June 2025 Issue

THE DIGITAL AGENDA Insights

Monthly Newsletter

IN THIS ISSUE

Digital ID

Faith & Religion in the Digital Era

Tech Should Serve Not Control

Welcome to The Digital Agenda Insights Monthly Newsletter

Governments across the world are rapidly rolling out national identity systems as part of a broader Global Digital Agenda. What began as simple ID cards has now evolved into the mass collection of deeply personal and permanent biometric data. Many countries have moved beyond fingerprints to high-resolution iris scans, justified under the guise of "unique identification."

At the same time, governments are pushing Central Bank Digital Currencies (CBDCs), with the National Identification Number (NIN) becoming the gateway to all essential services. This forms a tightly woven system designed to enable constant surveillance, limit personal freedom, and centralise control, framed as innovation and security.

At the Digital Agenda Forum, we believe that the **true digital agenda** should be one that harnesses technology to serve the God-ordained good, not become a tool of draconian control. It should uphold values and human dignity, rather than erode them.

Our Core Values

S **Stewardship**

P **Purpose**

A **Authenticity**

D **Dignity**

The Digital Agenda Insights Newsletter exists as a necessary interruption to the noise. In a world racing to digitise at any cost, we pause to ask the harder questions. Whose interests are being served? What freedoms are being traded? Through sharp commentary and clear-eyed analysis, we invite you to see beyond the surface of shiny tech and get into the deeper struggles for privacy, dignity, and democratic control. This newsletter is a call to stay awake, stay informed, and stay human.

We value innovation and recognise how technology can ease life. That's why we also use this platform to spotlight technologies that drive progress without intruding on or controlling humanity.

Come with us to navigate these pressing issues through the pages of this newsletter.

If you like our work, don't hesitate to partner with us.

Warm regards,

Lilian Agaba Nabwebale

For **Digital Agenda Forum**

Policy Watch: Mass National ID Renewal and Personal Data Protection Debate Deepens

Digital Agenda Forum Raises Red Flag on the Ugandan Mass National ID Renewal Exercise

On 16th June 2025, the Digital Agenda Forum issued an open letter to the Personal Data Protection Office (PDPO) raising serious concerns about the ongoing mass renewal of National ID cards in Uganda. The letter questioned the scope and sensitivity of personal data collected, the lack of a published Data Protection Impact Assessment (DPIA), the increasing dependency on the National Identification Number (NIN) across essential services, and opaque data sharing agreements with third parties such as banks and telecom operators.

PDPO and NIRA Issue Joint Response

In response, PDPO issued a formal reply on 26th June 2025, incorporating explanations from the National Identification and Registration Authority (NIRA). The response defended the biometric data collection, ***including iris scans***, as lawful, and justified it by referencing international best practices (e.g., World Bank's ID4D Initiative and ICAO standards). It also acknowledged that while a full DPIA is not yet complete, foundational safeguards are being implemented. PDPO further committed to auditing NIRA and issuing future guidance on NIN integration.

Analysis of the PDPO–NIRA Response Highlights Gaps and Contradictions

While the response acknowledges concerns and outlines steps taken, the analysis of this response notes:

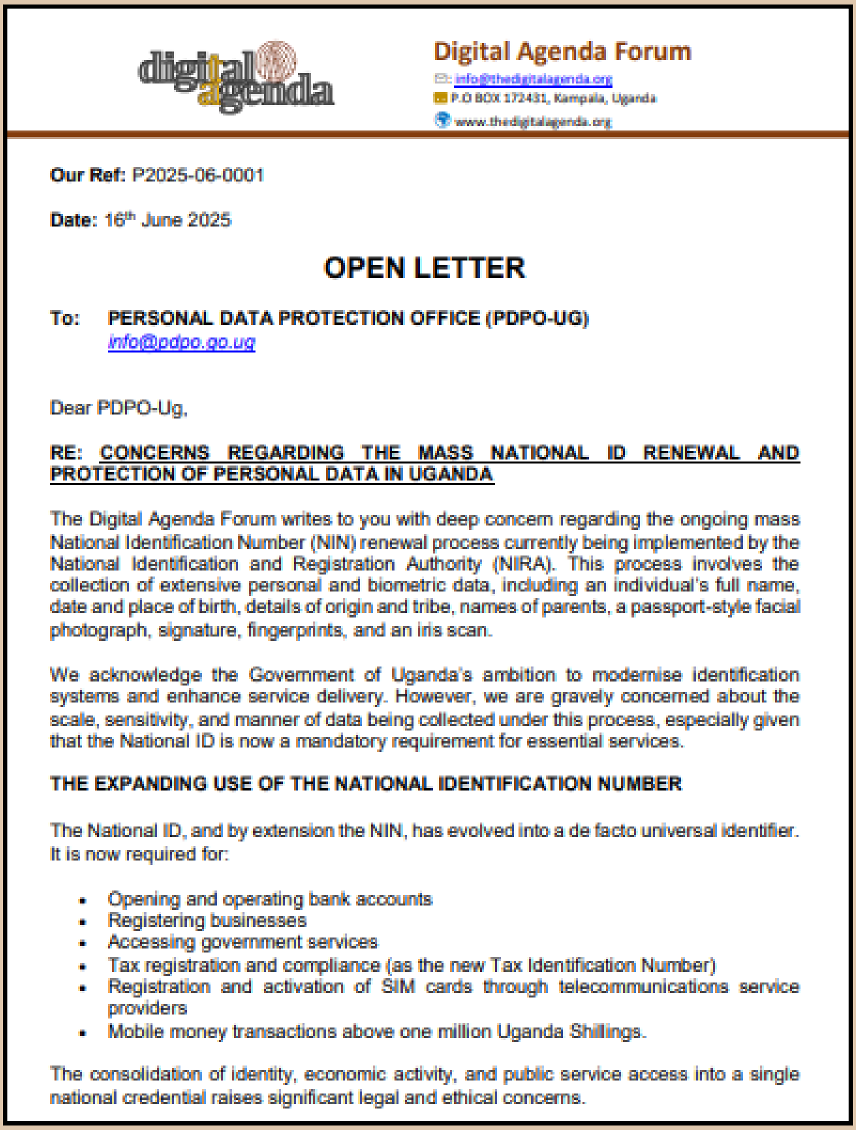
- Lack of transparency around data sharing agreements. At the least, NIRA would have provided a snippet of the key provisions covered in the data sharing agreements.
- Unclear timeline or content for the DPIA hence no basis for expanding biometric data collection to mass iris scanning.
- Absence of independent oversight or public accountability.
- A contradiction between NIRA's court position that Uganda's National ID is not a ***Digital ID*** and its use of digital ID frameworks (i.e. ID4D and ICAO) to justify expansive biometric data collection

The Forum reiterates that referencing global best practices without demonstrating local risk assessments and proportionality undermines public trust.

Why It Matters!

With the National ID serving as a gatekeeper to public services, it is crucial that data collection and processing respect rights. Thus, a continued call for greater transparency, proportionality, and accountability.

Open Letter to the Personal Data Protection Office (PDPO-UG) on Concerns Regarding the Mass National ID Renewal and Personal Data Risks in Uganda



Digital Agenda Forum
info@thedigitalagenda.org
P.O BOX 172431, Kampala, Uganda
www.thedigitalagenda.org

Our Ref: P2025-06-0001

Date: 16th June 2025

OPEN LETTER

To: **PERSONAL DATA PROTECTION OFFICE (PDPO-UG)**
info@pdpo.go.ug

Dear PDPO-Ug,

RE: CONCERNS REGARDING THE MASS NATIONAL ID RENEWAL AND PROTECTION OF PERSONAL DATA IN UGANDA

The Digital Agenda Forum writes to you with deep concern regarding the ongoing mass National Identification Number (NIN) renewal process currently being implemented by the National Identification and Registration Authority (NIRA). This process involves the collection of extensive personal and biometric data, including an individual's full name, date and place of birth, details of origin and tribe, names of parents, a passport-style facial photograph, signature, fingerprints, and an iris scan.

We acknowledge the Government of Uganda's ambition to modernise identification systems and enhance service delivery. However, we are gravely concerned about the scale, sensitivity, and manner of data being collected under this process, especially given that the National ID is now a mandatory requirement for essential services.

THE EXPANDING USE OF THE NATIONAL IDENTIFICATION NUMBER

The National ID, and by extension the NIN, has evolved into a de facto universal identifier. It is now required for:

- Opening and operating bank accounts
- Registering businesses
- Accessing government services
- Tax registration and compliance (as the new Tax Identification Number)
- Registration and activation of SIM cards through telecommunications service providers
- Mobile money transactions above one million Uganda Shillings.

The consolidation of identity, economic activity, and public service access into a single national credential raises significant legal and ethical concerns.

In an open letter dated 16th June 2025 (Reference: P2025-06-0001), the Digital Agenda Forum wrote to the Personal Data Protection Office (PDPO-Ug), expressing concerns over the mass National Identification renewal and the protection of personal data in Uganda, currently being implemented by the National Identification and Registration Authority (NIRA).

