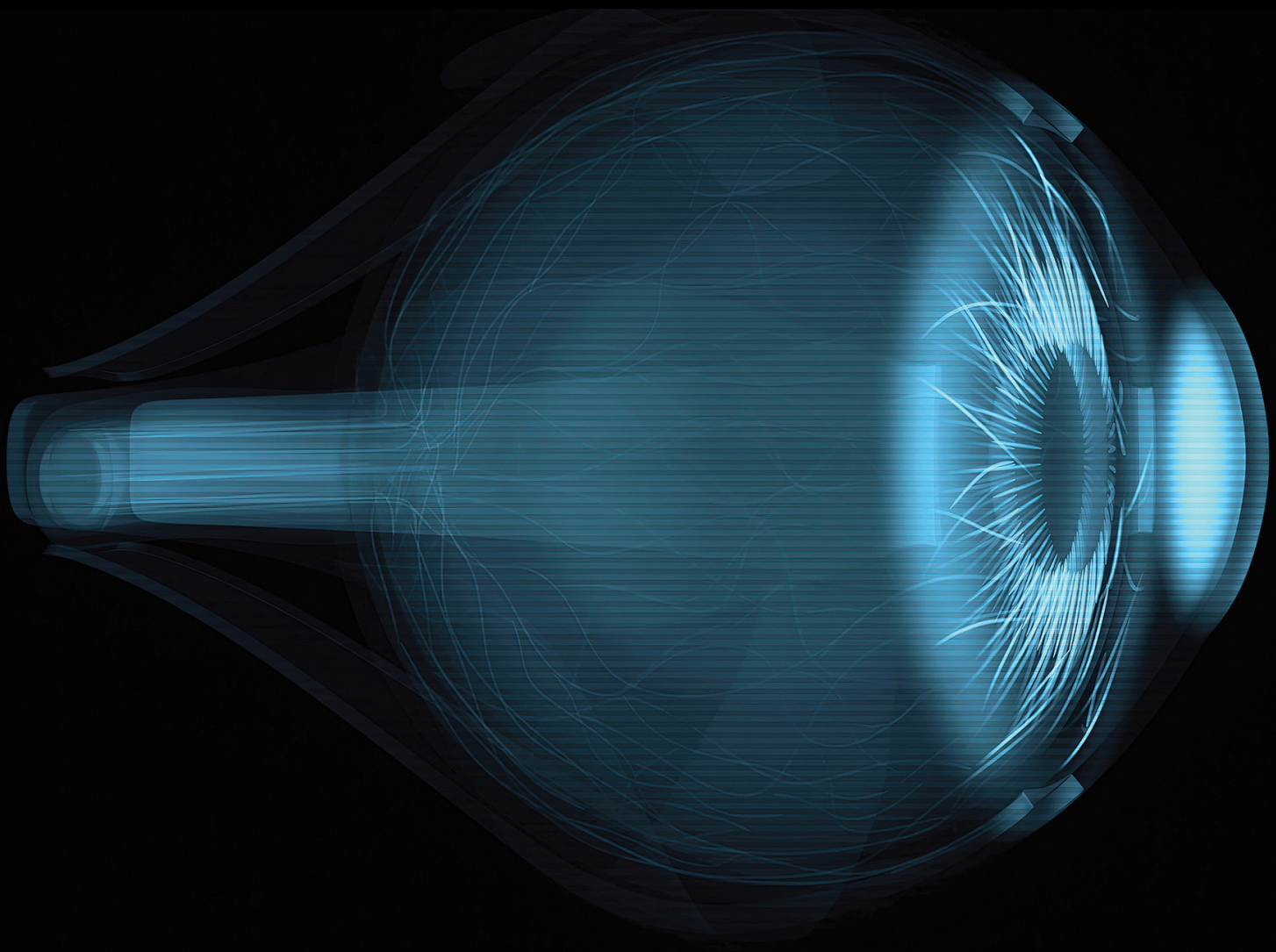
Atlantic Council DFRLab

Biometrics and digital identification systems in Africa:

Assessment of governance, vendors, and human rights



Sani Suleiman Sani

Authors
Sani Suleiman Sani

Contributors
Thobekile Matimbe
Aida Oluwagbemiga

Editors
Iria Puyosa
Kenton Thibaut

Biometrics and digital identification systems in Africa:

Assessment of governance, vendors, and human rights

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

Cover: Reuters/Science Photo Library

ISBN: 978-1-61977-378-3

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

2025

Table of contents

Executive summary

The rapid adoption of biometric and digital identification systems is transforming governance and public administration across Africa. Promoted as tools to modernize service delivery, enhance electoral integrity, and strengthen state capacity, these systems are becoming central to how identity and citizenship are managed. From national identification schemes and voter registration to border management and SIM card registration, biometrics have become deeply embedded in Africa's political, social, and economic landscape.

However, this technological expansion comes with profound risks. Weak legal frameworks, limited oversight, and a growing reliance on foreign vendors have created an ecosystem vulnerable to privacy breaches, state surveillance, and systemic exclusion. Biometric systems increasingly integrate electoral and civil identity data, giving governments vast surveillance capabilities while disenfranchising marginalized groups such as rural communities, migrants, and individuals without foundational identify documents (IDs).

The report explores the main use cases driving biometric and digital identification systems in Africa, focusing on their governance, vendor dynamics, and human rights impacts. Key areas include national identification and civil registration, which provide the foundation for legal identity and access to services; immigration management; elections, where they strengthen voter registration and authentication; and smart city initiatives, which leverage digital IDs for efficient service delivery and urban governance.

