey, marked by consultations and collaboration among various government bodies and technology experts. The project’s objectives prioritized data collection and centralization at the potential expense of people’s fundamental right to privacy, raising serious concerns about the likely misuse and abuse of citizens’ personal information. The implementation of data integrity and privacy protection protocols were not sufficient to allay fears of government overreach and intrusion into citizens’ lives.

The National Identification and Registration Authority (NIRA) plans to provide an app for card authenticity verification as to protect the owner’s privacy, without detailing how this would be achieved. However, this digital ID system also supports e-Consent and related technologies, which may enable invasive data collection and unregulated surveillance.

Therefore, the new National ID system for Uganda also known as Ndaga Muntu, while framed as offering heightened security and functionality, is fraught with human rights concerns and exclusion challenges. The broad definition of “biometric” and the potential for privacy infringements continue to cast a shadow over its implementation.

B. Overview of the position paper

This position paper primarily focuses on the human rights concerns surrounding Uganda’s existing ID infrastructure and the emerging new generation ID system. It highlights various issues related to inclusivity, data security, and privacy. The paper critically analyzes the National Security Identification System (NSIS), shedding light on its developmental trajectory and influence. It traces the project’s origins and emphasizes its shortcomings and the pressing need for a more transparent, inclusive, and accountable identification framework.

The establishment and role of NIRA in its effectiveness in citizen registration and data consolidation is examined, alongside a detailed exploration of privacy concerns and security vulnerabilities. It seeks to navigate the complex balance between security demands and individual rights in Uganda’s evolving ID landscape, implying that there are significant challenges and trade-offs to be addressed in achieving this balance.

Additionally, it raises apprehensions regarding the financial strain associated with ID replacement on marginalised populations facing exclusion due to mandatory ID usage. The impending introduction of the New Generation National ID Project is expected to involve capturing of more biometric data, raising questions about the potential risks associated with violating citizens’ right to privacy. The introduction of the New Generation National ID Project is discussed, with an emphasis on the integration of advanced biometric measures for security, but with lingering questions about how privacy rights will be upheld. It turns a spotlight on the gaps between the legal frameworks in place and their actual implementation.

The paper offers recommendations, primarily centered on the approach that promotes inclusivity and privacy.

7 Mr Samuel Muhimba, ‘Gov’t drops shs 50,000 charge for national ID renewal’ Wednesday 14 February, 2024 https://nilepost.co.ug/editors-choice/188406/govt-drops-shs50000-charge-for-national-id-renewal
for the improvement of Uganda’s National ID system, but they underscore the fact that there are significant shortcomings in the existing system.

In summary, the study underscores the ongoing struggle to strike a balance between security imperatives and individual rights as Uganda’s national ID landscape evolves, suggesting that achieving this equilibrium is a complex and challenging endeavour.

II. Current State of the ID System in Uganda

A. Legal and Regulatory Framework Governing Uganda’s National ID System

- **International and Regional Framework**

Uganda’s national identification system is grounded in both international and domestic legal frameworks, highlighting the state’s obligation to safeguarding identification and personal information while adhering to principles of inclusion and accountability. In adherence to international human rights standards, Uganda aligns itself with the Universal Declaration of Human Rights (UDHR)8 and the International Covenant on Civil and Political Rights (ICCPR).9 Particularly, Article 6 of the UDHR entitles everybody to the right to legal identity and just as vital is the overarching responsibility to protect the data that substantiates this identity. Article 17 of the ICCPR that provides for the right to privacy and recognition as a person before the law; and the African Declaration on Internet Rights and Freedoms,10 Principle 8, which recognizes the significance of protecting personal data online in the digital age.

Equally, worth noting is the UN legal identity Agenda 202211 with an overall objective to promote holistic, interoperable, and sustainable civil registration, vital statistics, and identity management systems for more than 300 million people to acquire a legal identity by 2025. Additionally, are the Sustainable Development Goals (SDGs), specifically SDG 16 Target 16.9 that calls for ‘legal identity for all, including birth registration, by 2030’12 acknowledged as crucial for advancing the 2030 Development Agenda commitment to leave no one behind.

Likewise, are the principles that guide identification for sustainable development critical in assessing features and advantages of ID infrastructure within this context.13 These principles are organized into three primary pillars: inclusion, design, and governance and discussed in detail below;

a) **Inclusion and Accommodative Features**

In the context of inclusion, the new ID attempts to address human rights issues by introducing enhancements supposedly accommodating persons with disabilities (PWDs) and older persons. These enhancements include the incorporation of biometric elements such as iris scanning and facial images, in addition to fingerprints and face recognition.14 While this may seem like a step in the right direction, it’s crucial to note that the focus here is primarily on biometric data potentially increasing the burden of data protection and privacy concerns including malfunctioning leading to exclusion. Moreover, the introduction of Optical Variable Ink as a deterrent against imitation might be seen as a superficial security measure that could potentially inconvenience users. While the inclusion of tactile features for those with sight challenges is a commendable effort,15 the overall effectiveness and true commitment to a discrimination-free identification system remains questionable, given the broader context of data privacy and accessibility concerns.

---


b) Mass Enrollment Strategies

NIRA intends to expand its reach by setting up mobile enrollment centres in 146 districts, covering 10,594 parishes seemingly with the aim of increasing accessibility. However, the emphasis on digital forms and online services may inadvertently exclude those without reliable internet connectivity, raising concerns around equitable access. While NIRA’s intention to cater for individuals in specific institutions like prisons and orphanages is laudable, the feasibility and effectiveness of establishing dedicated centers for their registration needs remain uncertain. Additionally, the plan to provide mobile kits through partnerships might be viewed with skepticism, as it could potentially raise questions about data security and the quality of the enrollment process. While NIRA portrays its intentions to cater for individuals in specific institutions like prisons and orphanages is laudable, the feasibility and effectiveness of establishing dedicated centers for their registration needs remain uncertain. While NIRA portrays

The new card incorporates a consent-based feature, ensuring seamless authorization for anyone to access or retrieve the card owner’s information in compliance with the Data Privacy and Protection Act, 2019. This enhances transparency by granting full visibility to those seeking access to the owner’s data. NIRA will also provide an App that will be used to verify the authenticity of a Card while protecting the privacy of the card owner. To allow card owners to manage their data with informed consent, e-consent and related technologies have been incorporated.

The new card incorporates a consent-based feature, ensuring seamless authorization for anyone to access or retrieve the card owner’s information in compliance with the Data Privacy and Protection Act, 2019. This enhances transparency by granting full visibility to those seeking access to the owner’s data. NIRA will also provide an App that will be used to verify the authenticity of a Card while protecting the privacy of the card owner. To allow card owners to manage their data with informed consent, e-consent and related technologies have been incorporated.

The reliance on Public Key Infrastructure (PKI) and unique digital certificates may seem like a security measure, but the effectiveness and security of these systems may be questioned, especially in the face of evolving cybersecurity threats. While the card is said to have ISO Standard biometric features and digital signatures in its 2D barcode, the actual protection of individuals’ data remains uncertain, as the readability of the card by specific cryptographic libraries raises concerns about potential access by unidentified or unauthorized persons. While the mentioning of alignment with data control standards is made, the practical implementation and the broader context of data security including considerations in relation to classification of the data to be collected and human rights protection still leave room for skepticism.

c) Consent and Data Management

The assurance of total transparency in data retrieval is subject to scrutiny, given the history of data breaches and misuse. In this second phase, NIRA appears to be making an attempt to create an accessible and user-friendly system. However, the effectiveness and timeliness of such notifications is not certain, including circumstances involving malfunctioning of the system.