Find the full four page letter at,

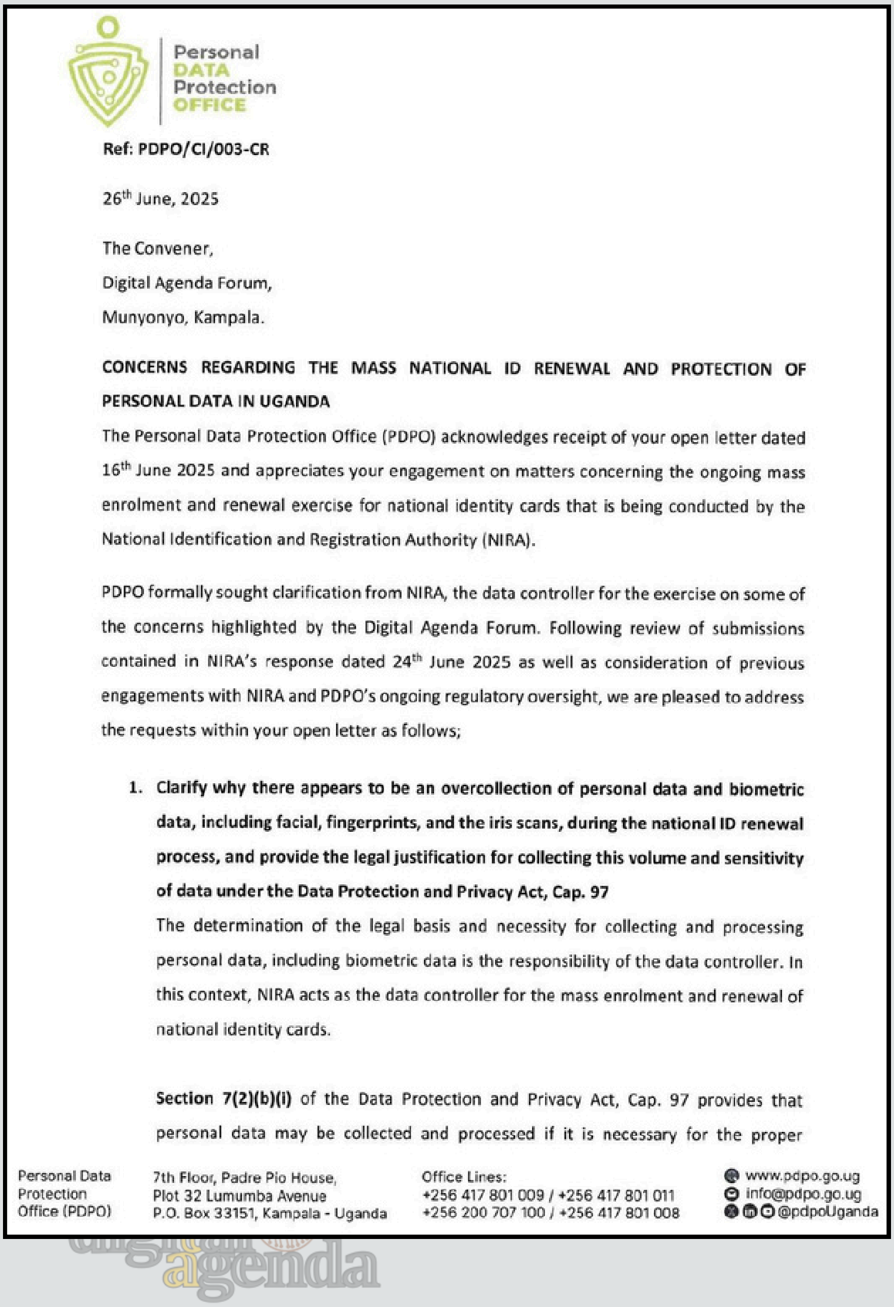
https://thedigitalagenda.org/wp-content/uploads/2025/06/Open-Letter-to-PDPO-on-Biometric-data-in-the-NIN.pdf

<u>What is at Stake?</u>

The National ID system centralises vast amounts of personal data. Without strict privacy safeguards, it risks becoming a tool for surveillance and misuse, rather than a means to serve and protect citizens.

Official response from PDPO-Ug to Digital Agenda Forum's Concerns Regarding the Mass National ID Renewal and Personal Data Risks in Uganda

In a letter dated 26th June 2025 (Reference PDPO/CI/003-CR), the Personal Data Protection Office (PDPO-Ug), responded to the concerns raised by the Digital Agenda Forum regarding the mass National Identification renewal and the protection of personal data by the National Identification and Registration Authority (NIRA).



Personal
DATA
Protection
OFFICE

Ref: PDPO/CI/003-CR

26th June, 2025

The Convener,
Digital Agenda Forum,
Munyonyo, Kampala.

CONCERNS REGARDING THE MASS NATIONAL ID RENEWAL AND PROTECTION OF PERSONAL DATA IN UGANDA

The Personal Data Protection Office (PDPO) acknowledges receipt of your open letter dated 16th June 2025 and appreciates your engagement on matters concerning the ongoing mass enrolment and renewal exercise for national identity cards that is being conducted by the National Identification and Registration Authority (NIRA).

PDPO formally sought clarification from NIRA, the data controller for the exercise on some of the concerns highlighted by the Digital Agenda Forum. Following review of submissions contained in NIRA's response dated 24th June 2025 as well as consideration of previous engagements with NIRA and PDPO's ongoing regulatory oversight, we are pleased to address the requests within your open letter as follows;

1. **Clarify why there appears to be an overcollection of personal data and biometric data, including facial, fingerprints, and the iris scans, during the national ID renewal process, and provide the legal justification for collecting this volume and sensitivity of data under the Data Protection and Privacy Act, Cap. 97**

   The determination of the legal basis and necessity for collecting and processing personal data, including biometric data is the responsibility of the data controller. In this context, NIRA acts as the data controller for the mass enrolment and renewal of national identity cards.

   Section 7(2)(b)(I) of the Data Protection and Privacy Act, Cap. 97 provides that personal data may be collected and processed if it is necessary for the proper

Personal Data
Protection
Office (PDPO)

7th Floor, Padre Pio House,
Plot 32 Lumumba Avenue
P.O. Box 33151, Kampala - Uganda

Office Lines:
+256 417 801 009 / +256 417 801 011
+256 200 707 100 / +256 417 801 008

www.pdpo.go.ug
info@pdpo.go.ug
@pdpoUganda

Beyond Identification!

When the National ID becomes a gateway to essential services, protecting the personal data it collects is not optional—it's a matter of rights, trust, and democratic accountability.

Find the full 21 page letter at,

https://pdpo.go.ug/media//2025/06/Response-to-Digital-Agenda-Forum-NIRA-June-2025-1_compressed.pdf

Gaps Identified in PDPO-Ug and NIRA Response to Concerns raised by the Digital Agenda Forum regarding the Mass National ID Renewal and Data Protection in Uganda

By Digital Agenda Forum

Introduction

This analysis reviews the joint responses issued by the Personal Data Protection Office (PDPO-Ug) and the National Identification and Registration Authority (NIRA) to concerns raised in the open letter titled "Open Letter to the Personal Data Protection Office (PDPO-Ug) on Concerns Regarding the Mass National ID Renewal and Personal Data Risks in Uganda."

While we acknowledge the engagement and efforts by both institutions to address the issues raised, we find several responses either incomplete, unsatisfactory, or lacking in legal, procedural, and rights-based clarity. This submission highlights the key unresolved concerns and identifies critical gaps that must be addressed to ensure Uganda’s National ID system upholds the principles of transparency, proportionality, inclusion, and accountability.

1. Legality and Proportionality of Biometric Data Collection

NIRA justifies collecting fingerprints, facial images, and iris scans as lawful under Regulation 15(1)(c) and references international best practices.

Gap: While the legal basis may exist, there is inadequate scrutiny of the necessity and proportionality of collecting such sensitive data, especially iris scans, which are highly intrusive. Legal authorization alone does not substitute for a demonstrated risk-based justification. No evidence has been provided as to why facial and fingerprint data are insufficient or why iris scans are necessary for the entire population.

2. Lack of a Completed and Published Data Protection Impact Assessment (DPIA)

PDPO acknowledges that a DPIA is underway and that only preliminary components have been implemented.

Gap: Without a completed DPIA, there is no transparent, public assessment of the risks posed by this large-scale collection of sensitive personal data. There is also no clear timeline for completion or a commitment to publish the DPIA in full, only a redacted summary is promised. This undermines public oversight.

3. Use of NIN Across Services and Function Creep

NIRA defends the use of the National Identification Number (NIN) across various sectors as a matter of policy and law.

Gap: There is no discussion of consent, opt-out mechanisms, or purpose limitation. The risk of function creep, where NIN use expands beyond original intent, is unaddressed. Surveillance, profiling, and exclusion risks are downplayed. PDPO-Ug merely notes it will issue future guidance, with no timeline or binding framework.

4. Transparency of Data Sharing Agreements

NIRA declines to disclose its data sharing agreements with third parties, citing confidentiality.

Gap: These agreements govern who can access citizens' personal data and under what terms. Their complete opacity undermines public trust. At minimum, a summary of terms, purposes, and parties involved should be publicly disclosed to ensure accountability and prevent misuse.

5. Compliance by Third Parties (Banks, Telecoms, etc.)

PDPO-Ug reports that the majority of third-party institutions are registered and compliant.

Gap: No public list of compliant or non-compliant entities has been provided. Nor is there any indication of enforcement mechanisms for persistent violations. The issue is not only registration but substantive compliance with data protection principles.

6. Transparency and Oversight Mechanisms

PDPO-Ug and NIRA emphasise internal controls, staff training, and audits.

Gap: There is no evidence of independent verification, public audit reports, or accessible redress mechanisms for data subjects. The audit of NIRA remains prospective, not completed.

7. On NIRA's Use of ID4D and ICAO Standards

NIRA references the World Bank's ID4D Initiative and ICAO/ISO standards to justify the breadth of biometric data collected.

a. Misuse of "Best Practices" as Blanket Justification

These international frameworks emphasise:

- Inclusion and proportionality
- Consent and accountability
- Data minimization and legal safeguards

Gap: NIRA uses these sources selectively without demonstrating compliance with the full range of principles they promote. ICAO, moreover, is tailored to travel documents, not foundational national ID systems.

b. No Contextual Relevance to Uganda

Uganda's context, marked by low

digital literacy, vulnerable populations, and limited access to redress mechanisms, requires localized, rights-based adaptation of global standards.

Gap: There is no evidence that NIRA has tailored these standards to local realities, nor that it has engaged in meaningful public consultation or stakeholder engagement.

c. ID4D Cautions Against Overreach

The ID4D Principles specifically caution against:

- Over-reliance on biometrics
- Failure to conduct DPIAs
- Risks of exclusion
- Absence of opt-out mechanisms

Gap: NIRA's reliance on iris scans, the most sensitive biometric, without a published DPIA or public justification is in tension with ID4D guidance, not in alignment with it.

d. Contradiction Between Court Ruling and ID4D Framing

NIRA cites the decision in Initiative for Social and Economic Rights (ISER) & Others v. AG and NIRA (Misc Cause No. 85 of 2022) to support its position. In that ruling, Justice Boniface Wamala held that:

- Uganda's national ID is not exclusionary or discriminatory by design.
- Uganda's ID is not a digital ID, as it does not require real-time electronic authentication for service access.

Implications for ID4D Claims

The ID4D initiative is focused specifically on digital identity systems that:

- Process identity information electronically
- Enable real-time authentication
- Are interoperable across government and private services

Gap: If Uganda's ID is not digital (as ruled), NIRA's use of digital ID frameworks (like ID4D) to justify its current practices is misleading. If the system is digital (as its biometric scope and cross-sector integrations suggest), then the court ruling undermines its legal transparency, and NIRA should fully comply with ID4D principles, including those on rights, redress, and safeguards.

There is a clear inconsistency between:

- What NIRA tells the court (the system is not digital); and
- What it implies to the public and regulators (by citing ID4D and implementing digital ID components)

If NIRA is pursuing a digital ID system, formally or informally, it must not proceed without fulfilment of ID4D principles in both design and practice.

The implied shift toward a digital ID system, whether openly stated or not, raises serious concerns that cannot be ignored.

- NIRA must not proceed under the

of modernization without:

- Public debate and legal mandate for any digital ID framework
- A halt to any data practices lacking a published Data Protection Impact Assessment (DPIA)
- Full disclosure of data sharing arrangements and third-party access
- Independent oversight to prevent abuse and ensure accountability.