The research reveals that foreign technology firms dominate Africa's biometric ecosystem; forty-nine African countries have at least one form of biometric system; and thirty-five out of the fifty-four countries on the continent use biometrics in their election processes. Companies such as Idemia (France), Semlex (Belgium), Veridos (Germany), Thales (France), and Huawei (China) provide the core technology, hardware, and algorithms that underpin these systems. African governments often finance these projects through loans from international institutions like the World Bank, creating dependencies that shape procurement and governance practices.

While biometric systems are often introduced to improve electoral processes and service delivery, their fragmented rollout forces citizens to repeatedly submit sensitive data across multiple platforms, increasing costs and risk of fraud. Many projects lack transparency, with procurement processes shielded under the guise of national security. Public knowledge of these systems remains low: a sample study in three countries by ICT Works found that only 38 percent of surveyed citizens were aware of their governments' purchases of biometric, facial recognition, or AI systems, highlighting a significant transparency gap.

To mitigate these risks, the report offers seven key policy recommendations:

1. Strengthening independent oversight bodies free from political interference;
2. Enacting comprehensive data protection laws covering the full life cycle of biometric data;
3. Ensuring transparent, participatory deployment processes; integrating human rights due diligence into all projects;
4. Establishing continuous oversight and remedies for rights violations;
5. Protecting electoral integrity and preventing the over-integration of ID systems;
6. Embedding a rights-based governance model rooted in privacy, equality, and non-discrimination.

The findings underscore that biometric and digital identity systems must not be viewed merely as technical tools for modernization. They are inherently political, with the potential to either strengthen democratic governance or instead entrench authoritarian control. Without robust reforms, these systems risk becoming instruments of exclusion and surveillance, rather than empowerment.

Introduction

The rapid adoption of biometric and digital identification systems across Africa marks one of the most significant shifts in governance and public administration in recent decades. Promoted as tools to improve service delivery, enhance electoral integrity, and modernize state capacity, these technologies are also reshaping the very architecture of identity and citizenship. From national ID schemes to voter registration, border management, and SIM card enrollment, biometrics are becoming deeply embedded in the social, political, and economic fabric of the continent. Yet, the transformative potential of these systems is matched by profound risks. Weak regulatory frameworks, vendor-driven ecosystems, and limited oversight raise urgent questions about privacy, exclusion, surveillance, and the broader implications for human rights and democratic governance. Against this backdrop, this research interrogates not only the technical and institutional features of biometric systems in Africa, but also the structural conditions that shape their deployment and impact.

Several important studies have already explored the rise of biometric digital identity in Africa, documenting both the drivers and challenges of these systems. The Collaboration on International ICT Policy for East and Southern Africa (CIPESA), in its policy brief *Biometrics and Digital Identity in Africa: Challenges, Opportunities and Policy Options*, provides a broad overview of how African countries are adopting biometric ID systems to enhance e-government, financial access, e-commerce, and national security.[1] The brief highlights the promise of secure and efficient identification systems, while cautioning against risks to privacy and data protection. Its focus lies in policy options that African states can consider to balance technological advancement with the safeguarding of fundamental rights.

Similarly, Research ICT Africa, in partnership with the Centre for Internet and Society (CIS), undertook a more granular, comparative study across ten African countries, including Ghana, Kenya, Nigeria, Lesotho, Mozambique, Tanzania, Uganda, Rwanda, Zimbabwe, and South Africa.[2] Using a rights-based evaluation framework, the project assesses the extent to which digital identity systems comply with international norms on privacy, data protection, and inclusion.[3] The Ghana case study, along with the wider comparative report, brings attention to governance practices, institutional arrangements, and the role of civil society in shaping accountability. This body of work provides valuable insights into how national contexts shape the design and implementation of digital identity.

Another report by CIPESA, *Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa,* provides an in-depth examination of the legal and policy landscapes affecting privacy rights across the continent.[4] Using a qualitative methodology, the study combines legal and policy analysis, literature review, and key informant interviews to identify and evaluate laws relevant to privacy in twenty-three African countries. The research focuses on four critical areas: surveillance practices, data localization requirements, management of biometric databases, and restrictions on encryption technologies. It pays particular attention to the safeguards and remedies enshrined in national laws and evaluates how well these align with international human rights standards, especially those aimed at protecting individuals from unsanctioned surveillance, censorship, and privacy violations. The report highlights how weak legal protections can enable state overreach, mass surveillance, and violations of digital rights. This makes it an essential resource for understanding the intersection of privacy, technology, and governance in Africa, and provides a foundation for advocacy efforts to strengthen privacy protections as digital ID systems and other data-intensive technologies expand across the continent.

In another significant report published by the Atlantic Council's DFRLab, titled ***D****igital Identities and Border Cultures: The Limits of Technosolutionism in the Management of Human Mobility,* author Nanjala Nyabola focuses on how digital identity systems intersect with migration management.[5] Nyabola argues that refugees and migrants face unique digital rights violations, largely because of their limited political power within the societies they enter. This vulnerability is intensified by "technosolutionism," the belief that complex social and political issues

1. "Biometrics and Digital Identity in Africa Challenges, Opportunities and Policy Options," Collaboration on International ICT Policy for East and Southern Africa (CIPESA), April 2024, https://cipesa.org/wp-content/files/Biometrics_and_Digital_Identity_in_Africa_Brief.pdf
2. Anri van der Spuy, "Digital identity in Ghana: Case study conducted as part of a ten-country exploration of socio-digital ID systems in parts of Africa," Research ICT Africa, November 2, 2021, https://researchictafrica.net/research/digital-identity-in-ghana-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/.
3. Vrinda Bhandari, Shruti Trikanad, and Amber Sinha, "Governing ID: A Framework for Evaluation of Digital Identity," Digital Identities: Designs and Uses, January 20, 2020, https://digitalid.design/evaluation-framework-02.html.
4. "Privacy Imperilled: Analysis of Surveillance, Encryption and Data Localisation Laws in Africa", CIPESA, February 2022, https://cipesa.org/wp-content/files/briefs/Privacy-Imperilled-Analysis-of-Surveillance-Encryption-and-Data-Localisation-Laws-in-Africa-Report.pdf.
5. Nanjala Nyabola, "Digital Identities and Border Cultures: The Limits of Technosolutionism in the Management of Human Mobility," DFRLab/Atlantic Council, August 2023, https://www.atlanticcouncil.org/wp-content/uploads/2023/08/Digital-Identities-and-Border-Cultures.pdf.