The new card incorporates a consent-based feature, ensuring seamless authorization for anyone to access or retrieve the card owner’s information in compliance with the Data Privacy and Protection Act, 2019. This enhances transparency by granting full visibility to those seeking access to the owner’s data. NIRA will also provide an App that will be used to verify the authenticity of a Card while protecting the privacy of the card owner. To allow card owners to manage their data with informed consent, e-consent and related technologies have been incorporated.

The reliance on Public Key Infrastructure (PKI) and unique digital certificates may seem like a security measure, but the effectiveness and security of these systems may be questioned, especially in the face of evolving cybersecurity threats. While the card is said to have ISO Standard biometric features and digital signatures in its 2D barcode, the actual protection of individuals’ data remains uncertain, as the readability of the card by specific cryptographic libraries raises concerns about potential access by unidentified or unauthorized persons. While the mentioning of alignment with data control standards is made, the practical implementation and the broader context of data security including considerations in relation to classification of the data to be collected and human rights protection still leave room for skepticism.

d) User-Friendly Design and Applicant Communication

Within the design framework, it’s suggested that identification systems should prioritize accurate data collection and user-friendly procedures for data access and correction to maintain accuracy over time. While this may sound reasonable, there is a need to critically assess how this principle translates into practice. NIRA’s promise to notify applicants of their application progress via SMS/email notifications seems like an attempt to adhere to this guideline. However, the effectiveness and timeliness of such notifications is not certain, including circumstances involving malfunctioning of the system.

---

21 Principle 2
24 Principle 8
It is essential to consider the broader context of data handling and security, especially when it comes to sharing sensitive information like telephone numbers and email addresses. While the principle emphasizes meeting people’s needs and concerns, the actual implementation and protection of individuals’ rights in the identification process remains uncertain.

**e) Enhanced Security and Privacy Measures**

Emphasizing the critical importance of security and privacy, it is asserted that safeguarding personal data from improper use requires a multifaceted approach involving legal and regulatory measures, system design, and adherence to technical standards. However, an examination of NIRA’s approach raises concerns about the effectiveness of these safeguards in practical implementation. The proposition of an App for verifying card authenticity, while seemingly a step towards protecting cardholders’ privacy, introduces potential vulnerabilities, especially concerning data stored on personal devices. Despite the mention of security measures such as incorporating digital images of the Court of Arms, securely embedded artifacts, and UV features for authentication, these sophisticated measures may not comprehensively address broader human rights concerns linked to unauthorized access, tampering and misuse of personal data within the identification system. The lack of clarity on how NIRA intends to ensure the safeguarding of individuals’ data leaves room for skepticism regarding the adequacy of their measures in protecting human rights during the identification process. A more comprehensive and transparent approach is needed to address evolving security threats and mitigate the risk of data breaches, ensuring the protection of individuals’ rights.

**f) Error Correction Mechanism**

NIRA’s approach to addressing errors and deficiencies, as outlined in Principles 8 and 9, raises concerns regarding potential human rights issues. While they claim to have mechanisms in place for error correction, the process seems to heavily rely on the discretion of NIRA officials. This could potentially lead to arbitrary decisions, putting applicants at risk of being denied important services or rights based on vague criteria like “inadequate or contradictory documentation” or the need for “further clarification.” Such ambiguity in the process raises questions about fairness, transparency, and the protection of individuals’ rights during the application procedure.

- **National Framework**

At the domestic level, the 1995 Constitution of the Republic of Uganda, as amended, has a number of provisions regarding citizenship. Articles 10 to 13 detail the citizenship acquisition process, Article 14 outlines conditions for citizenship revocation, and Article 15 specifies conditions for those obtaining foreign citizenship. The pivotal role played by the National Citizenship and Immigration Board, established under Article 16, involves issuing national identity cards, passports, and immigration permits. Additionally, Article 59(2) mandates citizens over 18 to register as voters, underscoring the crucial role of identification in civic processes. Article 27 of the Constitution reinforces the right to privacy.

Pursuant to the Constitution, the Citizenship and Immigration Control Act provides for acquisition of citizenship of Uganda to provide for the compulsory registration of all Ugandans and the issue of national identification numbers and the issue of national identity cards to citizens of Uganda. Upon registration, every citizen will be allocated by the citizenship and immigration board a national identification number and a document of identity.

This document establishes the nationality and identity of the holder for the time being in force issued or renewed by the government or some valid document of identity satisfactorily establishing the holder’s nationality or...
The Registration of Persons Act, 2015, establishes the National Identification and Registration Authority (NIRA) with a national identification register, maintained electronically or in any other form. This register includes information on registered persons, and the Act mandates continuous updates with obligations for individuals to notify changes. The use of national identification cards (IDs), introduced by the Act, is mandatory for accessing various services, emphasizing a unique national identification number (NIN) as evidence of citizenship. Upon registration, National identification cards are issued to citizens and aliens, with their respective ID numbers. While these measures enhance identification, they also raise concerns about security, potential misuse, proof of citizenship vis-à-vis residency and unauthorized disclosure of ID-related information.

Section 66 of the Act impacts services such as employment, voting, passport applications, and land transactions, simplifying processes but also raising privacy concerns if not effectively managed.

In addition to the above, the Act includes offenses and penalties. These range from failure to register, providing false information, to producing fraudulent identity documents. Section 77 of the Act provides for offenses relating to identification cards. Penalties, including fines and imprisonment, are prescribed according to the severity of the offense. The Act aims to deter misconduct while ensuring adherence to its principles.

To address disputes, the Act establishes an Identification and Registration Committee, with appeal avenues to the High Court, promoting accountability and transparency. However, challenges may arise in ensuring a fair and efficient process for resolving disputes. The Committee is mandated to oversee the registration process as stipulated in the regulation. Its primary function is to evaluate whether an individual meets the specified criteria for registration.

Despite progress, concerns about security, potential misuse, proof of citizenship, and unauthorized disclosure of ID-related information persist. In 2019, Uganda adopted the Data Protection and Privacy Act of 2019, expecting entities like the National Identification and Registration Authority (NIRA) to adhere to principles of accountability, legality, transparency, and data security. While the Registration of Persons Act emphasizes confidentiality, facing challenges in fully enhancing privacy within the National ID system, continuous efforts are necessary to bridge gaps, strengthen data protection mechanisms, and address emerging challenges in the digital landscape. The cornerstone of Uganda’s privacy protection efforts is the Data Protection and Privacy Act of 2019, highlighting explicit consent for data collection and processing and recognizing the sensitive nature of personal information. Other related legislation include the Data Protection and Privacy Regulations of 2021.