**If Uganda's National ID is not a Digital ID, then the justification for intrusive biometrics and ID4D/ICAO references falls apart.
Until these contradictions are resolved, the framework remains legally ambiguous, operationally opaque, and insufficiently accountable to the Ugandan public.**

Visit
https://thedigitalagenda.org/openletters/

BE A PANELIST

Join Our Webinars and Town Hall Panel

Are you an expert or enthusiast in digital technology? The Digital Agenda Forum welcomes knowledgeable individuals **(Technology Experts, Policy Makers, Legal Experts, Regulatory Bodies, Academics and Researchers, Civil Society Representatives, International Organisations, Ethics Experts, Industry Associations and Data Protection Authorities)** to join our panel discussions during our online Webinars and Town Halls. Our focus is on exploring the latest advancements in digital tech, with a key emphasis on digital IDs.
As a panelist, you'll have the opportunity to share your insights, engage with thought leaders, and contribute to shaping a balanced and inclusive digital future.

e-mail: info@thedigitalagenda.org

Digital Agenda Forum Participates in the 24th RNB Live Session held on June 26th, 2025 about the National ID System: Data Protection and Privacy

Lilian Agaba Nabwebale, Chair of the Digital Agenda Forum questioned NIRA's Executive Director on the rationale for mass collection of Special Category Data, particularly iris scans, under the National ID program.

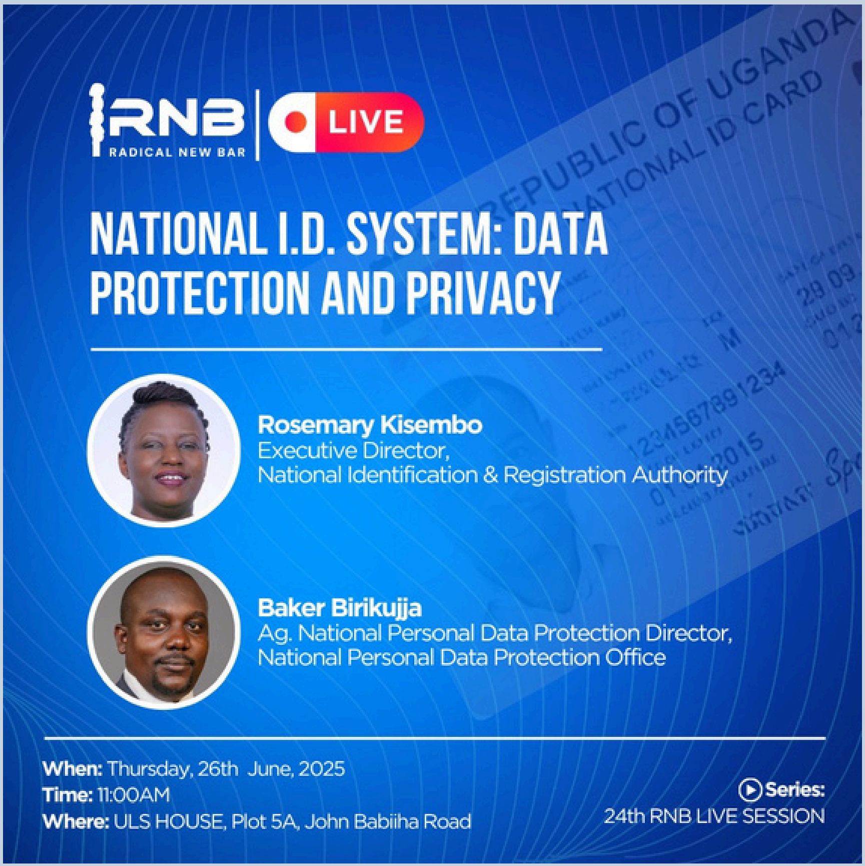
Hosted by the Uganda Law Society (ULS), the *24th Edition of #RNBLive - Press and Public Engagement with the #RadicalNewBar was held at the ULS House. Issue at hand was the National I.D System: Data Protection and Privacy.*

Find the full recording at

https://www.youtube.com/live/QUwmyVulBp8?si=Thk-QxHJx6-og4DN

OR

https://bit.ly/RNB-Live-24


RNB
RADICAL NEW BAR
LIVE
REPUBLIC OF UGANDA
NATIONAL ID CARD

NATIONAL I.D. SYSTEM: DATA PROTECTION AND PRIVACY

Rosemary Kisembo
Executive Director,
National Identification & Registration Authority

Baker Birikujja
Ag. National Personal Data Protection Director,
National Personal Data Protection Office

When: Thursday, 26th June, 2025
Time: 11:00AM
Where: ULS HOUSE, Plot 5A, John Babiiha Road

Series:
24th RNB LIVE SESSION

ISER & ORS V. NIRA

By Digital Agenda Forum

Among the key references cited by NIRA was the High Court decision in ISER & Ors v. NIRA, which it used to legitimize its practices and assert that the Ndaga Muntu system neither constitutes a digital ID nor infringes on constitutional rights.

Below we interrogate the Court's reasoning, highlight its blind spots, and place the decision within a broader national and international context on rights-based identity systems. By unpacking this ruling, we reveal why its use as blanket justification for mass biometric data collection and ID-linked service access is both legally and ethically insufficient.

BRIEF FACTS OF THE CASE

Three civil society organizations—Initiative for Social and Economic Rights (ISER), The Unwanted Witness (U) Ltd, and Health Equity and Policy Initiative Ltd (HEAPI)—filed a public interest petition challenging the implementation of the National Identification and Registration Authority's (NIRA) ID system, colloquially known as "Ndaga Muntu." The applicants alleged that the mandatory requirement of a National ID to access healthcare, education, and social protection services led to exclusion and violated constitutional rights.

LAW CITED

- The Constitution of the Republic of Uganda (Articles 8A, 20, 21, 22, 24, 45).
- The Registration of Persons Act, 2015
- National Identification and Registration Authority (NIRA) regulations
- Data Protection and Privacy Act, 2019

ISSUES RAISED

1. Whether the Ndaga Muntu system constitutes a digital ID with legal implications on rights.
2. Whether denial of access to essential services due to lack of a National ID violates constitutional rights.
3. Whether NIRA's implementation of the ID regime is discriminatory and unconstitutional.
4. Whether the ID system is supported by adequate legal, regulatory, and technological safeguards.

COURT'S RULING ON EACH ISSUE

1. Is Ndaga Muntu a "Digital ID System"?

No. The Court held that the system is not a digital ID, since it "functions primarily offline" and does not deny access based on internet availability.

Implication: Despite its biometric data and central registry, without live-online authentication, it doesn't meet the Court's definition of "digital." This was the central basis for rejecting claims of digital-system harms.

2. Mandatory Use & Claims of Discrimination/Exclusion

The petitioners' claims that requiring

the Ndaga Muntu for SAGE social grants and public health services excludes older persons and women were dismissed.

Reasoning: The Court reasoned that the system itself does not exclude users in absence of internet, and physical card issuance suffices.

3. Is NIRA's implementation of the ID regime discriminatory and unconstitutional?

No. It emphasized that the National ID is merely a means of identification and not a tool of exclusion by design.

The Court noted that individuals are not systematically denied services because of lack of ID unless they fail to comply with legal registration processes.

Implication: The Court rejected arguments that mandatory use of National ID led to unconstitutional exclusion from rights-based services.

4. Is the ID system supported by adequate legal, regulatory, and technological safeguards?

The ID system is legally grounded in the Registration of Persons Act and accompanying regulations. It cited the existence of a complaints mechanism under section 83(1) of ROPA, as well as oversight by the NIRA Board.

On technological safeguards, the Court concluded there was no evidence of system misuse or breach, and since the ID system is not "digital", data protection standards under that category didn't strictly apply.

Implication: The Court held that existing legal and administrative structures were adequate to safeguard users' rights.

Structural Interdict & Declarations of Illegality

The High Court declined to issue a structural interdict or any orders mandating alternative forms of ID. It also declined to declare mandatory ID linkage for services as unconstitutional.

Implication: The petitioners' core reliefs including declaratory relief, alternative documentation, and structural oversight were all denied.

CRITIQUE

a) Unduly Narrow Interpretation

By treating "digital" as solely dependent on internet connectivity, the court ignored key digital components including biometric data, centralized digital registry, and electronic issuance systems, essentially overlooking system architecture and data flows.

b) Comparative Jurisprudence

In India's Aadhaar, courts recognized biometric, centralized databases as constituting a digital ID even where offline authentication was possible. The Supreme Court there invalidated mandatory Aadhaar linkage for welfare services for lack of adequate safeguards (e.g., Justice K.S. Puttaswamy II, 2018).

The EU Court of Justice struck down indiscriminate data retention as disproportionate, emphasizing structural digital capacity and surveillance risk.

Regional Precedents: In Katiba Institute v Huduma Namba (Kenya, 2020), Kenya's High Court halted a similar ID system until safeguards were legislated. The Zimbabwean Constitutional Court has also required identity systems to comply with dignity and inclusion principles.

c) Benchmarks of International Standards

ICCPR Article 17 and UN experts demand system-level safeguards: necessity, proportionality, transparency, oversight.

The Venice Commission recommends robust oversight for ANY centralized, biometric identity system regardless of its surface mode of use.

Minimum Core Obligations under International Law: Under ICESCR General Comment Nos. 3 and 19, Uganda is bound to ensure non-discriminatory access to minimum essential levels of social protection and health. The use of a rigid identification mechanism that excludes vulnerable groups violates these obligations, which are immediate, not subject to progressive realization.

a) Legal & Rights Analysis

The court failed to apply the "systemic digitality" test, instead focusing on physical access trends.
The absence of requirements on judicial oversight, data protection, alternative Ids, and non-discrimination assessments marks a key jurisprudential gap.

Right to an Effective Remedy: While Section 83 of ROPA creates a complaints committee, the judgment failed to examine whether this mechanism is accessible, functional, or widely known to aggrieved citizens. Article 50 of the Constitution guarantees practical, not merely formal, access to justice.

Intersectionality and Vulnerability: The ruling ignored how age, gender, poverty, and rurality intersect to exacerbate exclusion. Article 32(1) mandates affirmative action, which was not applied in assessing the impact of the ID regime on marginalized groups.

Impact on Electoral Participation: The NIRA registry links to the voter roll, raising democratic concerns. Any error in ID issuance can result in disenfranchisement, undermining Articles 1 and 59 of the Constitution and echoing warnings from courts in Ghana and Kenya.

AREAS FOR CONSTITUTIONAL CHALLENGE

1. Violation of Privacy Rights

Constitutional Provisions Infringed include:

Article 27(2): “No person shall be subjected to interference with the privacy of that person’s home, correspondence, communication or other property.”

Article 24: Protection from inhuman and degrading treatment (relevant to data misuse, coercive enrollment, or excessive surveillance).

Article 43(2)(c): Limits state action that violates fundamental rights under the guise of public interest.

Argument: The collection of biometric data without robust legal safeguards (e.g., clear consent protocols, data minimization, independent oversight) constitutes a disproportionate interference with the right to privacy.