can be solved primarily through technology, without adequate consideration of the human and societal dimensions involved. The report highlights how wealthy countries play a dominant role in defining the global "border culture." These nations set the terms for how migration is managed by producing and distributing knowledge about border technologies and digital identity systems. As a result, frameworks and systems are often designed in affluent countries but deployed uncritically in poorer nations, creating a fundamental disconnect between policy and lived reality. This imbalance not only excludes the voices and experiences of the Global South, but also leads to material consequences for migrants, such as heightened surveillance, restricted mobility, and systemic exclusion. When digital identity systems are introduced into migration management, individuals are reduced to data points in a bureaucracy, the report concludes.

Beyond regional organizations, international actors have contributed to shaping the debate. The World Bank's Identification for Development (ID4D) initiative has advanced the case for digital ID as an enabler of financial inclusion, service delivery, and digital transformation.[6] At the same time, advocacy groups such as Amnesty International, Access Now, and Privacy International have added their own rights-based critiques, warning against surveillance, exclusion, and weak legal protections.[7] At the continental level, the African Union's Malabo Convention on Cybersecurity and Data Protection, which has been in effect since 2023, along with the AU Data Policy Framework established in 2022, emphasizes both individual and collective data rights.[8] These include the right to information, data access, and personal data protection.

Taken together, the literature establishes that biometric identity systems are now a central part of Africa's digital transformation agenda, with strong policy, rights, and governance implications. However, much of the existing research has focused either on high-level policy frameworks or on national case studies. Our study takes a different vantage point, looking at the broader ecosystem behind BDI deployment, from the role of vendors and supply chains to the interplay of private sector actors, cross-border integration, and the political economy of identity management. By situating biometric systems within this wider context, the report adds a complementary perspective that speaks not only to policy and rights, but also to the structural, commercial, and developmental dimensions shaping digital identity in Africa.

This report provides a continent-wide analysis of the adoption and deployment of biometric ID systems across Africa, offering a holistic picture that goes beyond the country-specific focus of many previous studies. It explores the key use cases driving these technologies, including national identity and civil registration systems, which are foundational for legal identity and access to essential services; immigration management, where biometrics are used to secure borders and manage migration flows; electoral processes, where they play a crucial role in voter registration and authentication to enhance electoral integrity; and smart city initiatives, where digital ID systems support urban innovation and data-driven governance.

A unique contribution of this study is its examination of the vendor landscape and supply chain, shedding light on the global and local companies powering Africa's biometric infrastructure—a dimension often overlooked in previous research. By connecting this vendor ecosystem to governance frameworks and human rights implications, the report reveals how technological choices and procurement decisions affect privacy, accountability, and sovereignty. Through its continent-wide scope, the study captures patterns, risks, and opportunities that may be missed in country-specific studies, offering policymakers, civil society, and development actors an integrated perspective on the future of governance for biometric systems in Africa.

6. Ardic Alper, Oya Pinar; Clark, Julia; Galicia Rabadan, Guillermo Alfonso; Marin, Georgina. Digital Public Infrastructure and Development: A World Bank Group Approach - Digital Transformation White Paper Volume 1 (English). Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099031025172027713
7. Advocacy Briefing for Defending the Rights of Refugees, Asylum Seekers, and Migrants in The Digital Age. Amnesty International. September 12, 2025. https://www.amnesty.org/en/documents/pol30/0290/2025/en/

Díaz, Marianne. Why do we need tailored identity systems for our digital world? Access Now. September 11, 2024. https://www.accessnow.org/digital-identity-systems/

Digital National ID systems: Ways, shapes, and forms. Privacy International. October 26, 2021. https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms

8. African Union. Convention on Cyber Security and Personal Data Protection. June 27, 2014, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

Methodology

This study employs a qualitative and comparative approach, drawing on a review of legal frameworks, policy documents, and regional instruments such as the Malabo Convention and the African Union Data Policy Framework, alongside case studies from selected African countries.[9, 10] Secondary sources, including academic literature, reports from civil society organizations, and media accounts, were triangulated to capture both the technical architectures of biometric systems and their lived consequences for ordinary citizens. Attention is paid to the role of private vendors, the organization of supply chains, and the interaction between national frameworks and continental or global governance norms. By combining documentary analysis with a critical rights-based perspective, the study situates biometric ID systems within broader debates on data governance, sovereignty, and social justice in Africa.

One of the primary tools used to guide the analysis was the Evaluation Framework for Digital Identities developed by the Centre for Internet and Society (CIS).[11] This framework serves as a reference point for assessing how well digital identity systems align with international human rights norms and data protection principles. It offers a structured methodology for evaluating the governance and implementation mechanisms of digital ID systems within specific country contexts, with a particular focus on the balance between innovation and the protection of fundamental rights.

The study also considered the UNDP Model Governance Framework for Digital Legal Identity Systems, which provides practical guidance for the design, implementation, and management of digital identity systems.[12] This framework emphasizes the creation of ethical, inclusive, and accountable digital ID ecosystems, setting out structures and processes that ensure these systems protect human rights, mitigate risks, and establish clear lines of accountability among the various actors involved. Crucially, it promotes a rights-based approach, ensuring that individuals retain meaningful control over their personal data and are protected against misuse or abuse. This guidance is particularly relevant in contexts where digital ID systems are integrated with essential services such as voting, healthcare, and social protection. Failures in governance or system design in these areas can lead to systemic discrimination, exclusion, or the denial of essential services to vulnerable populations.