Granting legal identity requires extensive personal data; names, birth dates, gender, and demographic information like residential addresses. As Uganda rolls out legal identity system, it is crucial to implement robust protection laws that address the unique challenges and mitigate privacy risks. Legal Data breaches, unauthorized access, and misuse can have dire consequences, not just technologically but also socio-economically and politically.
A. Significant Milestones achieved by the existing ID System

**Enrollment for accessing National IDs**

As of November 2022, Uganda’s National Identification and Registration Authority (NIRA) continued its efforts to strengthen the national ID system, albeit with a set of glaring issues related to human rights and exclusionary concerns. One notable aspect of this endeavour was the overwhelming influx of applications received, totaling 30.3 million from an estimated population of 43.7 million\(^{57}\), ensuring that the depicted number does not downplay the fundamental issues. This high application rate, at 69%, may mask deeper problems and pressures within the population, such as fears of exclusion or limited access to essential services without a national ID.

Additionally, while NIRA did manage to process and register 25.9 million citizens,\(^{58}\) constituting 86% of the total applicants, this achievement may also highlight the difficulties citizens face in accessing this vital document.\(^{59}\) It is concerning that 14% of applicants were unable to secure registration due to double applications, incomplete information and questions regarding citizenship verification among others,\(^{60}\) potentially resulting in their further marginalization from crucial services and rights.

**ID Infrastructural improvements**

NIRA’s peddled transparency efforts, including SMS notifications, a USSD platform (*216#), and an online website for checking registration status,\(^{61}\) should be seen as essential steps, but they should not overshadow the fact that such mechanisms might be necessary due to the underlying complexities of the registration process.

Equally of concern is NIRA’s information harmonization initiative with 68 institutions.\(^{62}\) While it may seem like a commendable effort to link identities with services, without clear safeguards and legal remedies, this integration could potentially lead to intrusive surveillance, marginalization in access to key services and unwarranted tracking of citizens by various institutions, raising serious human rights violations including the right to privacy.

The system infrastructure improvements\(^{63}\), while portrayed as proactive, might be seen as merely reactive measures to safeguard an ID system that could be inherently flawed in terms of privacy and security. Rather than addressing the root issues, these upgrades may be seen as patching up a system that lacks strong foundations.

NIRA’s partnership with the Uganda Security Printing Company Limited (USPC) for reliable supply of blank ID cards\(^{64}\) and security documents,\(^{65}\) while framed as enhancing quality and availability, might also be viewed with skepticism. It raises questions about the potential for state-controlled ID issuance, which could further limit access.

Relatedly, one of the most glaring is the government’s slow progress in incorporating constitutional and human rights principles and global ID standards into Uganda’s national identification system. The absence of robust privacy, inclusivity, and data protection measures could result in severe consequences, potentially jeopardizing the interests of those reliant on public services. Addressing these challenges is not only crucial but urgent, as they fundamentally impact the long-term effectiveness and legitimacy of Uganda’s national ID system.

In a move driven by the need to sustain the National Identity Card project financially, the government put forth a proposal to amend Regulation 32 of the National Citizenship and Immigration Control Regulations. This contentious amendment sought to introduce an option for individuals to willingly contribute payments towards their National

---

58 NIRA website FAQs
64 Report of the Auditor General on the Financial Statements of the National Identification and Registration Authority for the year ended 30th June 2022, p 16.
Identity Cards in the fiscal year 2013/2014. This strategy created a financial burden for persons to obtain an essential document for civic participation.

The year 2014 saw Uganda’s attempt to establish a modernized identification system with the launch of the National ID Enrollment Exercise and Issuance. For the government, this event heralded a new era of streamlined citizen registration, data integration, and enhanced national security, but it also presented serious human rights concerns. The issuance of National Identity Cards might have been celebrated by some, but it also represented a worrisome culmination of an enrollment exercise, taking place against a backdrop of a normative framework with inadequate safeguards yet, it involved collecting and verifying biometric data from individuals.

In compliance with Form D of the Third Schedule of the Uganda Citizenship and Immigration Control Act, 2006, the National ID Card contained a comprehensive range of personal data, including the individual’s full name, previous or maiden names, sex, age, postal and residential addresses, occupation, and marital status. It delved further into physical attributes such as height, eye and hair color, as well as details about the place and date of birth, including village, sub-county, county, and district. The card also captured information about indigenous community affiliation, parentage (including fathers’ and mothers’ names, birthplaces, and clan particulars), previous nationality, and two contemporary descendants. Additionally, it included particulars of the applicant’s children, passport and driving license details, tax identification number, and blood group. This extensive dataset aimed to provide a comprehensive and accurate representation of an individual’s identity for official documentation and verification purposes. Despite the Constitution’s dispositions on respect for economic and cultural rights, the aggressive process without proper safeguards, could be seen as a breach of people’s privacy.

The President’s pronouncements regarding the strategic advantages of the National ID project, including its ability to combat electoral fraud and reduce ghost employees, were, at best, questionable. These claims conveniently ignored the possibility of misusing and abusing this extensive data collection, potentially infringing upon the very rights they purported to safeguard.

In 2014, the National ID Enrollment Exercise and Issuance Official Launch, rather than being perceived as a project centered on people and their rights, generated concerns about the government’s increasing control over its citizens’ personal data. The government’s emphasis on data administration and technological amalgamation tended to obscure the paramount imperative of safeguarding privacy amidst the pursuit of national progress.

By 2015, the government managed to enroll around 15 million individuals aged 16 and above for National ID cards through a mass enrollment campaign. Alongside this, the government completed the National Security Information System (NSIS) project, which led to enactment of the Registrations of Persons Act, 2015.

Under the 2015, The National Identification and Registration Authority (NIRA), a corporate body with perpetual succession and official seal was established. It has the power to acquire, hold, and dispose of property, sue and be sued, and perform all lawful acts as a corporate entity. The Authority’s primary functions include creating, managing, and operating the National Identification Register, registering citizens and lawfully resident non-citizens, recording births and deaths, assigning unique national identification numbers, issuing identification cards, harmonizing data from other government databases, and ensuring information security. It is mandated to cooperate with government agencies and may collaborate with various players in the registration sector. The Authority also possesses the power to charge fees for its services. In executing its functions, it must adhere to information security practices and industry regulations.

However, it’s crucial to recognize that these achievements were accompanied by significant human rights concerns and challenges.

67 Neema Iyer (n 5 above), p 11
69 Zetes supplies 4250 biometric kits to Uganda, https://itweb.africa/content/P3gQ2qGxYnJvnRD1, Accessed on August 28, 2023.
While NIRA worked on creating an advanced identification system, its primary aim was to establish stringent measures for addressing perceived national security threats such as criminal activities, terrorism and immigration control.

III. Areas of Improvement and Challenges Encountered: Implications and Solutions

A. Exclusion Concerns and marginalized populations

The barriers preventing inclusivity are multifaceted and collectively hinder the efficiency, transparency, and accessibility of their services. These barriers, if left unaddressed, can have significant implications for citizens’ rights, service quality, and the overall effectiveness of the identification system hence, exclusion matters can be explored from various viewpoints; ranging from legal parameters, financial and technical challenges.

i) Legal Parameters

The implementation of the current national identification system, in accordance with Section 66, mandates the use of national IDs for accessing public services, employment, financial transactions, and other crucial activities. While the concept of utilizing ID cards for identification and accessing essential services may be advantageous, the mandatory nature of their requirement, without viable alternative options, has resulted in an unjust exclusion of vulnerable groups.