2. Equality & Non-Discrimination

Constitutional Provisions Infringed include:

Article 21(1) & (2): Guarantees equality before the law and prohibits discrimination based on age, sex, social or economic standing, etc.

Article 32(1): Requires affirmative action for marginalized groups.
Article 45: Preserves other inherent human rights not explicitly listed.

Argument: Requiring a National ID as a precondition for access to health, education, and social protection has a disproportionate impact on women, the elderly, and rural poor, who face greater barriers to enrollment. Even if neutral in form, such practices amount to indirect (de facto) discrimination.

3. Due Process & Procedural Fairness

Constitutional Provisions Infringed include:

Article 42: Provides the right to just and fair treatment in administrative decisions.

Article 44(c): Due process is non-derogable, even during emergencies.

Article 28(1): Fair hearing in civil and criminal matters, extended by jurisprudence to administrative processes affecting rights.

Argument: Registration of Persons Act, 2015 and its regulations fail to establish clear procedural safeguards (notice, appeals, hearings) for when ID issuance is delayed, denied, or defective thus violating basic tenets of administrative justice.

4. Overbreadth & Vagueness

Constitutional Provisions Infringed include:

Article 2(2): Any law inconsistent with the Constitution is void to the extent of the inconsistency.

Article 20(2): Obligates all organs of government to respect, uphold, and promote rights.

Argument: The Registration of Persons Act does not clearly define:

i. What constitutes "sufficient proof of identity"

ii. Whether any alternative forms of identification may be used

iii. What data NIRA can collect, store, and share

This opens the door to arbitrary enforcement and unequal treatment, which courts globally have struck down as unconstitutional (e.g., India's Aadhaar, Kenya's Huduma Namba).

5. Separation of Powers

Constitutional Provisions Infringed include:

Article 1(1) & (2): Sovereignty belongs to the people and shall be exercised in accordance with the Constitution.

Article 79(1): Only Parliament has the power to make laws.

Article 126(1): Judicial power must promote substantive justice.

Argument: The judiciary's deference to the executive and NIRA without reviewing proportionality and rights safeguards has allowed a regulatory body to determine constitutional boundaries, undermining the principle of checks and balances.

While ISER & Ors v. NIRA was cited by NIRA to defend the legality of its ID system, a deeper analysis reveals that the judgment did not adequately address key constitutional and human rights concerns. By narrowly defining "digital," overlooking structural exclusion, and deferring to executive authority without demanding stronger safeguards, the ruling leaves critical gaps in protection. The continued reliance on this decision to justify mass biometric enrolment and ID-linked service access risks entrenching exclusion, weakening oversight, and undermining constitutional guarantees of privacy, equality, due process, and accountability.

Legal and Policy Gaps in Uganda's Biometric Data Framework

By Digital Agenda Forum

Despite Uganda having the Data Protection and Privacy Act (DPPA) and the Registration of Persons Act (ROPA), several gaps remain regarding biometric data governance:

1. Lack of a specific legal definition and framework for biometric data: Neither the DPPA nor ROPA adequately define biometric data as a distinct, high-risk category warranting specific protections.

2. Consent and purpose limitation: The legal framework does not clearly mandate informed, specific, and revocable consent for biometric data collection, nor does it restrict secondary uses (e.g., data sharing across agencies).

3. Retention and deletion: There are no explicit rules governing how long biometric data may be retained, or requirements for secure deletion once the data is no longer needed.

4. Oversight and accountability: There is no independent authority dedicated to biometric data, and enforcement under the DPPA is weak. NIRA, the primary implementer, is both operator and controller, raising conflicts of interest.

Generally in Uganda, there's no structural incentive or obligation for agencies to separate powers or submit to external audit on how they collect, store, and use personal data.

5. Cross-sector applicability: Current laws regulate biometric data only in specific contexts (e.g. national ID), not across all sectors like health, banking, education, and law enforcement where biometric systems are being deployed.

6. Transparency and redress: There are no public reporting obligations for biometric data breaches, profiling, or algorithmic decisions; nor are there accessible complaint or redress mechanisms tailored to biometric harms.

RECOMMENDATION

To address these gaps and ensure fundamental rights are protected, Uganda should enact a standalone Biometric Data Protection Law. This law should:

- Define biometric data as a special category of sensitive personal data.
- Establish clear rules on lawful processing, consent, data minimization, and purpose limitation.
- Require independent oversight through a dedicated supervisory body.
- Provide enforceable data subject rights, including redress for harm.
- Regulate biometric data use in both

public and private sectors.

- Mandate periodic audits and transparency reporting by data controllers.

Such a law should complement existing laws (ROPA, DPPA) and ensure Uganda aligns with international standards including the African Union Convention on Cybersecurity and Personal Data Protection and International best practices such as OECD, GDPR, on clear distinction of roles.

On National Centralised Biometric Data

NIRA, the primary implementer, is both operator and controller, raising conflicts of interest.

This analysis is presented by the **Digital Agenda Forum** as a contribution to public policy discourse at the intersection of technology, society, and rights, and is intended to support rights-based digital governance in Uganda.

RECOMMENDATIONS FOR POLICY AND LEGAL REFORM

- Establish a multi-stakeholder oversight body for NIRA including civil society, technologists, and human rights experts.
- Amend the Registration of Persons Act to provide for alternative identification methods for essential services.
- Require meaningful consultation and participatory design for digital governance systems.
- Enact a standalone law regulating biometric data collection and use, in line with international best practice.
- Strengthen the institutional independence, accessibility, and visibility of the ROPA Section 83 complaints committee.

For more Insights

Follow us on X @DigitalAgendaT

and Visit

https://thedigitalagenda.org

Legal Analysis of Uganda's National Identification System: Surveillance Risks, Legislative Gaps, and the Path Forward

By Digital Agenda Forum

1. Introduction

Uganda's National Identification and Registration framework is primarily governed by the Registration of Persons Act, 2015 (RPA) and the Data Protection and Privacy Act, 2019 (DPPA). While the stated goal of these laws is to enhance national planning, service delivery, and civil registration, their implementation has revealed profound risks to constitutional privacy, autonomy, and non-discrimination. These risks are embedded in the statutory design of the system, particularly in the unrestricted data sharing mandates, the absence of adequate safeguards, and the lack of oversight.

Here below, we systematically identify the legal gaps within Uganda's national ID architecture and propose actionable reforms to prevent digital ID surveillance.

2. Constitutional Foundations and Limits

Uganda's Constitution, under Article 27(2), explicitly protects every person from "interference with the privacy of [their] person, home, or correspondence." This provision is central to interpreting any statutory regime that involves the collection, processing, and sharing of biometric or identifying information. Furthermore, Article 43 requires that any limitation on constitutional rights must be demonstrably justifiable in a free and democratic society.

The National ID system, as currently structured, must be reviewed in light of these constitutional benchmarks. A statutory scheme that enables mass biometric enrolment, mandates ID use for everyday services, and permits undefined government access cannot pass the necessity and proportionality tests enshrined in Article 43.

3. Key Statutes Regulating the National ID System

3.1. Registration of Persons Act, 2015 (RPA)

The RPA establishes the National Identification and Registration Authority (NIRA) and vests it with powers to manage the National Identification Register. Under **Section 5**, NIRA's functions include the registration of citizens and issuance of National Identity Cards. Critically, **Section 65(1)** outlines how ID data can be used, and here lies a major vulnerability: paragraph (l) allows for use of this data for "any other purpose as may be prescribed by the Minister."

This sweeping language effectively

grants the Executive unfettered discretion to expand the scope of ID use without parliamentary approval or public consultation. Furthermore, Section 66 mandates that every person must present a National ID or identification number (NIN) to access services including health, education, and financial services. This turns the ID into an internal passport, thereby enabling systemic exclusion of any person whose ID is lost, expired, or under dispute.

Section 67 grants ministries, departments, and agencies (MDAs) the right to access the National Identification Register for "verification and authentication," but it fails to require any audit trail, data-minimization test, or privacy assessment before such access is granted.

3.2. Data Protection and Privacy Act, 2019 (DPPA)

The DPPA is Uganda's principal law governing personal data, and it sets out basic data protection principles under **Section 3**, including purpose limitation, data minimisation, and lawful processing. However, **Section 7(2)(b)(ii)** of the Act creates a major loophole by exempting processing that is "necessary for national security." In practice, this exception allows law enforcement, intelligence services, and other public bodies to override privacy rights without an assessment of proportionality or necessity.

Section 11(3)(a) reinforces this exemption by allowing the government to collect and process personal data without notice or consent in such contexts.

While the DPPA requires "appropriate technical and organizational measures" to safeguard data, it does not mandate Data Protection Impact Assessments (DPIAs) for high-risk projects such as biometric re-enrolment, facial recognition in ID verification, or integration with vehicle GPS tracking systems. It also lacks explicit provisions for the deletion or anonymization of biometric data upon expiry of purpose.

4. Specific Legislative Gaps and Surveillance Risks

4.1. Unlimited Secondary Use of ID Data

Section 65(1)(l) of the RPA permits the use of ID data for "any other purpose the Minister may determine." This clause undermines the principle of purpose limitation and exposes citizens to profiling, surveillance, and predictive analytics without parliamentary debate. It allows the ID system to be linked with digital number plates, SIM-card registration, or Safe City CCTV databases, all without constitutional or democratic oversight.

4.2. Compulsory Presentation for Public and Private Services

Section 66 of the RPA makes the National ID or NIN a mandatory prerequisite for accessing essential services. This provision effectively criminalizes invisibility and violates the right to non-discrimination under Article 21 of the Constitution. It has disproportionately impacted rural populations, elderly citizens, and refugees,many of whom lack birth records or supporting documentation to register for an ID.

4.3. <u>Broad Access Without Accountability</u>

Section 67 grants access rights to all MDAs for data “verification” purposes, but it includes no language requiring oversight mechanisms, time-bound access, or logging of queries. There is no requirement that agencies justify their need for access, nor are there provisions for affected persons to be notified that their data was queried or shared.

4.4. <u>National Security Overrides Without Proportionality</u>

Section 7(2)(b)(ii) of the DPPA allows state bodies to process data for national security without consent, but it fails to include any standard of necessity or proportionality. There is no requirement for judicial warrant, independent review, or post-facto notification, thereby exposing citizens to secret and indiscriminate surveillance.

4.5. <u>No Right to Erasure or Time Limits on Retention</u>

The RPA is silent on how long biometric data (fingerprints, facial images) can be retained. **Section 14** of the DPPA encourages data minimisation but does not provide an enforceable right to erasure. This creates a permanent biometric footprint that can be used to monitor, track, and profile citizens for life, regardless of changes in purpose or consent.