In addition to these global frameworks, the study acknowledged the Smart Africa Initiative, a collaborative effort led by African Heads of State and Government. Smart Africa seeks to accelerate sustainable socio-economic inclusion and development across the continent through the strategic use of information and communication technologies (ICT).[13]

9. “African Union Convention on Cybersecurity and Personal Data Protection,” African Union, June 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.
10. “AU Data Policy Framework,” African Union, February 2022, https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf.
11. Vrinda Bhandari, Shruti Trikanad, and Amber Sinha, Governing ID: Principles for Evaluation of Digital Identity,” The Center for Internet & Society, 2022, https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf.
12. “Model Governance Framework for Digital Legal Identity Systems,” UN Development Program, 2023, https://www.governance4id.org/..
13. “Digital Transformation Drives Development in Africa,” World Bank, January 18, 2024, https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa.

The state of deployment of biometric technologies in Africa

The World Bank estimates that around half a billion people in Africa cannot prove their identity, and has mobilized more than $1.2 billion to support ID projects in forty-nine countries.[14, 15] Through its Identification for Development (ID4D) initiative, it is currently assisting some of these countries in Africa, including Rwanda, Nigeria, and Tunisia, as well as in Asia and South America.

The provision and possession of a legal identity is recognized as crucial for promoting development and forms part of the UN’s Sustainable Development Agenda and related Sustainable Development Goals (SDGs). Under SDG 16.9, states have committed to provide “legal identity for all, including birth registration” by 2030. The African Union (AU) sees legal identity as crucial for reaching the goals of Agenda 2063.[16] The regional body asserts that a modern, urbanizing continent with increasingly complex business transactions makes legal identity a necessity.[17]

Across the continent, the deployment of biometric and digital identity systems has moved from pilot initiatives to large-scale national programs. Today, more than forty countries on the continent have either rolled out or announced plans to implement biometric IDs, often tied to foundational registries that underpin access to public services, elections, mobile connectivity, and financial systems. Out of fifty-four African countries, thirty-five use biometrics in elections.[18] These systems typically capture fingerprints, facial recognition data, and in some cases iris scans, storing them in centralized databases that serve as the backbone of national identification.

This expansion of biometric ID systems is far from uniform. In Nigeria, for example, the National Identity Management Commission has driven one of the continent’s most ambitious biometric registration programs, linking millions of citizens’ fingerprints and facial images to a centralized national identity number. Kenya has earlier implemented the Huduma Namba, a biometric national ID intended to consolidate service access, while simultaneously deploying biometric kits for voter registration through the Independent Electoral and Boundaries Commission. Similarly, in South Africa, biometric data plays a central role in both the national ID system and in social grant distribution, while Ghana has integrated biometrics into its electoral rolls and e-passport system. Even outside national ID registries, countries such as Tanzania and Uganda have tied biometric registration to mandatory SIM card verification, making mobile connectivity contingent on biometric capture.

The drive toward biometric registration is no longer experimental; it has become a core feature of Africa’s digital transformation, shaping how states interact with citizens and how citizens access rights, entitlements, and opportunities. Governments present these programs as solutions to pressing developmental challenges like streamlining service delivery, improving financial inclusion, and enhancing security. Yet, the scale and speed of deployment raise fundamental questions about governance, oversight, and sustainability. Different government ministries, departments, and agencies are responsible for procuring these technologies, with security-related agencies and those that require accurate citizen data, such as electoral commissions, leading the way. For instance, in Liberia, procurement and deployment of biometric systems include the National Identification Registry, Ministry of Foreign Affairs, Liberia Immigration Service, Liberia National Police, and the National Election Commission. Meanwhile, in Uganda, the main institutions responsible for managing and deploying these systems include the Uganda Police Force, the National Identification and Registration Authority (NIRA), the Electoral Commission, the Ministry of Science and Technology, and the Ministry of Internal Affairs.

Biometric technologies are procured from different countries, mainly outside Africa. For example, the government of Uganda procured CCTV surveillance systems from Huawei, a Chinese company, while it procured FinFisher from Gamma International Limited in the UK. Additionally, Uganda procured NIRA’s biometric system from Mühlbauer GmbH in Germany.

14. "World Bank," DigWatch, October 16, 2025, https://dig.watch/actor/world-bank.
15. “Harnessing the power of biometric technology in Africa,” Africa Smart Today, https://africasmarts.today/smart/harnessing-the-power-of-biometric-technology-in-africa/.
16. Agenda 2063, themed “The Africa We Want,” is Africa’s master plan for transforming Africa into the global powerhouse of the future. It was signed and committed to by the African governments during the AU’s 50th anniversary in May 2013. The declaration marked the re-dedication of Africa towards the attainment of the pan-African vision of an integrated, prosperous and peaceful Africa.
17. “Digital Identification and Biometrics In East Africa: Opportunities and Concerns”, SAIIA, November 9, 2023, https://saiia.org.za/research/digital-identification-and-biometrics-in-east-africa-opportunities-and-concerns/.
18. Tomas Statius, John-Allan Namu, Daniel Howden, and Lionel Faull, “Biometrics in Africa’s Elections,” Lighthouse Reports, May 24, 2022, https://www.lighthousereports.com/investigation/biometrics-and-the-enslavement-of-african-elections.

Expanding frontiers of biometric deployment in Africa

Biometric and digital identity technologies have moved far beyond their initial role in foundational national ID systems to become critical infrastructure across multiple sectors. Today, these technologies underpin a growing number of public and private services, shaping how individuals access rights, entitlements, and opportunities. From civil registration systems aimed at establishing legal identity for all, to electoral processes designed to safeguard the integrity of democratic participation, biometric ID systems are increasingly integrated into the core functions of governance.