Section 76(a) of the law criminalizes non-registration according to the Act’s stipulations. Those failing to comply may face a fine amounting to UGX shs. 2,400,000/= or an imprisonment of 5 years or both, with potential adverse effects on marginalized or vulnerable groups already struggling to obtain identification cards.

Similarly, Section 64(5) imposes penalties for failure to inform the Authority about any changes or errors in recorded information, without reasonable cause. The imposition of criminal sanctions for not promptly updating personal information could be perceived as excessively harsh and disproportionate.

Equally, Section 54 of the Registration of Persons Act (ROPA) 2015 is the bedrock for mass enrollment. It requires the registration of every Ugandan citizen, regardless of their location within or outside the country, with NIRA. Simultaneously, individuals holding national identification cards must initiate the renewal process with NIRA at least two months before the card’s expiration of the ten period. Mass Enrolment aims to register all unregistered Ugandans, including children, at the parish level, ensuring increased access for citizens. Mass Renewal is focused on renewing cards issued between 2014 and 2015 in compliance with the Registration of Persons Act, 2015. However, exemptions exist for non-residents and refugees, reflecting a need for balance between inclusion and control.

ii) Technical Hurdles

The technical challenges faced at NIRA service units disproportionately affect vulnerable and disadvantaged groups. Among these, NIRA requires about seven (7) working days as its standard timeline from the date of application to issue an applicant an identity card. However, in practice, it takes an average of twenty-one (21) days for an identity card to be produced from the time of enrolment to card printing. This exceeds acceptable standards, which is detrimental as it obstructs the timely delivery of crucial services to citizens. These delays lead to frustration and dissatisfaction among applicants,

73 Section 54 of the Registration of Persons Act, 2015.
74 Regulation 23 (1) of the Registration of Persons Regulations SI 67 of 2015.
Compounding the challenge is the failure to notify applicants of application errors. Without proper feedback mechanisms, flawed applications remain uncorrected for extended periods, perpetuating inaccuracies and prolonging the application process.\(^7\) Additionally, the lack of clear communication about card availability creates difficulties for citizens in knowing when their IDs are ready for pickup, resulting in repeated fruitless visits and transportation expenses.\(^8\) This opacity contributes to the inefficiency of the system and may discourage individuals from actively participating in the identification process. NIRA contends with a shortage of staff for data processing, with only 14 personnel handling applications across the nation.\(^9\) Furthermore, the performance of personalization machines has declined due to prolonged use beyond recommended operational lifespans.\(^2\) Leading to inefficiencies, congestion, and compromised accessibility and timeliness of services for citizens.

The inadequacy of customer service management and the absence of comprehensive awareness campaigns contribute to limited citizen engagement. Without dedicated staff to address complaints, citizens are left with unresolved issues, potential dissuading them from seeking ID services. The lack of accessible support beyond regular office hours, isolates citizens further, hindering them from fully utilizing NIRA’s services.\(^8\)

Moreover, the concentration of registrations and collections in specific urban areas, evident by the congestion at these locations, perpetuates a lack of inclusivity.\(^1\) This geographical bias hinders citizens from other regions in accessing services, underscoring the need to address this issue to ensure equitable access for all.

In conclusion, the barriers impeding inclusivity are complex and interlinked. Tackling these challenges necessitates a comprehensive and coordinated approach involving streamlining processes, investing in modern infrastructure, prioritizing transparent communication, ensuring proper governance, and optimizing resource allocation. Overcoming these barriers is imperative for NIRA to fulfill its mandate. Access to services should depend on providing accessible, reliable, and inclusive identification services to all Ugandan citizens.

### B. Analysis of the Financial burden on Citizens

**High Cost of ID Replacement and its implications on citizens /Marginalized Groups**

Uganda, with a population of approximately 45 million people,\(^6\) is still grappling with poverty, ranking among the world’s poorest nations. As of 2021, around 30.1% of the population, equivalent to 12.3 million individuals, lived below the poverty line of $1.77 per person per day, as reported by the Uganda Bureau of Statistics.\(^6\) Against this backdrop, the implications of the high cost of replacement for the national and alien identification cards, have far-reaching effects on both individuals and the nation at large.

The Schedule, Part A of the Registration of Persons Regulations, 2015, S.I. No. 67 provides for fees regarding ID services. At the heart of the issue is the steep fixed fee of UGX shs. 50,000/- ($13.78 USD) for replacing identification cards,\(^7\) and making updates or rectifying errors. The announcement in February 2024 by the State Minister of Internal Affairs waiving ID renewal fees is a welcome development in one hand, but takes away with other hand with increasing the fees up to UGX shs. 200,000/- ($ 52.9 USD) for rectify errors not as a result of NIRA from

---

UGX shs. 50,000/-.

Furtherstill, despite the Minister’s waiver during his appearance before the Parliamentary Defence and Internal Affairs Committee, the renewal fees are still in existence on NIRA’s form fees at the website. 

Equally, express services for receipt of cards within 48 hours are set to cost the same as replacement for varying reasons. Whether the cost is set at UGX shs. 50,000/- or 200,000/-, these fees are pretty high for an ordinarily Ugandan. This financial hurdle presents a significant challenge to disadvantaged persons/groups, especially women, youth, PWDs and older persons.

Given the dire economic circumstances, a person living below the established poverty line of $1.77 USD per day would require roughly 8 days to amass the funds necessary to replace an ID worth $13.78 US Dollars. Comparing with the new international poverty line of $2.15 per person/day adopted in September 2022 that the World Bank has used and estimated 42.2% of the population as living in extreme poverty and, equally confirmed in the findings of latest Multidimensional Poverty Index Report by the Government of Uganda. 42.1% of the population was estimated to be multidimensionally poor. This starkly illustrates how the high cost places a considerable burden on disadvantaged persons who are already struggling to meet their basic needs. The financial burden of obtaining an ID is significantly heightened by various factors, such as service inaccessibility, frequent travels, and accommodations needed for distant locations. For individuals facing these challenges, the expenses tied to the ID application process, along with the costs of transportation to and from the relevant authorities, represent a substantial portion of their income. Moreover, the elevated cost of replacement only worsens their financial struggles, further marginalizing them from essential societal functions.

For the youth in Uganda, who often have limited financial resources and may be dependent on their families, the high replacement fee can be a major obstacle. Replacing their IDs, which are necessary for various activities such as enrolling in schools, opening bank accounts, or seeking formal employment, becomes more challenging, potentially limiting their opportunities for personal growth and economic advancement. While, older persons, who may be on fixed pensions or limited retirement benefits, may find it particularly challenging to afford the replacement fees. As they rely on their IDs for accessing health services and social assistance, the high cost can hinder their ability to maintain their identification documents up-to-date, potentially affecting their access to Social Assistance Grants for Empowerment (SAGE) programme.

Examining the expenses related to replacement of national IDs in Rwanda, Kenya, Tanzania and South Africa, it is apparent that Uganda charges a higher replacement fee of 50,000/- Ugandan Shillings (approximately $13.75 USD). In contrast to neighboring Tanzania, where the replacement charge is Tanzanian Shillings 20,000/-.