4.6. <u>Weak Penalties and Poor Enforcement</u>

Under **Section 81** of the RPA, unauthorised disclosure of ID data attracts a fine of up to 72 currency points or a maximum of five years in prison. This is insufficient to deter state agencies or private actors from misuse, especially given the potential political or financial gains of unlawful surveillance. The DPPA contains similarly low fines and does not empower the Personal Data Protection Office (PDPO) to impose administrative penalties scaled to organizational turnover.

4.7. <u>Institutional Conflicts of Interest</u>

The PDPO is structurally embedded within the National Information Technology Authority (NITA-U) under **Section 4** of the DPPA. This compromises its independence, particularly as NITA-U also supports government digital transformation initiatives that rely on the National ID system. There is no independent board, no public appointments process, and no parliamentary reporting requirement for the PDPO.

5. From Civil Registration to Surveillance Infrastructure

The statutory scheme described above, particularly **Sections 65–67** of the RPA and **Section 7** of the DPPA, has enabled the transformation of the National ID system into a surveillance backbone. ID data is now cross-linked with:

a) Intelligent Transport Monitoring System involving GPS-tagged number plates,
b) SIM-card registration that requires NIN verification, and
c) Financial KYC frameworks that mandate ID validation for account access.

None of these integrations were preceded by a legislative process or privacy impact assessments. As a result, the National ID, intended as a development tool, has become a central pillar in an opaque digital surveillance ecosystem.

6. Recommendations for Legal Reform

To realign Uganda's ID system with constitutional rights and global privacy standards, the following legal amendments are recommended:

6.1. **Amend Section 65 of the RPA**

Remove paragraph (l) and replace it with:

"Data from the National Identification Register may only be used for additional purposes upon publication of regulations approved by Parliament and after a Data Protection Impact Assessment has been tabled."

6.2. Limit Mandatory ID Requirements
Amend Section 66 to:
"No person shall be denied access to basic public services such as health, education, and humanitarian aid solely on account of failure to produce a National Identification Number."

6.3. Introduce Right to Erasure and Retention Limits
Insert a new provision stating:
"Biometric data shall be irreversibly encrypted and deleted ten (10) years after last verification unless renewed by the data subject."

6.4. Reform the Data Protection Authority
Amend Section 4 of the DPPA to create a fully independent Data Protection Authority with its own budget, board, and power to impose administrative penalties up to 2% of gross annual revenue.

6.5. Mandate Data Protection Impact Assessments
Insert a new section in the DPPA stating:
"All public-sector digital systems involving biometric processing or data-linkage across agencies shall be subject to a publicly disclosed Data Protection Impact Assessment prior to implementation."

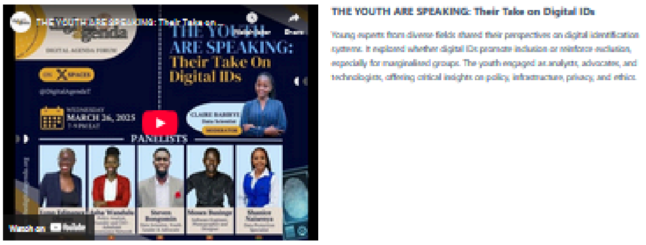
7. Conclusion

Uganda's current National ID legal framework contains multiple statutory loopholes that empower government and private actors to surveil, exclude, and profile citizens without clear legal limits or accountability. These powers contravene the right to privacy under Article 27 of the Constitution and undermine democratic governance.

Reform is not just necessary but urgent. By amending the Registration of Persons Act and the Data Protection and Privacy Act in line with the recommendations above, Uganda can achieve a modern, inclusive, and privacy-respecting identity system that empowers its people rather than monitors them.

Find Our Past Webinars
at
www.thedigitalagenda.org/webinars

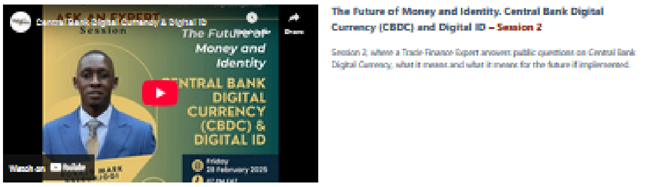
Online Town Hall of 26 March 2025



THE YOUTH ARE SPEAKING: Their Take on Digital IDs

Young experts from diverse fields shared their perspectives on digital identification systems. It explored whether digital IDs promote inclusion or reinforce exclusion, especially for marginalised groups. The youth engaged as analysts, advocates, and technologists, offering critical insights on policy, infrastructure, privacy, and ethics.

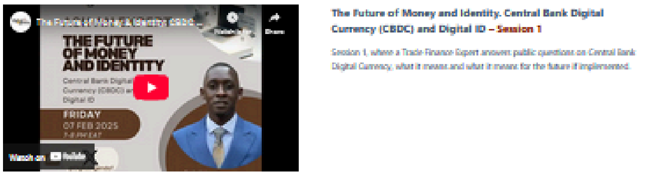
Ask an Expert Session of 28 February 2025



The Future of Money and Identity. Central Bank Digital Currency (CBDC) and Digital ID – Session 2

Session 2, where a Trade Finance Expert answers public questions on Central Bank Digital Currency, what it means and what it means for the future if implemented.

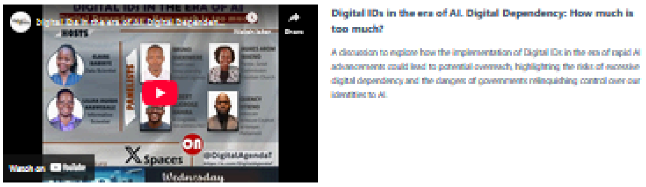
Ask an Expert Session of 07 February 2025



The Future of Money and Identity. Central Bank Digital Currency (CBDC) and Digital ID – Session 1

Session 1, where a Trade Finance Expert answers public questions on Central Bank Digital Currency, what it means and what it means for the future if implemented.

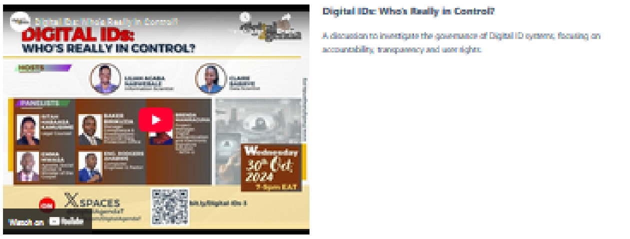
Online Town Hall of 04 December 2024



Digital IDs in the era of AI. Digital Dependency: How much is too much?

A discussion to explore how the implementation of Digital IDs in the era of rapid AI advancements could lead to potential overreach, highlighting the risks of excessive digital dependency and the dangers of governments relinquishing control over our identities to AI.

Online Town Hall of 30 October 2024



Digital IDs: Who's Really in Control?

A discussion to investigate the governance of Digital ID systems, focusing on accountability, transparency and user rights.

Online Town Hall of 21 August 2024

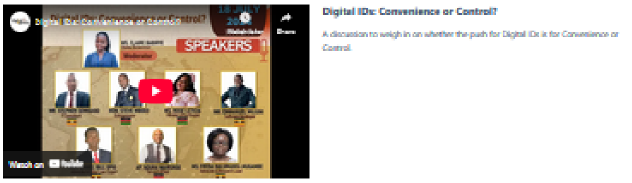
Digital IDs: Can they live up to their promise?

Digital IDs: Can They Live Up To Their Promise? – XSpace discussion

On 21st August 2024, a vibrant and timely discussion was held on X Space under the title "Digital IDs: Can They Live Up to Their Promise?" This session brought together experts from various fields to dissect the emerging issues surrounding digital identification systems and their implications on society. Moderated by Data Scientist Claire Babirye, the session … Continue reading

Digital Agenda

Online Town Hall of 18 July 2024



Digital IDs: Convenience or Control?

A discussion to weigh in on whether the push for Digital IDs is for Convenience or Control.

Logged Out of the Republic: The National ID Ruling and the Future of Digital Citizenship

By Evelyne Naikoba, Governance and Strategy Specialist

In an era defined by rapid digital transformation, national identity systems have become central to how states manage their populations. From financial inclusion to public service delivery, governments around the world are turning to digital identity schemes as the infrastructure of modern governance. Amidst this, a critical question is emerging: Can a tool meant for inclusion become an instrument of exclusion? Uganda's recent High Court ruling on its National Identification Register 'Ndaga Muntu' has brought this question to the fore, and the consequences extend far beyond its borders.

Earlier this month, the **High Court of Uganda** rendered a ruling that may have appeared modest in legal scope but carries deep constitutional consequences. The Applicants led by civil society groups challenged the national digital ID system, *Ndaga Muntu*, on grounds that it had denied Ugandans access to critical services such as healthcare, education, and social protection. The challenge argued that this violated fundamental rights enshrined in Uganda's Constitution, including the right to equality, privacy, and access to public services. Rather than engage deeply with these claims, the High Court adopted a narrowly administrative and factual lens, concluding that the system was not "digital" because it operated offline in some aspects, and that the exclusion of individuals did not rise to the threshold of constitutional violations. In essence, the Court refrained from asserting its role as guardian of the Constitution, choosing instead to defer to executive design and bureaucratic practice.

While the ruling may settle the matter in court–for now–it leaves open larger constitutional and human rights questions that many countries are now grappling with including: **What makes an ID system digital? How do we protect consent, privacy, and due process in automated governance? And where do we draw the line between state efficiency and human dignity?**

Uganda's case must be understood within the broader context of global digital identity developments. Under the auspices of Sustainable Development Goal 16.9, the push for "legal identity for all" has evolved from a commitment to civil registration into a sweeping effort to build centralized, biometric-based digital ID infrastructure. Through the World Bank's Identification for Development (ID4D) initiative, countries have been encouraged, and in some cases incentivized, to adopt foundational ID systems that serve as a prerequisite for accessing both public and private services. Uganda, like more than 170 other countries, has implemented such a system with little public scrutiny and minimal legal oversight.

These kinds of systems encode power because they collapse identity verification, surveillance, and service eligibility into a single infrastructure, allowing states –and in some instances private actors– to control not only who you are, but what you may access. Across jurisdictions, digital ID regimes have already been challenged for their discriminatory impact and overreach. In India, the Aadhaar system led to mass exclusion from welfare programs, with reports of starvation and death following failed biometric authentication. In Kenya, Huduma Namba was stopped by the High Court pending the passage of adequate data protection legislation. In Nigeria, mandatory mobile linkage to digital IDs resulted in millions of citizens losing telecom access. What connects these cases is a common architecture encompassing centralization, biometric dependency, intergration with public service access, no opt-out mechanisms, and the absence of procedural safeguards.

The High Court's assertion that Uganda's system is not "digital" because it does not yet function online ignores internationally accepted definitions. Under World Bank and UN frameworks, a digital ID system is defined not by its user interface, but by its architecture–particularly when it involves biometric enrolment, centralized databases, and automated identity verification processes.