Beyond traditional state services, biometric technologies are now being applied to migration management, SIM card registration, and even smart city initiatives, where they play a role in urban surveillance and the delivery of digital public services. These diverse applications reflect a broader trend: biometrics are no longer confined to niche, security-focused projects but are becoming a central pillar of Africa's digital transformation agenda.

The following sections explore some of the most prominent domains of biometric deployment, examining both their operational benefits and the critical challenges they raise, including privacy risks, exclusionary outcomes, and questions of accountability.

Biometric usage – civil registration

Biometrics, which include fingerprints, facial images, and iris scans, are being increasingly integrated into civil registration systems. By capturing unique biological and behavioral characteristics, countries aim to establish a "foundational identity" for citizens beginning at birth, making it easier to track life events like marriages and deaths.

The Rwanda Digital Acceleration Project was approved in 2021 and has seen investments in the modernization of the national ID system, including the introduction of a digital ID for online transactions and the digitization of civil registration records. In Nigeria, the Digital ID for Development project was approved in February 2020; the following year, technical assistance was provided for the implementation of the project, focusing among other things on strengthening legal frameworks, introducing data protection safeguards, and improving cybersecurity. Tunisia has benefited from technical assistance for the development of a roadmap for digital IDs. Support is also provided for the development of models for digital authentication and the operationalization of a unique citizen identifier.[19]

Fayda ("value" in Amharic), Ethiopia's biometric digital ID program, aimed to enroll all eligible adults by 2025.[20] A pilot phase launched in 2021 and completed in 2022, registered the first 100,000 individuals. The Ethiopian National Identity Program (NIDP) noted that the pilot revealed important lessons: national ID authorities should not be regarded as "one-stop shops" holding all personal data; instead, they should limit data collection and prioritize transparency, ensuring registrants are informed about when and how their data is used.[21] The NIDP reported over 1.4 million registrations, aiming to issue digital IDs to 10 million people in 2023.[22] Fayda is envisioned as the primary foundational ID system, replacing several functional IDs and integrating into the financial sector for "Know Your Customer" (KYC) purposes, the civil registry, and Ethiopia's broader digital economic transformation. Collected biometrics include fingerprints, iris scans, and facial data.[23]

Uganda's national biometric digital ID, Ndaga Muntu, was introduced in 2015 as mandatory for all citizens. Originating from the National Security Information System (NSIS) initiative previously launched in 2014 to reform civil registration ahead of the 2016 elections, Ndaga Muntu is required for accessing public services such as healthcare, travel passports and social grants, as well as private services like banking, SIM registration, education enrollment, and formal employment.[24]

Research by the Center for Human Rights and Global Justice, the Initiative for Social and Economic Rights, and Unwanted Witness confirms this, noting that Ndaga Muntu has caused significant exclusion, particularly among women, older persons, and marginalized groups hindering their ability to access basic services.[25]

In Zimbabwe, modernization of the legal ID system began in 2021, upgrading the national population registry and linking it with other services. The government announced an integrated digital system based on the updated register.[26] Digital ID is framed as part of Zimbabwe's digital transformation agenda, facilitating access to both public and private services.[27]

The Digital ID Transformation Strategy for the Gambia reflects a deliberate effort to position identity management as a catalyst for socio-economic transformation. Its vision is "to build a digital identity solution to enable Government, Citizens, and Businesses to participate in the digital economy effectively," and it emphasizes the role of identity not merely as an administrative tool but as an enabler of inclusive economic participation.[28] The limited publicly available details about the initiative suggest the Gambia is framing its digital ID not as a standalone project but as part of a broader digital economy agenda integrating identity into service delivery, commerce, and governance. However, the absence of explicit commitments on privacy oversight, data minimization, and independent accountability structures leaves open questions about the depth of rights protections in practice.

The rapid adoption of biometric-driven civil registration systems is redefining how identities are established and managed, but gaps in privacy protections and oversight risk turning these systems into tools of exclusion rather than empowerment. When foundational ID programs expand without strong safeguards, they can erode public trust and entrench systemic inequalities, limiting access to essential services and rights. This creates a dynamic where identity becomes not just a means of inclusion but also a mechanism of control, shaping how citizens engage with the state and how power is exercised through data.

While progress has been significant, such as Ethiopia's ambitious Fayda program and Uganda's Ndaga Muntu, implementation challenges, particularly around inclusion, privacy, and accountability, remain a concern.

Biometric migration

In West Africa, the adoption of biometric technologies has moved beyond national ID programs into the realm of migration governance and border control. Governments, regional alliances, and international actors now deploy biometric systems not only to facilitate travel and identification, but also to regulate mobility, monitor migration flows, and enforce new security regimes. These developments reflect a growing intersection between digital identity, sovereignty, and geopolitical influence in the region.