In contrast to neighboring Tanzania, where the replacement charge is Tanzanian Shillings 20,000/-.

ID Replacement Costs in Comparison to Selected African Countries


95 Principle 7.


Moving to Kenya, the replacement charge is 2,000 Kenyan Shillings (approximately $12; £10). While it is lower than Uganda, it is still high compared to Kenya’s GDP rated at 5% in 2023 from 4.8% in 2022 according to the 28th edition of Kenya Economic Update and poverty line where 16.1% of its population lives below the international poverty line, currently rated at $2.15 per day despite its large and developed economy in eastern and central Africa.

In Rwanda, the cost of replacing a lost or damaged national ID is set at Rwandan Francs (Rwf) 1,500 (approximately USD 1.27). Additionally, applicants have the option to apply for a temporary ID, incurring an extra fee of Rwf 500 (approximately $0.42 USD). When compared to Uganda’s replacement cost, Rwanda’s fees are notably lower, making the replacement of national IDs more affordable for Rwandans.

Shifting focus to South Africa, the Department of Home Affairs offers to replace an ID free of charge if errors in personal information are identified upon issuance. However, the issuance of a Temporary Identity Certificate (TIC) carries a fee of 70.00 South African Rand (approximately $3.79 USD), and replacing a lost, stolen, or damaged ID costs 140 South African Rand (approximately $7.59 USD). Both the TIC issuance fee and the replacement fee are considerably lower than Uganda’s renewal cost, showcasing a substantial contrast in pricing structures.

The above cost analysis reveals that Uganda’s national ID replacement fee of Uganda Shillings 50,000/- or 200,000/- (approximately $13.75 and $52.9 USD respectively) is relatively higher compared to neighboring countries like Kenya and Rwanda, as well as countries further afield like South Africa and India where the replacement cost for the Aadhaar is at R 50 (approximately $ 0.60 to 1.5 USD). While some countries offer cost-effective replacement options or even free replacements, Uganda’s fee appears to be on the higher end within this comparative context. In summary, the significant disparity in replacement fees between Uganda and other African nations, both nearby and afar, points to the relatively higher financial burden imposed on Ugandan citizens seeking ID replacements. This disparity is a critical concern considering the socio-economic challenges faced by a considerable portion of the population living below the poverty line and the already marginalized groups within Ugandan society.

C. Privacy Concerns and Data Protection Issues: Identifying Vulnerabilities and Potential Risks

i) Legal and Regulatory Framework

The Registration of Persons Act, 2015 inadequately delineates robust privacy safeguards in the processing of personal data, thus failing to establish efficacious monitoring mechanisms. This deficiency engenders apprehensions regarding the identity of data assessors, the modalities of data storage, and subsequent data utilization, thereby necessitating urgent regulatory scrutiny and rectification.

Conversely, Section 7 of the Data Protection and Privacy Act, 2019 mandates explicit consent from data subjects
prior to the collection or processing of personal data. However, the provision of Section 7(2)(b) confers upon NIRA the authority to collect personal data for the lawful execution of public duties by public entities. Given that such data is frequently shared with both public and private entities, it is imperative for NIRA to disclose to data subjects the identities of entities granted access to their data, as stipulated by Section 13(1)(g) of the Data Protection and Privacy Act, 2019. The absence of a comprehensive published privacy policy within NIRA exacerbates this concern, necessitating urgent attention to ensure compliance with regulatory mandates.

As a result, NIRA must establish robust mechanisms to apprise data subjects adequately. Given the sensitive nature of the information amassed during the registration procedure, the absence of a well-defined, explicit, and informed consent protocol renders applicants vulnerable to potential misuse both by governmental entities and private enterprises.

Previous reports issued by Unwanted Witness and more recently in our Privacy Score Card Report, have underscored NIRA’s deficiency in implementing privacy safeguards, NIRA’s lack of a published privacy policy and its subpar performance across various metrics.

The lack of responsiveness to correspondence, exemplified by our letter dated March 5, 2024, regarding the aforementioned concerns, heighten apprehensions surrounding NIRA’s compliance with regulatory standards and its capacity to safeguard the privacy rights of individuals.

Since the Data Protection Act was enacted much later (2019) with elaboration on concepts of personal data and sensitive data among other things, the question to ask is how easily can the Data Protection Act be applied to the Registration of Persons Act?

A notable aspect is Section 65 of the Act, 2015, which enumerates various purposes for utilizing the data in the register. Section 65(1)(h) permits the utilization of register information for law enforcement reasons. While some of these intentions, like national security and law enforcement, appear reasonable, the inclusion of “any other purpose” raises apprehensions about the potential arbitrary or excessive exploitation of personal data without appropriate constraints or safeguards. It is crucial to institute clear safeguards to safeguard individuals’ privacy rights and to forestall the arbitrary or abusive use of personal data.

There is an urgent imperative to re-evaluate the data collection practices of NIRA. This encompasses addressing deficient data protection guidelines, the absence of robust consent mechanisms, and the potential misapplication of data. This reassessment is essential to augment transparency and fortify oversight in the safeguarding of individuals’ personal data while simultaneously upholding the fundamental right to privacy.

### ii) Technological Challenges

Gaps exist in ensuring the reliability and resilience of the technological infrastructure supporting the ID system to prevent system failures, hacking, or cyberattacks. The 2022 Auditor General’s report highlighted significant shortcomings in the existing privacy safeguards within the current ID system. One conspicuous concern pertains to the system’s maintenance and updates, which were neglected due to the absence of a documented plan and budget constraints. This neglect directly impacts the system’s reliability and functionality. Specifically, outdated hardware becomes less compatible with newer security measures and technologies, thereby exposing the system to evolving threats.

### iii) Privacy and Data Security

Ensuring that personal data is securely stored, protected from unauthorized access or misuse, and that stringent protocols are in place to safeguard individuals’ privacy. Section 55(1) of the Registration of Persons Act, 2015 lacks the essential concept of data minimization, which involves collecting and processing the least personal data needed for a specific purpose. On the contrary, the provision requires the collection of a wide range of personal and sensitive data, comprising ethnicity, tribal affiliation, and biometrics, without a clear justification. This substantial collection of data places NIRA with a huge burden of safeguarding it. In view of the foregoing, data minimality is crucial for privacy protection ably provided for in Section 14 of the DPPA as it aims at reducing risks linked to breaches, profiling, and misuse.

---

106 The Data Protection Act (n 31 above), Section 7 (1).
Whereas it is a principle contained in the later-enacted Data Protection Act; and typically, legislation on national registers globally preceeds data protection laws, the question is whether the Data Protection Act can read alongside the Registration of Persons Act. Ignoring this principle raises concerns about privacy violations, as personal data is collected without considering the necessity aspect.

**iv) Reliability and Accuracy**

Ensuring the accuracy of data and preventing errors that might lead to identity theft, fraud, or mistaken identity. As of June 2022, ID cards, approximately 1,648,981, were left uncollected. More worrisome is the fact that 96% of these unissued IDs had not been collected for over six months, with some remaining uncollected for over five years.