Uganda's ID system unquestionably meets these criteria. The Court's characterization of the system as "offline" and therefore non-digital serves only to shield it from the kind of legal scrutiny that such systems demand.

Moreover, the absence of robust legal safeguards renders the ID regime constitutionally suspect. The system does not guarantee data minimization, consent, or opt-out rights. There are no binding mechanisms for redress or appeal in cases of exclusion, nor are there legislative limits on how biometric data is stored, shared, or retained. These omissions violate **the right to privacy under Article 27, the right to equality under Article 21, and the right to fair and just administrative action under Article 42** of the Constitution.

It is also important to situate this moment within the wider ambitions of global governance. The World Economic Forum has long promoted digital identity as the linchpin of the Fourth Industrial Revolution. In WEF policy documents and pilot projects, digital identity is positioned as a precondition to accessing everything from international travel to e-commerce, healthcare, and even climate-related entitlements. The goal is not merely national identification but global interoperability, where citizens across countries are brought into uniform systems of credentialing that can be integrated, exchanged, and monitored. When states adopt this vision without constitutional temperance, they are building not inclusion, but dependency. And when courts fail to interrogate these systems rigorously, they relinquish their constitutional duty in the face of technical abstraction.

When access to essential services–public utilities, financial institutions, healthcare, education, and social security–depends on biometric registration, the notion of "voluntary" agreement collapses. One cannot meaningfully consent when the alternative is exclusion from the basic infrastructure of modern life. This contradicts the Constitution's underlying assumption that rights are inalienable and not subject to technological preconditions. It also violates emerging international standards around informed consent in digital systems, where individuals must be given real choices as opposed to coerced enrolment disguised as reform.

While I acknowledge that the introduction of the ID system has brought undeniable benefits such as streamlined access to services and improved security, there remains a constitutional imperative to clarify the limits of state power in a digital age. Identity systems must be designed around the individual, not the state. They must be guided by law, constrained by rights, and overseen by independent institutions. The line between innovation and intrusion will be drawn not by the ambition of global partners, but by the strength of our constitutional commitments.

To ensure the national ID system truly serves Ugandans, it must be revised to reflect a foundation of transparency, meaningful consent, and respect for individual rights. This includes recognizing and accommodating the legitimate unwillingness of some individuals to enroll in additional biometric data biometric data collection without facing exclusion or discrimination. Embedding robust legal protections, providing viable alternatives, and establishing independent oversight are essential to prevent abuse and safeguard dignity. Only by prioritizing individual autonomy can the ID system become a genuine tool of empowerment that strengthens democracy rather than undermines it.

For curated insights on leadership, policy and effective government, follow @GovLeadEdge on X.

GOVERNANCE AND LEADERSHIP EDGE

21 posts

Leadership. Influence. Legacy.
www.evelynenaikoba.com
EMPOWERED TO LEAD, DEVOTED TO SERVE
EN
EVELYNE NAIKOBA
Following

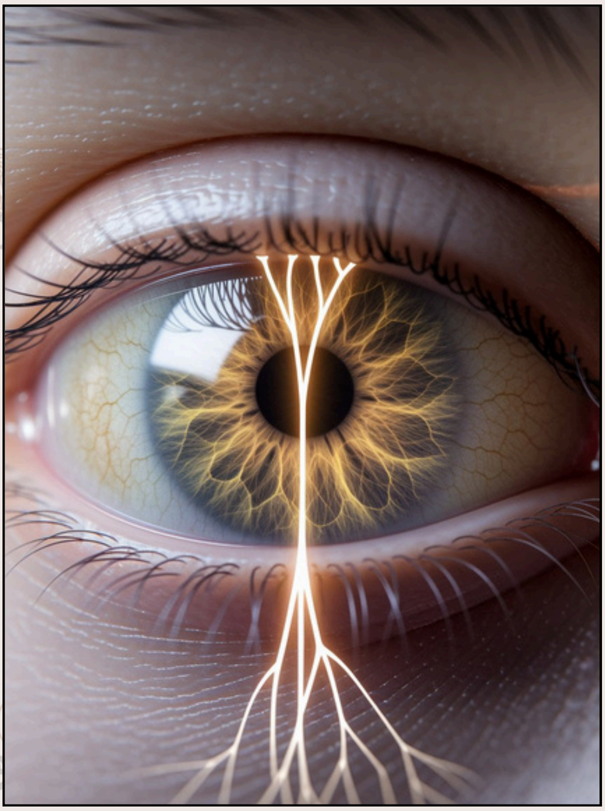
GOVERNANCE AND LEADERSHIP EDGE

@GovLeadEdge

Shaping policy,sharpening leadership, steering futures.

Why Your Fingerprint and Eye Scan Might Not Be the Best for Our National ID

By Asha Wandulu – Policy Analyst, CEO of Ashalumi Governance Network



The way we are collecting information for our National IDs, especially using very personal details like fingerprints and eye scans (what we call "biometric data"), raises some big questions. As someone who cares about how our government works for all its people, I want to explain why collecting this kind of sensitive data can actually cause problems, even though it's presented like it will help.

1. Your Private Information is at Risk

Imagine your fingerprint or your eye pattern is like a key. Right now, NIRA is collecting these unique keys from millions of Ugandans. If these keys are stored in one big place, what happens if that place isn't fully secure?

Hacking and Theft: Just like a physical key can be stolen, digital keys (your biometric data) can be hacked. If criminals get hold of your fingerprint or eye scan, they could potentially use it to pretend to be you, accessing your bank accounts, mobile money, or even getting loans in your name. We've seen real examples from other parts of Africa, like a case in Kenya where a journalist, Japhet Ndubi, lost his phone and later discovered fraudsters had used his fingerprints to access his mobile money account and even take out a loan, leaving him with months of debt.

Misuse of Data: Even if it's not hacked, who else gets to see or use this information? The government might say it's only for national ID, but what if in the future, this data is used for something else without our permission? For example, could it be used to track people's movements or activities? This is called "function creep," where data collected for one purpose is used for another. It takes away our freedom to live our lives without constant watching.

Errors and No Going Back: Unlike a password you can change if it's compromised, you can't change your fingerprint or your eye. If there's an error in your biometric record, or if it's misused, it's incredibly difficult, if not impossible, to fix the problem.

2. Leaving People Behind (Exclusion)

While the goal is to register everyone, using sensitive biometric data can actually push some of our most vulnerable people away from getting an ID, because of;

Worn-Out Fingerprints: Think about our hardworking farmers, market vendors, and construction workers. Many people who work with their hands for many years have worn-out fingerprints. The machines used for scanning might not be able to read their prints accurately. We've already heard stories in Uganda of older people being turned away because their fingerprints couldn't be captured, denying them access to important services like health care or social grants such as Senior Citizen Grant (SAGE). One report even mentioned an elderly man who died trying to travel to verify his worn fingerprints for a social benefit. This is heartbreaking and unacceptable.

Lack of Accessibility: For people with certain disabilities, or those living in very remote areas, getting to a registration point that has the right equipment can be a huge challenge. If they can't provide the "sensitive" data, they might be left out entirely.

What We Need Instead: A Simpler, Safer Way!

Does registering for an ID truly need our fingerprints and eye scans? No. There are simpler and safer ways to do this that respect everyone's privacy and doesn't risk exclusion.

Basic Information is Enough: For a national ID, information like your full name, date of birth, place of birth should be enough. This information, combined with well-managed records, can uniquely identify a person without needing highly sensitive data**.**

Stronger Data Protection, Not More Data: Instead of collecting more sensitive data, the focus should be on making sure the information already collected is extremely well protected. This means:

Clear Rules (Laws): We need very clear laws about who can access our data, why, and how it will be used. These rules should be easy for everyone to understand. Uganda's Data Protection and Privacy Act, 2019, is a good start, but its application to this mass collection needs to be very clear and well-enforced.

Independent Oversight: An independent body should watch over NIRA and other government agencies to make sure they are following the rules and protecting our data.

Transparency: We, the citizens, should know exactly what happens to our information. There should be clear communication about data storage, security measures, and how to correct errors and clearly respect people's fundamental constitutional right to privacy.

Ashalumi Governance Network (AGN)
216 posts

Ashalumi Governance Network (AGN)
@AGovNetwork

Navigating Governance, inspiring Policy!!!!

Email: info@ashalumi.org

Kampala - Uganda Joined December 2024

57 Following 729 Followers

Centralized National ID Database: A Hotspot for Cyber threats

By Claire Babirye, Data Scientist

Recently I was watching 'The Resident' on Netflix and in one particular episode, a former patient who was once failed by the very hospital meant to save them, hacks into Chastain Park Memorial's system, shutting down power. Interestingly, the motive was personal, it was payback but it risked lives at the same time showing how fragile even the most high-tech institutions can be. *Now imagine something similar happening here in Uganda not to a hospital per say but to the centralized national ID database.*

Uganda's National Identification and Registration Authority (NIRA) is in charge of the centralized national ID database and currently it is conducting a nationwide mass enrollment and renewal drive for national IDs. This effort, targeting millions of citizens, involves the collection of sensitive data including fingerprints, facial images, and iris scans. While framed as a step toward digital transformation, it also exposes the country to serious cyberthreats with long-term consequences for privacy, identity integrity, and national security.

This database serves as a central hub for sensitive personal identification information of nearly the entire Uganda population. Cybersecurity experts warn that such centralization creates a single point of failure, making it a lucrative target for hackers, insiders.

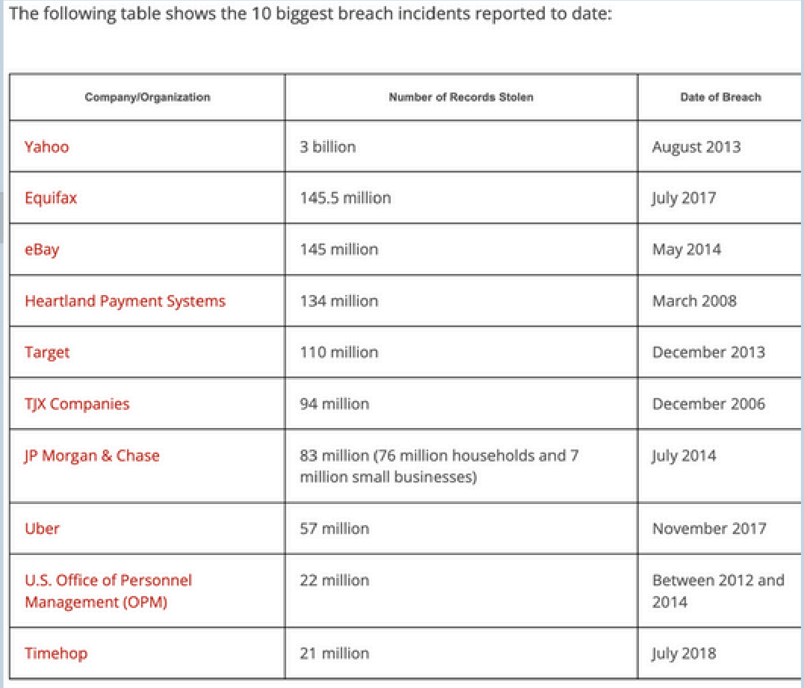
A cautionary precedent is the 2019 BioStar 2 breach[1], where researchers discovered a publicly accessible database used by the biometric access control platform. The breach exposed over 27.8 million records, including fingerprint data, facial recognition images, and other sensitive personal details. Critically, the system stored actual biometric templates rather than hashed versions, making them directly usable if copied. The exposed data, linked to over 5,700 organizations across 83 countries, demonstrated how weak architectural decisions can turn biometric systems into liabilities.