In West Africa, the regional Economic Community of West African States (ECOWAS) National Biometric Identity Card (ENBIC) was approved in 2015 to facilitate free movement for the 320 million citizens of the ECOWAS zone.[29] The card will make it possible for the citizens of member states to move around the ECOWAS area, serving as a residency permit, a passport, and proof of identity. It is expected that further functionalities, such as identification for e-commerce, will be added. Senegal was the first country to fully implement the scheme, while Ghana and Nigeria are among those following suit.[6] However, the newly formed Alliance of Sahel States (AES) has also announced plans for a new biometric passport to harmonize travel documents across the region.[30]

In March 2024, Burkina Faso secured $150 million in support from the World Bank's International Development Association to advance its Digital Acceleration Project and develop a biometric passport initiative aimed at strengthening AES regional connectivity and integration. On September 4, 2024, the country launched these new biometric passports. The passports were reportedly produced by the Chinese biometrics firm Emptech.[31]

This shift takes place against a broader backdrop where biometrics have become a central tool in immigration and border governance across West Africa. Interpol's West African Police Information System (WAPIS) is an interoperable biometric ID platform used to collect criminal-related data on West Afri-

19. "Digital identification in Africa: Frameworks and initiatives", Diplo, November 2022, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-identification-africa/.
20. Ethiopia has not achieved this target, however; rather, it shifted the goal. The government announced in May 2025 that it ultimately aims to enroll 90 million citizens by 2027. According to the National ID Program Office, more than 15 million Ethiopians have already registered for Fayda. Over one thousand active enrollment points have been established across the country. Source: "Ethiopia's Digital ID System Now Integrated Across 55 Key Institutions," ID Techwire, May 30, 2025, https://idtechwire.com/ethiopias-digital-id-system-now-integrated-across-55-key-institutions/.
21. "Digital Identification and Biometrics In East Africa: Opportunities and Concerns," SAIIA, November 9, 2023, https://saiia.org.za/research/digital-identification-and-biometrics-in-east-africa-opportunities-and-concerns/.
22. Gabriellah Abraham, "Commentary: Ethiopia's Digital ID Ecosystem: A Legal and Policy Review," Ethiopian Business Review, last updated May, 11, 2023, https://ethiopianbusinessreview.net/ethiopias-digital-id-ecosystem-a-legal-and-policy-review/
23. "Digital Identification and Biometrics In East Africa: Opportunities and Concerns," SAIIA, November 9, 2023, https://saiia.org.za/research/digital-identification-and-biometrics-in-east-africa-opportunities-and-concerns/.
24. Ibid.
25. Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness.Kampala, Uganda: June 8, 2021. https://www.unwantedwitness.org/download/uploads/Chased-Away-and-Left-to-Die-.pdf
26. Ayang McDonald, "Integrated digital system in Zimbabwe to enhance ID issuance, birth registration," Biometric Update, April 10, 2023, https://www.biometricupdate.com/202304/integrated-digital-system-in-zimbabwe-to-enhance-id-issuance-birth-registration.
27. Ayang Mcdonald, "Zimbabwe looks forward to digital ID rollout after population registry reform," Biometric Update, July 15, 2025, https://www.biometricupdate.com/202507/zimbabwe-looks-forward-to-digital-id-rollout-after-population-registry-reform.
28. "Gambia National Digital Identity Strategy," UNECA, October 24, 2023, https://www.uneca.org/sites/default/files/TCND/Digital%20ID%20Transformation%20Strategy%20_Gambia%20V_9.p df.
29. "Digital identification in Africa: Frameworks and initiatives," Diplo, November 2022, https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-identification-africa/.
30. Ayang Macdonald. Sahel states under military rule unveil common biometric passport Jan. 29. BiometricUpdate. January 27, 2025. https://www.biometricupdate.com/202501/sahel-states-under-military-rule-unveil-common-biometric-passport-jan-29,
31. Victor Chidubem, "European Biometric ID Program in West Africa: Between European External Border Securitization and ECOWAS Free Movement," African Security, Volume 18, Issue 3, May 4, 2025, https://doi.org/10.1080/19392206.2025.2491206.

can migrants, integrating it into EU-centralized and Interpol databases. Deployed by European security establishments, WAPIS enables monitoring of criminal records and tracking or controlling irregular migrant movements within the ECOWAS subregion. The pilot phase targeted Benin, Ghana, Mali, and Niger, countries that also completed the digitization of their police records.[32]

To complement WAPIS, the Automated Fingerprint Identification System (AFIS) has been rolled out in Niger and other states, yet weak civil registry systems persist, creating gaps in identity verification. Meanwhile, the EU continues to fund large-scale (€25–30 million) biometric civil registry projects in countries such as Senegal and Mali, implemented by Civipol, a public-private partnership that acts as a technical operator for the French Ministry of the Interior, delivering security and identification services in projects funded by development aid.[33, 34, 35]

In Niger, although a 2003 law authorized the issuance of national e-ID cards, high costs (2,000 CFAF, about €3) left many citizens unable to obtain them. This challenge mirrors the wider problem of "biometricization" across Africa, where over half the population lacks legal proof of identity, leaving many people *de jure* stateless.[36]

Such limited enrollment in national biometric ID systems has constrained identity construction and significantly shaped irregular migration patterns, especially in Niger. Migrants now face European external border systems that require biometric cross-matching at checkpoints, combined with state-led militarized restrictions, producing a coercive regime of "unfree movement" within ECOWAS.[37]

Biometric usage in elections

Across Africa, biometrics are no longer limited to civil identification and border management; they have become a central feature in electoral processes. As governments strive to enhance the integrity of elections, biometric technologies are increasingly being used to tackle long-standing issues such as accidental voter duplication listings in state electoral documents, multiple voting attempts by individual voters, and inaccurate voter rolls. This trend reflects both a political desire for more credible elections and a technological shift toward data-driven governance, though it also raises important questions about data protection, accessibility, and trust in electoral bodies.