This predicament not only results in wastage of resources but also highlights inefficiencies in the system’s administration and distribution. The extended period of non-collection raises questions about data management practices and citizen information protection. These unissued IDs represent a potential risk of privacy as they contain sensitive data that could be misused if they were to fall into the wrong hands.

**v) Ethical Use of Data**

Concerns about how collected data will be used and whether it aligns with ethical principles, including potential misuse or surveillance. The ID system is highly centralized in nature which could enable mass surveillance. Equally, the system in its design, collects and stores large amounts of personal data without sufficient justification nor safeguards for ensuring data security. There is a risk that government or other entities could misuse the data collected for surveillance purposes. Worth noting, NIRA has never conducted a Data Protection Impact Assessment as per the Data Protection and Privacy Regulations nor does it have a noticeable privacy policy in place. Addressing these ethical concerns requires careful planning, robust legal frameworks, and ongoing oversight to ensure that the National ID system respects individual rights and contributes positively to society.

### IV. Introducing the New Generation ID System

**A. Overview of the features and benefits of the new ID system**

In 2022, the Minister of State for Internal Affairs, while justifying the basis for mass renewal, reported to Parliament on the impending expiration of the first batch of National ID cards originally issued between 2014 and 2015. These cards had deteriorated due to the substandard quality of their Polycarbonate material. In the new exercise, the government also disclosed its intentions to incorporate additional biometrics into the National Identity Card system, potentially expanding its surveillance capabilities.

Building on previous efforts, the government announced an expensive upgrade to the National Identity Card system, which is set to commence in June 2024 at a cost of Sh300 billion. This project shall be executed through public-private partnership between the Government of Uganda (51%) and a German firm Veridos (49%). The ambitious project aims to renew and enroll all citizens of the country, ostensibly in line with the government’s broader Digital Transformation program and its commitment to leveraging Information and Communication Technology (ICT) and digital services.

---

110 Report of the Auditor General on the Financial Statements of the National Identification and Registration Authority for the year ended 30th June 2022, p10
111. Report of the Auditor General on the Financial Statements of the National Identification and Registration Authority for the year ended 30th June 2022, p6
112 Section 79 of the Registration of Persons, Act 2015.
116 ibid
The introduction of the new identity, detectable under Ultraviolet (UV) light, while touted as a security measure, raises concerns about the card's potential surveillance capabilities. These UV-detectable features could be exploited for monitoring and tracking individuals without their consent. This could result in exclusion or discrimination against individuals who value their privacy and may choose not to use the ID card if they believe it compromises their personal information or activities.

On the functional side, the new card system seeks to emphasize data privacy and protection, supposedly allowing cardholders to control their information. The integration of Public Key Infrastructure (PKI) is presented as a safeguard for online transactions, but there are valid concerns about how this might affect individuals’ privacy. The inclusion of a 2D barcode containing ISO Standard biometric features, readable only by authorized organizations, raises questions about who these authorized organizations are – public or private and the potential for abuse.

B. Cost, Exclusion, Privacy and Data Protection Considerations in the New Generation ID

The introduction of Uganda’s New Generation National ID Project brings transformative potential but is marred by significant challenges spilling over from the current ID system and sustainability concerns as already highlighted above. These are further examined below in the context of the next generation ID;

**Exclusionary and privacy concerns**

The government’s efforts to modernize identification and registration systems may ostensibly promise improved public services, but void of human rights safeguards coupled with challenges around sustainability. While the new ID system introduces the capturing of more biometrics, authorities are not willing to undertake a Data Protection Impact Assessment (DPIA) throughout the mass enrollment exercise. The DPIA helps to identify risks arising out of the processing of personal data and to minimize these risks as far as and as early as possible equally provided for by the Data Protection and Privacy Regulations.

Equally, the new generation ID system is embedded with features as discussed above and this begets the question as to whether these extra features are necessary and in excess of what is required as provided in Section 14 of the DPPA. A lot is collected compared to the ID systems in India and Tanzania were the data collected focuses on four areas.

In the realm of digital rights, organizations like Unwanted Witness have repeatedly sounded the alarm over the potential for mass surveillance through the National ID system. It’s evident that the government’s pursuit of data collection as per the legislation in place in the absence of adequate safeguards heightens the potential for misusing collected personal data.

The use of advanced biometric technologies raises ethical dilemmas, with surveillance and misuse potential being very real threats. The question of striking a balance between security and individual rights remains unanswered. Moreover, achieving interoperability with existing government systems and databases is a daunting task, and inadequate public awareness and education about the project’s implications could lead to skepticism and resistance.

---

123 Ibid same as above n(109) Regulation 12.
Financial Accessibility

Financial accessibility which remains as a glaring issue, as the project’s costs could disproportionately affect marginalized groups, exacerbating inequalities as discussed in earlier sections of the paper. As already observed, while NIRA in its form fees still indicates UGX shs. 50,000/- for renewal, its FAQs provides for free ID renewal. Individuals however, will still be required to pay an exorbitant fee of UGX shs 50,000/= (Fifty Thousand Uganda Shillings Only—approximately $13.75 USD), for replacement of identity cards placing an undue burden on those living below the poverty line of $1.77 per person/day.

Sustainability concerns

Financial and operational sustainability without compromising accessibility is one of the principles for building a sound ID system. The New Generation ID project is primarily funded by government of Uganda budget. It is scheduled to commence with an allocation of UGX shs.300Bn in FY 2023/24 through a supplementary budget. NIRA planned to commence the mass enrollment exercise of National IDs in January 2023 while renewals are scheduled to start on 1st June, 2024 up to June 2025, targeting 17.2 million citizens who have never been registered and 20 million Ugandans who wish to renew their National IDs. Notwithstanding Cabinet approval the budget, the requisite funds were not provided in the 2023/24 financial year budget as envisaged. Consequently, this has affected the timely roll out of the project by NIRA to renewal of National IDs and enrolment of new Ugandans. Yet, a majority of the current National IDs are set to expire in August 2024.

Additionally, the move by the government through the amendment of the National Citizenship and Immigration Control Regulations requiring citizens to access IDs at a fee -UGX shs.50,000/- as already highlighted, is exorbitant and places undue burden for those living below the poverty line. Addressing funding and maintenance questions is integral to the long-term success and sustainability of National ID systems. Governments need to adopt strategic financial planning, engage in transparent governance practices, and explore innovative funding models to ensure these systems meet evolving needs over time.

Equally, the lack of robust technological infrastructure in remote areas further complicates matters, leaving many without access to essential services. Registration is not fully digitalized and presents concerns in respect of costs related to paperwork as well as security of the system. Despite the existing legal frame as discussed previously above and enabling the NID system, it is not adequately supportive which is critical to NID system sustainability.

Unlimited Data Collection

Equally is the vulnerability of collected personal data, with the looming threat of data breaches and unauthorized access. Section 55(1) of the RoPA mandates an extensive and invasive collection of personal information during the registration process, as outlined in Schedule 3. While this information is claimed to be necessary, it presents a serious challenge to human rights and data protection principles. The comprehensive list includes not only basic personal details but also highly sensitive data such as biometric information and tax identification numbers. This overreach in data collection raises significant concerns about privacy and the potential for misuse or abuse of personal information. It seems to disregard the principle of data minimization as provided for under the DPPA, which advocates for limiting the collection of sensitive data to what is strictly necessary for the intended purpose.