Let's say someone with technical know-how may be a disgruntled citizen denied services, or an external hacker with a political agenda gains access to this database. Has it crossed our mind on what they could do with the iris scan, fingerprint and facial image data? In today's digital ecosystem that's ecosystem that's everything! With that data, they wouldn't just know who you are, they could even choose to be you.

We are living in times where Artificial Intelligence can recreate your face and behaviour with just a few features and data points! And to circle back on what someone could do with this data;

- They could create ultra-realistic deepfakes and thus the people targeted could find themselves represented in digital content they never created, saying or doing things they never did.
- Bypass facial recognition security systems.
- They could impersonate you across systems, access services meant only for you and even present themselves as the kind of person others trust, consult, or rely on. Imagine someone becoming that "essential" version of you, the one whose advice is sought after.

Probably one could say the story in 'The Resident' is a fiction, real-world examples aren't far off. According to cybersecurity firm TrendMicro, some of the world's most recognized companies including Yahoo, eBay, and Uber have been named among the top 10 biggest data breach incidents globally[2]. These are massive platforms with significant security budgets, yet they still fell victim to breaches.



The following table shows the 10 biggest breach incidents reported to date:

Company/Organization	Number of Records Stolen	Date of Breach
Yahoo	3 billion	August 2013
Equifax	145.5 million	July 2017
eBay	145 million	May 2014
Heartland Payment Systems	134 million	March 2008
Target	110 million	December 2013
TJX Companies	94 million	December 2006
JP Morgan & Chase	83 million (76 million households and 7 million small businesses)	July 2014
Uber	57 million	November 2017
U.S. Office of Personnel Management (OPM)	22 million	Between 2012 and 2014
Timehop	21 million	July 2018

In the wrong hands, your biometric data isn't just a risk, it's a shortcut to your life. If this biometric data were accessed or leaked by a malicious insider, a cyber criminal, the damage would be permanent since unlike passwords, biometric attributes cannot be changed. It's not just data at risk, it's lives!

[1] *https://www.trendmicro.com/vinfo/us/security/news/online-privacy/over-27-8m-records-exposed-in-biostar-2-data-breach*

[2] *https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-101*

Are Children the New Data Centres?

By Evelyne Naikoba, Governance and Strategy Specialist

An infant's fingerprints being captured during National Identification registration. — Courtesy of NIRA

Have you ever paused to ask how we moved so seamlessly from barefoot afternoons and sunlit play to a world where a child's first reflex is to swipe? Not long ago, childhood meant scraped knees, hide-and-seek, bikes left lying in the driveway, and breathless games that ended only when the sun went down. But today, toddlers swipe before they can form full sentences, 10-year-olds know more about YouTube algorithms than nature trails, and classrooms are replaced by dashboards, families fight nightly battles over tablets, gaming consoles, and screen time.

It is a shift that unfolded almost imperceptibly. The transformation was never declared. There was no collective debate about what would replace unstructured play, no referendum on the replacement of real-world curiosity with algorithmically mediated experience. And yet, in the space of barely a generation, we have witnessed the most radical reengineering of childhood in human history – by design, data, and device.

Today, children are born into ecosystems of pervasive digitality. They are introduced to screens not as tools but as mirrors and reflective surfaces where their interests, movements, and emotions are continuously recorded and remapped.

Concerned parents across the globe try to limit device use, fearing the effects on mental well-being, social development, and sleep, even as they lament the loss of "attention spans" or the rise in anxiety and strange mood swings after hours of digital immersion. But while we're busy worrying and focused on how much time children spend on devices, we've been missing something even more serious and far more invisible. Few have fully grasped the more disquieting reality that modern childhood has become a data-generating function within the infrastructure of surveillance capitalism.

What if the issue isn't just what children are doing on screens but what these devices are doing to them in return?

Because behind every animated learning app, online classroom, and "educational" game lies a data machine mining children's attention, emotion, and identity like raw ore.

What began as educational enrichment — a math app here, a virtual classroom there — has quietly metastasised into something else entirely. Behind every "educational app," each interactive toy, each cheerful online lesson, is a system quietly watching, logging , storing, and learning. Children, the youngest among us, have become the ideal source of rich unfiltered, unguarded and incredibly revealing behavioural data. And the systems that harvest this data are growing more sophisticated by the day.

Children have become the test bed for machine learning, the training ground for emotion recognition software, the raw input for behavioral analytics, and, increasingly, the lab rats for predictive systems that promise to know who they are and what they will become before they do. Every pause in a reading app, every wrong answer on a quiz, every smile caught by a webcam is stored, tagged, and used to train artificial intelligence and shape future predictions of this child's personality and how to reach them, market to them, teach them, or influence them. This, as you might realise, is done without consent, understanding, and often without oversight.

Children have become the test bed for machine learning, the training ground for emotion recognition software, the raw input for behavioral analytics, and, increasingly, the lab rats for predictive systems that promise to know who they are and what they will become before they do.

This quiet harvesting is global. In China, in accordance with state policy, classrooms are equipped with facial recognition cameras, AI-based emotion tracking, and EEG brainwave-monitoring headbands to monitor attentiveness. These systems not only collect performance data but record focus, micro-expressions, gaze shifts, mood, and physiological signals to score obedience and emotional compliance.

In the United States, children interact daily with platforms like Google Classroom and ClassDojo. Framed as tools for engagement, these systems quietly collect rich streams of data including response times, tone of voice, facial affect, behavioural feedback from teachers – in order to "personalise" learning and sometimes monetise it. Most parents sign off with a click, unaware that their child's educational "journey" is also serving to refine proprietary algorithms owned by commercial entities.

In India, children are registered at birth via Aadhaar, the world's largest biometric identity system. Their fingerprints and iris scans are linked to their school performance, vaccinations, and even attendance – constructing a biometric dossier before the age of five. In countries across Africa and Latin America, edtech solutions funded by Silicon Valley philanthropies are embedded into public education systems under the banner of providing solutions that promise efficiency – but operating as data collection pipelines in regulatory vacuums. These same platforms harvest engagement data, attention patterns, and familial metadata creating permanent digital profiles in places where children have few legal rights over their own information.

Even in refugee camps administered by the United Nations, biometric data is used to manage food allocation, access to education, and health records. These are the most vulnerable children alive. And yet, their data is often stored indefinitely, managed by outsourced contractors, and is rarely subject to meaningful oversight. What happens when data collected under the name of survival becomes a permanent record that follows a child across borders and into adulthood?

What ties these disparate cases together is a strategic and systemic convergence designed by global institutions, fuelled by technology companies, and framed by policymakers who often see children as both vulnerable and "scalable" through predictive monetization.

This new architecture of childhood is built not only by corporations but with the enthusiastic participation of global governance institutions. The World Economic Forum, under the guise of "The Fourth Industrial Revolution," actively promotes emotion-tracking AI in classrooms, biometric learning platforms, and the behavioural personalisation of education. The United Nations supports initiatives like ID4D, advocating for universal digital identity beginning at birth. Major philanthropic foundations channel billions into "edtech for the poor," effectively creating experimental zones in the Global South where consent is elastic and regulation is weak.

What is being lost in this shift is profound. The issue goes beyond data privacy. It strikes at the heart of what it means to be a child. Childhood, once defined by freedom, messy growth, trial and error, imagination, and risk, is becoming a realm of metrics and optimisation. The unquantifiable spaces — wonder, boredom, silence — are being coded out of existence. We are not merely digitising education; we are redesigning the epistemology of growing up.

What is being lost in this shift is profound. The issue goes beyond data privacy. It strikes at the heart of what it means to be a child. Childhood, once defined by freedom, messy growth, trial and error, imagination, and risk, is becoming a realm of metrics and optimisation.

Instead of learning freely, children are nudged, scored, and moulded by invisible systems. When a child hesitates on a question, the system notes it. When they show frustration, it's tagged. When they smile during a lesson, their emotion is analysed, and possibly sold. Over time, these profiles don't just track a child; they begin to decide for them — what they're shown, how they're taught, which paths they're offered. All shaped by data that the child never agreed to give, in systems they can't see, governed by code no one fully understands.

Children are treated, not as citizens-in-development, but as data assets viewed as objects of computation and a living feedback loops. And the language used — access, inclusion, empowerment — is persuasive. Who would oppose tools that help children learn? But when access means surveillance, when empowerment comes at the cost of privacy, when inclusion requires a lifetime of data exposure, we must ask whether this is the future we want for our children.

We must begin to draw ethical boundaries in this rapidly accelerating domain. Data minimisation must become non-negotiable in any system designed for children. A child should have the right to be forgotten — not at 18, but always. Schools and parents must demand transparency: what data is being collected, who owns it, and how long it lives. Platforms designed for children should be subject to independent audits, just like food, medicine, or toys. Digital consent must be layered, reversible, and meaningful. And there must be international consensus on prohibiting the use of children's data for AI training or behavioural marketing.

Moreover, we must reckon with the deeper societal implication: that a future which teaches children to expect continuous observation is a future that normalises authoritarianism – subtly, insidiously –through interfaces designed to reward conformity and legibility.

If we fail to protect the mystery, interiority, and unpredictability of childhood, we may find ourselves raising a generation who will never know what it means to be truly unobserved – and who, as a result, may never feel truly free.