Across Africa, governments are deploying biometric systems for voter registration to combat multiple voting, where individuals attempt to cast ballots multiple times in different locations, and to enhance the accuracy of voter rolls. During this process, citizens provide personal information such as their name, identification number, and residence details, along with biometric data like fingerprints and facial images, which are stored in a centralized voter database.[38] Registration is typically carried out by government officials using a Biometric Voter Registration (BVR) kit or a mobile biometric terminal.[39] On election day, voters must present either the receipt issued at registration or their official voter ID card. Before voting, the biometric de-duplication process removes duplicate entries, ensuring that each individual casts only one vote.[40]

Comparative insights show that while the use of biometric voting has grown quickly, the reasons for adopting it and the results achieved vary widely across countries. Widespread nationwide implementation has taken place in countries like Kenya, Ghana, and Nigeria, where BVR systems were introduced as part of major electoral reforms, often under intense

32. Thapelo Ndlovu, "SADC's Rocky Path: The Challenges of Biometric and Digital Identity Systems," Digital Southern Africa, Issue 3, April 2024, https://africaninternetrights.org/sites/default/files/Digital%20Rights%20Southern%20Africa_ED3-2.pdf.
33. Ibid.
34. Ibid.
35. The French government owns 40 percent of CIVIPOL's shares, while private security and defense companies Thales, Airbus, Idemia, and Défense Conseil International collectively own the remaining 60 percent.

See Stambøl, Eva Magdalena and Jegen, Leonie. The case of Civipol: Commodified mobility policing in West Africa and its colonial continuities. Statewatch: 2024.https://www.statewatch.org/analyses/2024/the-case-of-civipol-commodified-mobility-policing-in-west-africa-and-its-colonial-continuities/.

36. In May 2010, a group of experts met in Prato, Italy, to discuss the definition of a stateless person under international law. The meeting was organized by the United Nations High Commissioner for Refugees (UNHCR), and addressed both the interpretation of the definition of a de jure stateless person under Article 1(1) of the 1954 Convention Relating to the Status of Stateless Persons, and more generally the definition of a de facto stateless person, a condition recognized under international law for individuals with no nationality in any country.
37. Victor Chidubem, "European Biometric ID Program in West Africa: Between European External Border Securitization and ECOWAS Free Movement," African Security, Volume 18, Issue 3, May 4, 2025, (2025), accessed August 14, 2025, https://doi.org/10.1080/19392206.2025.2491206.
38. Deniz Yurdasen, "How Biometrics Is Becoming a Norm of Elections in Africa", Aratek Biometrics, September 30, 2022, https://www.aratek.co/news/how-biometrics-is-becoming-a-norm-of-elections-in-africa.
39. Ibid
40. Ibid.

public and international scrutiny. In contrast, some countries have taken a sector-specific approach, applying biometric systems to targeted areas rather than across the entire electoral process. In places like Zimbabwe and Uganda, where biometric voting has helped reduce obvious cases of voter duplication, it has not resolved deeper issues such as disputed voter rolls or allegations of manipulation, showing that technology alone cannot fix certain underlying governance challenges.

A critical but sometimes overlooked aspect of BVR systems is its deep entanglement with foundational national ID systems. In many African countries, electoral biometric data is not stored separately, instead it is cross-referenced with or directly integrated into national civil registries. While governments often justify this integration as a cost-saving measure and a way to improve population data accuracy, the implications go far beyond efficiency. Once voter data becomes part of a centralized identity infrastructure, it is no longer used solely for elections. Instead, it can be accessed by multiple state agencies for taxation, welfare distribution, border management, or even security surveillance. In this way, what begins as a tool for electoral integrity risks reinforcing patterns of exclusion and normalizing the repurposing of personal data across sectors, blurring the line between governance and surveillance.

For instance, when voter data becomes accessible to tax authorities, social protection agencies, border security, and law enforcement, the same information that allows a citizen to cast a ballot can also be used to track their movements, economic activities, or political affiliations. In contexts where democratic institutions are fragile or where ruling parties dominate the state apparatus, this creates the risk of digital repression. Governments can exploit centralized databases to identify and target opposition supporters, limit their access to state services, or intimidate dissidents through surveillance.

Moreover, the fear of being tracked or profiled may discourage individuals from engaging in political activities such as protests, union organizing, or voting for opposition candidates. This chilling effect erodes freedom of association and freedom of expression, both of which are foundational to democratic principles. In extreme cases, biometric systems could be used to deliberately disenfranchise marginalized groups, especially if access to voting is tied to having a national ID, leaving those without one unable to participate in elections.

For example, Uganda's National ID program, launched in 2014 and expanded under the Registration of Persons Act of 2015, has become deeply integrated into everyday life, making registration effectively mandatory. A National ID is now required to purchase a SIM card, access public education and healthcare, obtain a passport, open a bank account, or engage in many other basic services. This expansion has significantly increased the government's access to citizens' personal and biometric data, centralizing sensitive information—including fingerprints, facial images, and demographic details—into a single, powerful system. While initially promoted as a tool to improve service delivery and curb fraud, this centralized database gives the state an unprecedented level of oversight and control over its population.

Concerns are heightened by the absence of strong privacy protections and the program's history of mismanagement. Allegations—though denied by the government—of a major data breach in 2017, though denied by the government, exposed weaknesses in data security, and authorities have confirmed that biometric data is shared with telecommunications companies for SIM card verification.[41] Reports of corruption, such as enrollment officers soliciting bribes, further undermine public trust.[42] The integration of facial recognition technology raises even greater risks. In a context where freedom of expression and freedom of assembly are already under threat—with documented cases of security forces firing on protesters and targeting journalists and activists—the National ID database could easily be used to track dissent and suppress opposition.[43]

41. Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness.Kampala, Uganda: June 8, 2021. https://www.unwantedwitness.org/download/uploads/Chased-Away-and-Left-to-Die-.pdf
42. 11 Arrested over corruption in National ID Registration. Parliament of Uganda. August 5, 2025. https://www.parliament.go.ug/news/4170/11-arrested-over-corruption-national-id-registration-muhoozi
43. Michael Karanicolas, "Serious Concerns Around Uganda's National Biometric ID Program," Yale Law School Information Society Project, November 20, 2019 https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/serious-concerns-around-ugandas-national-biometric-id-program.