The burden imposed on NIRA for managing and securing this vast amount of data further complicates the human rights landscape, potentially leading to data breaches and infringements on individuals’ right to privacy.

---

129 2019/20 Household survey.
132 Section 55(1) of the Registration of Persons Act, 2015.
133 Schedule 3 of the Registration of Persons Act, 2015.
134 Guiding Principles of Identification (n 115 above).
Comparing with neighbouring countries like India, the NID system-Aadhaar among other things is designed to capture four (4) pieces of personal information namely: mandatory demographic information, optional demographic information, details of parents or legal guardian and biometric information.\(^{135}\)

**Design**

The new National ID system in Uganda, despite its purported inclusivity-focused design, brings forth a plethora of human rights concerns. While the incorporation of biometric elements like iris scanning and facial images may be aimed at accommodating persons with disabilities and the elderly, it introduces significant privacy and security risks. The collection and storage of such sensitive biometric data open the door to potential breaches and misuse, highlighting a blatant disregard for individuals’ privacy.

Although Optical Variable Ink is touted as a measure to prevent imitation, its actual effectiveness against sophisticated forgery techniques remains uncertain. Moreover, the tactile feature designed to assist those with sight challenges may inadvertently expose their vulnerability, making them potential targets for identity theft.

In the pursuit of a discrimination-free identification system, it seems that crucial considerations regarding data protection, accessibility, and security have been sidelined, potentially compromising the overall integrity and user safety of the system. Even the security attributes of the ID card, such as Optical Variable Ink and UV verification, while aimed at countering counterfeiting, raise concerns about personal data exposure.

The inclusion of a 2D barcode with ISO Standard biometric features, accessible only by authorized entities, raises questions about the identity of these organizations and the potential for misuse of the data they can access. The verification app provided by NIRA similarly fails to provide clear assurances about the owner’s privacy.

In sum, while Uganda’s new National ID system introduces security measures and enhanced functionality, the vague definition of “biometric” and the potential for privacy infringements under certain regulations underscore the critical need for robust safeguards and a careful balance between security and privacy to protect individuals’ rights and data.

**Cost of replacement in the new generation ID system**

Whereas ID card renewal fee is currently waived and making it free for all, the legal reality presents citizens seeking replacements with having to part with UGX shs. 50,000/- ($13.78) or 200,000/- ($52.9), is quite high compared to other countries as discussed above. This replacement fee stipulated in Schedule A of the 2015 Regulations raises questions about accessibility, particularly for those who may already face financial constraints.\(^{136}\) Furthermore, NIRA’s provision of express services for expedited card issuance, which may come at an additional cost, adds to the financial burden for applicants.

On top of these monetary concerns, Regulation 23 in the Registration of Persons Regulations SI 67 of 2015 introduces punitive fines for individuals who fail to renew their national ID, with the potential for a maximum daily penalty of 40,000/=, aiming more at punishment than encouraging compliance. This punitive approach exacerbates the marginalization of vulnerable individuals and contravenes the principles of identification that emphasize that costs should never be a barrier to obtaining identity credentials required to fulfill rights or access essential services and entitlements.\(^{137}\)

Despite the evolution of Uganda’s New Generation National ID, it is still encumbered by challenges that could potentially marginalize vulnerable populations and result in significant violations of privacy and human rights. To ensure a fair and unbiased implementation of the project, it is imperative for the government to take immediate and transparent action to address these concerns.

---


\(^{137}\) Guiding Principles for Identification (n109 above), Principle 2.
V. Conclusion

The introduction of Uganda’s new National ID system may highlight progress in security and functionality, but it also introduces a host of pressing human rights concerns, reminiscent of the issues that plagued the previous system. The incorporation of sensitive biometric data serves as a stark reminder of the critical need to protect privacy and uphold data protection principles. However, the current system lacks a coherent approach, leaving it vulnerable to potential abuses. A delicate balance must be struck between inclusivity, privacy, minimal data collection, robust security, transparency, informed consent, and vigilant oversight to fortify the system against the looming human rights challenges it presents. Achieving this equilibrium is not only pivotal but imperative to ensure that Uganda’s citizens can harness the benefits of technological advancements without forfeiting their fundamental rights and privacy. The existing exemptions for non-residents and refugees, also reflect a need for balance between inclusion and control.

In light of data security concerns, the Data Protection and Privacy Regulations for 2021 mandate NIRA to conduct a pre-assessment of procedures and their potential impact on data protection and privacy prior to embarking on mass renewal and enrollment activities. 138

The 2022 Auditor General report’s findings shed light on NIRA’s inadequacies in formulating a data migration strategy, 139 exposing glaring vulnerabilities that jeopardize the privacy and security of individuals’ data. 440 This revelation underscores the pressing need for a Data Protection Impact Assessment (DPIA). As per the report, NIRA’s lack of a comprehensive strategy has left data exposed to security breaches, putting individuals’ data and privacy rights at risk.

Consequently, it is essential for NIRA to initiate a DPIA before proceeding with mass enrollment and renewal for the new generation ID. This exercise is proposed to serve as a means to improve data protection measures, maintain data integrity, and ostensibly protect individuals’ privacy rights through transparent and effective data handling practices. The essence of conducting a DPIA, as claimed, is to identify and mitigate potential risks to individual rights and freedoms concerning their personal data, ostensibly ensuring a proactive approach to data protection. Through systematic assessment, NIRA aims to identify risks associated with data collection and processing and develop mitigation measures to safeguard personal data, though the actual effectiveness of these measures remains to be seen.

VI. Recommendations

This section sets out to highlight appropriate recommendations made to key stakeholders – state and non-state actors for addressing cost, exclusion and privacy concerns in the New Generation ID. These include the following;

Recommendations to Parliament

Parliament is mandated to make laws pertaining to any matter for the systematic functioning, and effective administration of Uganda. Additionally, it is obligated to safeguard the integrity of this Constitution and advance the principles of democratic governance within Uganda. 441 To its efficient discharge of its functions, it has a number of committees 442 and the ones relevant to the National ID include: The Committee on Equal Opportunities; the Committee on Human Rights, the Committee on Information, Communication Technology and National Guidance; the Committee on Legal and Parliamentary Affairs; the Committee on Gender, Labour and Social Development; the Committee on Finance, Planning and Economic Development; and Budget Committee. Parliament should:

1. Review and amend Section 76(a) and Section 64(5) of the Registration of Persons Act to ensure that penalties for non-registration and failure to update information are proportionate and considerate of vulnerable groups. This would prevent the imposition of harsh penalties on marginalized individuals who may face difficulties in complying with the law and updating their information in a timely manner.

2. Amend Section 55(1) of the Registration of Act, 2015 and the Schedule 3 to the Act to advance data minimization and privacy by limiting the unnecessary collection of person data during the registration process.

141 Article 79(1) & (3) of the Constitution of the Republic of Uganda, 1995, as amended.
3. Amend Section 65 of the Act to provide a more precise and well-defined list of permissible purposes for which data in the register can be used. While the inclusion of national security and law enforcement purposes is crucial, the current phrasing of “any other purpose” is overly broad and could potentially lead to the misuse of personal data.