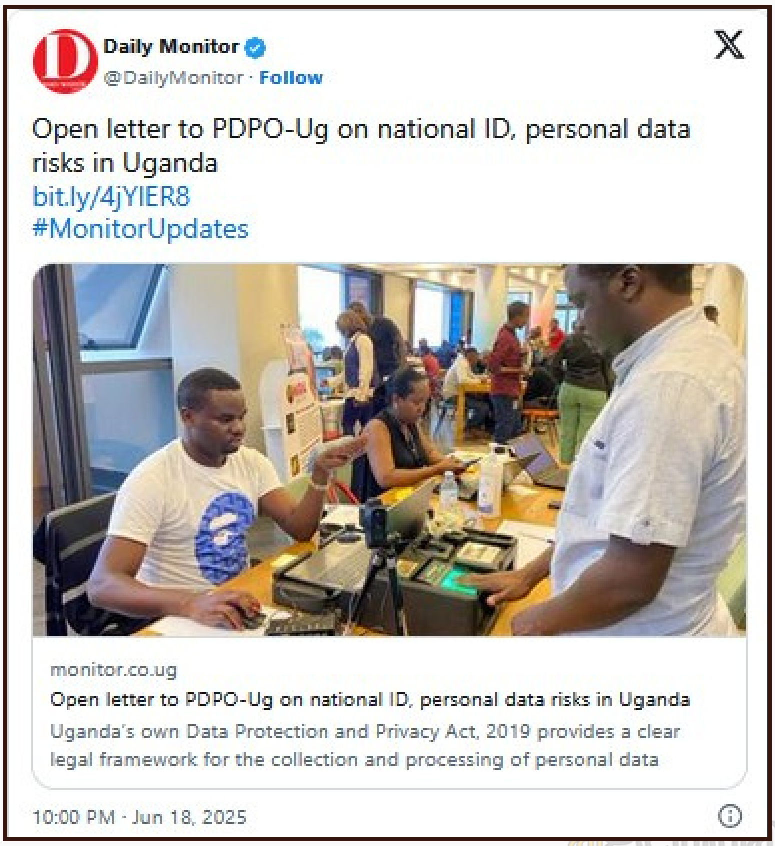
Childhood must never be a business model, beta test, or a dataset. It is, and must remain, a realm of becoming – protected not only by parents, but by principle, by policy, and by the fierce insistence that some aspects of human life are not for capture.

Not now. Not ever.

For curated insights on leadership, policy and effective government, follow @GovLeadEdge on X.

IN THE NEWS

By Digital Agenda Forum



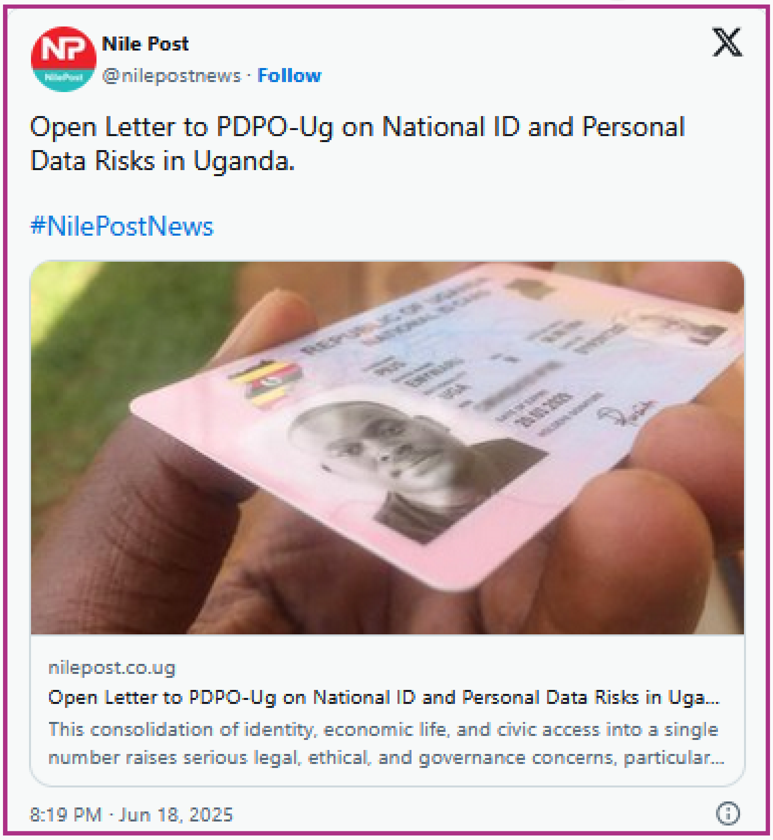
Daily Monitor
@DailyMonitor · Follow

Open letter to PDPO-Ug on national ID, personal data risks in Uganda
bit.ly/4jYIER8
#MonitorUpdates

monitor.co.ug
Open letter to PDPO-Ug on national ID, personal data risks in Uganda
Uganda's own Data Protection and Privacy Act, 2019 provides a clear legal framework for the collection and processing of personal data

10:00 PM · Jun 18, 2025

Read article at https://www.monitor.co.ug/uganda/oped/letters/open-letter-to-pdpo-ug-on-national-id-personal-data-risks-in-uganda-5086658



Nile Post
@nilepostnews · Follow

Open Letter to PDPO-Ug on National ID and Personal Data Risks in Uganda.

#NilePostNews

nilepost.co.ug
Open Letter to PDPO-Ug on National ID and Personal Data Risks in Uga...
This consolidation of identity, economic life, and civic access into a single number raises serious legal, ethical, and governance concerns, particular...

8:19 PM · Jun 18, 2025

Read article at https://nilepost.co.ug/opinions/266012/open-letter-to-pdpo-ug-on-national-id-and-personal-data-risks-in-uganda

“Don’t Worry, It’s Just an ID…” Until It’s Not!

By Lilian Agaba Nabwebale, Information Scientist & Minister of the Gospel

If modernity means scanning every inch of your body to access basic services, then yes, we’re right on track.

First, it was fingerprints. Now, they say, let us add in eye scans, apparently because after five years our fingerprints have expired. We dig too much, they say. So naturally, the solution must be more scanning.

What will they ask for in the next five years? Saliva or Hair strands for DNA? Won’t they soon say it should now be a chip implant, all in the name of “unique identity”? After all, the law is open-ended. It allows collecting anything deemed fit for unique identification. Tagging everyone like goods.

What started off “innocently” in 2014, saying the National ID was only for those above 16, quietly lowered the age to 5-year-olds. Now, even one-day-old infants must be registered or rather tagged!

For without the NIN, there is no unit trust, no investment, no transacting, no school, no inheritance, no healthcare, no phone number, no access to money, no travel, no employment, no services of any sort. You will not access food too.

A steady noose, and we clap along. Could it because we don’t keep history and don’t study patterns? Alas! You are not human without a Number.

Isn’t this what they’ve been saying all along, that you will own nothing and be happy?

There’s a particular fury that boils up when authorities are questioned on this. As if obedience without question is the only rule. Asking is seen as defiance, and silence is demanded. In their design, silence is loyalty, and questions are rebellion.

So, you think the mark of the beast will happen in one go? That it will be a single, obvious event? You think the devil is that stupid? Even Jesus acknowledged his cunning, and told us to be as shrewd as the children of this world (Matthew 10:16). Yet here we are, stage after stage, rollout after rollout, and we keep calling it "development".

Have you ever paused to see how ***centralised identity systems*** have been used before? In slavery. In genocides. In systems of total control. Or maybe history is just another dusty file no one wants to read.

After all, what could possibly go wrong with giving up your bodily data to access your constitutional rights?

"Don't worry, it's just an ID," they say. Until it's not!

So do we sit and watch on? Is that what Jesus told us to do? Is He coming back for a church that's defeated and hiding in closets? What happened to the authority He gave us? [Luke 10:19] Is the devil more powerful than we are? Must we sit idle because "it was foretold"? Is it even his time yet?

What Now?

We must stop pretending this is normal. We must stop baptising control and calling it progress. Silence is not wisdom, and passive endurance is not faith.

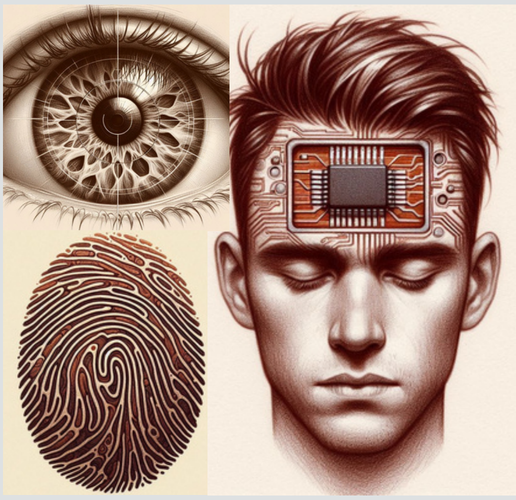
It's time to wake up. To question loudly. To challenge boldly. To push back against policies dressed in digital suits but carrying the same old chains. If we do not draw the line now, they will redraw it for us, again and again, until there's nothing left to call our own. Not even our bodies.

Let us document. Let us organise. Let us educate those who have no idea what is being traded for convenience. Let us arise to the truth.

For the church, this is not the time to hide in buildings or behind prophecy. It is time to occupy until He comes. To speak truth without fear. To remember the authority we were given. The gospel is not just about saving souls for the next life, but standing for truth in this one.

If we don't rise, they will keep tightening the grip. One scan, one law, one compromise at a time.

So rise. Speak. Do not become accomplices of the devil. Use your voice while you still have one, **before silence becomes oppression.**



FOR MORE FROM THE DIGITAL AGENDA FORUM

FOLLOW US ON X

DIGITAL AGENDA

Following

Digital Agenda
@DigitalAgendaT

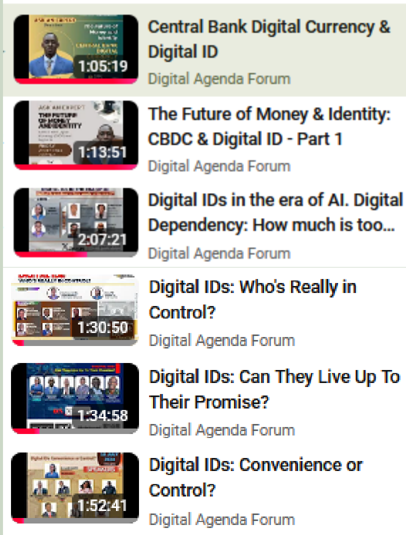
Insights on developments in the Tech industry

thedigitalagenda.org Joined July 2024

196 Following 232 Followers

Subscribe to our YouTube Channel

at https://www.youtube.com/@DigitalAgendaT



1:05:19 Central Bank Digital Currency & Digital ID
Digital Agenda Forum

1:13:51 The Future of Money & Identity: CBDC & Digital ID - Part 1
Digital Agenda Forum

2:07:21 Digital IDs in the era of AI. Digital Dependency: How much is too...
Digital Agenda Forum

1:30:50 Digital IDs: Who's Really in Control?
Digital Agenda Forum

1:34:58 Digital IDs: Can They Live Up To Their Promise?
Digital Agenda Forum

1:52:41 Digital IDs: Convenience or Control?
Digital Agenda Forum

Follow us on

TikTok

@digitalagendat

Visit our Website at

www.thedigitalagenda.org

LinkedIn at digital-agenda-forum

Radio interviews on the digital agenda!
www.thedigitalagenda.org/radio

This is a publication of the Digital Agenda Forum.

Contact Us

For further inquiries and information

Digital Agenda Forum
📍 Munyonyo, Kampala, UG
📞+256 782 408607
📧 *info@thedigitalagenda.org*
✉️ P.O BOX 172431, Kampala
🌍 www.thedigitalagenda.org