4. Amend Section 66 of the Act not to make the use of identification cards a prerequisite for accessing public/basic essential services and provide for other forms of identifications to minimize exclusion to ensure no one is left behind and as the ID infrastructure evolves to universal access.

5. Allocate resources to improve the efficiency of NIRA service units, making them more accessible for elderly and disabled individuals and Persons with Disabilities (PWDs) during enrollment. This would enhance the accessibility and usability of the ID application process for all citizens, ensuring that technical challenges do not hinder vulnerable groups from obtaining IDs.

6. Revise the data collection requirements in Schedule 3 to limit the collection of sensitive personal information to what is strictly necessary for identification purposes. By minimizing data collection, NIRA can reduce the burden of managing and securing vast amounts of data and uphold individuals’ privacy rights.

7. Reforms in respect of collection, storage, and sharing of data, to include sensitive biometric data with robust safeguards against unauthorized access and misuse to enhance citizens’ trust in the ID system.

8. Collaborate with relevant international organizations and human rights groups to develop guidelines and best practices for inclusion of non-nationals in the identification system.

9. Revise the Registration of Persons Act to include provisions that allow for alternative forms of identification for accessing essential services, ensuring that no one is unjustly excluded.

Recommendations to Ministry of Internal Affairs

1. Evoke the Minister’s powers under Section 8 of the Registration of Persons Act, 2015, and direct the reduction of the cost of replacement fee structure substantially to at least $4 US dollars or exemptions for marginalized and low-income individuals. This approach would alleviate the financial burden on disadvantaged groups, promoting inclusivity and ensuring that replacement fees do not disproportionately affect those struggling with poverty.

2. Introduce provisions for alternative identification options, such as temporary IDs, for individuals facing challenges in obtaining a National ID also known as Ndaga Muntu to prevent exclusion from accessing essential services.

3. Invest in modernizing and expanding NIRA’s infrastructure, including upgrading hardware and software systems, as well as expanding the network of service units to ensure more equitable access for citizens across different regions. This will improve the efficiency of data processing and decrease processing times.

4. Review existing regulations to ensure that non-nationals, including refugees and asylum seekers, are not subject to discriminatory practices. Simplify and make the identification process more accessible for this group.

Recommendations to the National Identification and Registration Authority

1. Undertaken a comprehensive Data Protection Impact Assessment as mandated by Regulation 12 of the Data Protection and Privacy Regulations, 2021 to systematically evaluate potential risks and impact on individuals’ privacy and data security before implementation of any significant changes/expansions to the National ID system. Regular updates and reviews of the DPIA should be undertaken to address emerging risks and evolving privacy concerns.

2. Publish a Privacy Policy to ensure alignment with Sections 3(a), (b), (e) and (f) of the Data Protection and Privacy Act, 2015.

3. Consider implementing tiered fee structures where individuals living below the poverty line, the elderly, and youth have reduced replacement fees or are exempted from fees altogether.

143 Section 84 of the Registration of Persons Act, 2015 provides that the Minister may, by statutory instrument, amend the Schedules to the Act and the same shall be laid before Parliament.
4. Reevaluate the severity of penalties for non-registration and failure to update information, ensuring they are proportionate and don’t disproportionately impact marginalized groups.

5. Implement automated feedback mechanisms to notify applicants of errors or issues in their applications promptly and receive corrected information to reduce on delays in processing and inaccuracies.

6. Implement a comprehensive data migration strategy that prioritizes data security and includes transparent data protection regulations in line with the DPPA and DPPR.

7. Provide clear guidelines for data sharing with appropriate consent mechanisms to ensure citizens have control over their data.

8. Implement efficient data management practices to prevent the accumulation of uncollected ID cards. This will safeguard citizens’ sensitive data and prevent potential breaches.

9. Implement robust security measures to protect biometric data from unauthorized access and potential misuse. Regularly audit and update security protocols to address emerging threats.

10. Provide specialized training for NIRA personnel to handle biometric data from vulnerable groups like the elderly and Persons with Disabilities.

11. Operationalization of the complaints handling mechanism, to receive and investigate complaints

12. Undertake audits and evaluation of its own systems.

**Recommendations to the Personal Data and Protection Office**

1. Provide guidance to NIRA about their obligations and responsibilities while collecting data,

2. Supervise NIRA and monitor them on all matters in relation to data collection,

3. Collaborate with NIRA to reassess the data collection process, with a focus on collecting only necessary information to fulfill identification requirements, thereby reducing the burden on data management.

4. Conduct audits in NIRA’s data collection operations to ensure compliance with the data protection laws of Uganda

5. Collaborate with relevant stakeholders to draft comprehensive data protection regulations that clearly define how citizens’ data will be collected, stored, and shared, while ensuring robust security measures.

**Recommendations to the Uganda Law Reform Commission**

The Uganda Law Reform Commission (ULRC) is a Constitutional body established by Article 248 of the 1995 Constitution and operationalized by the ULRC Act, Cap 25 2019 with a mandate to study and keep Ugandan Laws under constant review. To this end, ULRC should:

1. Revisit the penalties for non-registration and failure to update information. Penalties should be proportionate and reasonable, ensuring that vulnerable groups are not unfairly punished.

2. Recommend amending the Registration of Persons Act to provide a clear pathway for non-nationals, including refugees and asylum seekers, to access identification services without discriminatory charges.

3. Propose for clear, legitimate interest and informed consent mechanisms for data collection and usage for citizens to have control over how their data is utilized, including options for opting out.

4. Recommend a review of the data collection requirements, aligning them with best practices in data minimization. Collect only the information necessary for identification and essential services.

5. Recommend a strategy to address the issue of uncollected IDs, including regular reminders, better tracking, and secure destruction of uncollected cards after a specified period.

6. Revise Schedule 3 of ROPA to ensure that only essential information is collected, minimizing the burden on NIRA and enhancing data security.

7. Propose robust measures to secure biometric data, including encryption, secure storage, and strict access controls. Consider involving independent experts to audit the security of biometric data.
Recommendations to Civil Society Organisations

1. Engage in advocacy efforts to reduce the renewal fees for national IDs. By working with relevant authorities and using data to demonstrate the impact of these fees on marginalized groups, CSOs can push for policy changes that make ID renewal more affordable.

2. Advocate for enhancement of rights of citizens including clarity on consent requirements, data usage limitations and penalties for data misuse in the DPPA, ROPA and other key legislation.

3. Monitor compliance with DPPA including other relevant legislation and ensure accountability.

4. Refer and submit complaints regarding data breaches for management and appropriate resolution.

5. Lead public awareness campaigns to educate and empower citizens to be vigilant about their rights regarding personal data and privacy and hold authorities accountable.

6. Undertake initiatives in collaboration with legal and data experts to research in areas of concern including inclusivity and control and advocate for reforms. Engage in dialogues with policy makers to advocate for policy changes that promote inclusivity and fairness in the ID renewal process.

7. Engage with policymakers to ensure that data collection practices align with privacy principles on identification and limit the collection of sensitive personal information to promote data minimization.

8. Collaborate with independent auditors to assess data management practices within NIRA. Continuously monitor the implementation of privacy safeguards in the new ID system.
Past works on ID