Table 1: Biometric voting systems deployment in Africa between 2007 and 2025

Region	Countries that deployed biometrics in their elections
West Africa	Ghana, Nigeria, Liberia, Sierra Leone, Senegal, Togo, Niger
East Africa	Kenya, Uganda, Tanzania, Rwanda, Somaliland
Southern Africa	Zimbabwe, South Africa, Zambia, Botswana, Lesotho, Eswatini, Namibia
Central Africa	Cameroon, Congo, Angola
North Africa	Egypt, Libya

Other usages of biometrics on the continent

Beyond elections, border control, and foundational ID systems, biometric technologies in Africa are finding application across a diverse range of sectors from trade facilitation and urban management to civil service monitoring and transport security. These deployments reflect a broader shift toward digital governance ecosystems, where biometric data becomes an integral component of service delivery, public safety, and economic integration.

One rising biometric utility usage is the number of urban safety and "smart city" projects across the continent.[44] Zimbabwe has recently integrated biometric and AI technology into urban management. In the capital Harare, an AI-based smart traffic system developed domestically by state-owned telecom provider TelOne under the Safe City project deploys sensors and cameras at intersections and major roads.[45] Its aims include easing congestion, reducing road accidents, enforcing traffic laws, and improving overall urban safety. The project is expected to expand to other major cities. Zimbabwe also envisions a smart city initiative for a newly planned capital on the outskirts of Harare, though it has faced criticism from digital rights advocates concerned about surveillance, data privacy, and public accountability.[46]

In Nairobi, the question of whether its own safe city project could lead to a loss of privacy looms large for millions of Kenyans, whose every move is captured by the flash of a CCTV camera at intersections across the capital. Kenya's Integrated Public Safety Communication and Surveillance System (IPSCSS) operates nearly 2,000 fully functional CCTV cameras equipped with facial recognition capabilities.[47] The project was developed and is managed by Huawei in partnership with Safaricom. These surveillance cameras are connected to integrated biometric databases, pulling data from various sources to support public security operations. However, there is no mechanism for auditing the data or algorithms driving this system. This lack of transparency creates a closed loop, where the system's effectiveness cannot be independently verified because the very data needed to assess its impact is controlled and processed within the system itself.

In East Africa, Uganda and Kenya have also begun biometric enrollment of civil servants, citing chronic absenteeism as a key motivation. The problem, which undermines service delivery in multiple sectors, was highlighted as far back as 2010 when the World Bank reported absentee rates of 15 to 25 percent among teachers in some African countries.[48] Through biometric attendance systems, governments aim to ensure accurate payroll management, reduce "ghost" workers, and improve institutional efficiency.

In several African countries, biometric data collection has been integrated into mobile network operations, often as part of SIM card registration requirements. For instance, in Tanzania, Nigeria, and Zambia, legislation mandates that telecom operators capture fingerprints, facial images, or other biometric identifiers before issuing SIM cards.[49] This approach is intended to enhance security, reduce identity fraud, and improve traceability in telecommunications, particularly in financial transactions and mobile money services. In other countries, telecom operators collect biometric data voluntarily, motivated by the same goals of fraud prevention, subscriber authentication, and regulatory compliance, but without a formal legal mandate.

44. Thobekile Matimbe, "Smart Cities, Safe Citizens – Zimbabwe," Paradigm Initiative, February 6, 2024, https://paradigmhq.org/report/smart-cities-safe-citizens-zimbabwe/.
45. "Zimbabwe steps up home-grown smart traffic management system," Bulawayo 24 News, June 19, 2025, https://bulawayo24.com/index-id-news-sc-national-byo-254081.html.
46. Ayang Mcdonald, "Integrated digital system in Zimbabwe to enhance ID issuance, birth registration," Biometric Update, April 10, 2023, https://www.biometricupdate.com/202304/integrated-digital-system-in-zimbabwe-to-enhance-id-issuance-birth-registration.
47. Bulelani Jili, "The Rise of Chinese Surveillance Technology in Africa (part 5 of 6)," Electronic Privacy Information Center, September 22, 2022, https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-5-of-6/.
48. "Public administration : Africa adopts biometric clocking of civil servants", Africa News Agency, April 6, 2023, https://africa-news-agency.com/public-administration-africa-adopts-biometric-clocking-of-civil-servants/.
49. "Londa 2021," Paradigm Initiative, May 5, 2022, https://paradigmhq.org/wp-content/uploads/2022/05/Londa-English-Report-real.pdf.

Citizens in Mali receive their first biometric voter cards during a distribution event led by Secretary General of the Ministry of Territorial Administration Baba Hamane Maiga.

Source: Reuters/LE PICTORIUM

While the integration of biometrics into mobile systems can improve security and service reliability, it also introduces significant privacy and data protection concerns. The collection, storage, and use of sensitive biometric data, especially facial recognition, creates risks of misuse, unauthorized surveillance, and data breaches. In Uganda, Tanzania, and Zimbabwe, there is documented evidence that facial recognition technology has been used by state actors to monitor, track, and identify government critics or opposition figures, particularly during election periods.[50] Such practices raise concerns about civil liberties, freedom of expression, and political repression, as individuals may be monitored or targeted without due process.

Moreover, the involvement of both public authorities and private companies in biometric collection complicates accountability. Telecom providers often store and manage vast amounts of personal data, sometimes with insufficient oversight or independent auditing.In cases where governments request access to these datasets, the lack of robust legal frameworks and enforcement mechanisms can create opportunities for abuse, including unauthorized surveillance, profiling, or targeting of specific groups. These dynamics highlight the urgent need for comprehensive data protection laws, independent regulatory oversight, and transparency in both public and private biometric initiatives.

Biometric applications are also expanding into aviation and transportation hubs. Some African airports are introducing biometric e-gates and passenger verification systems to streamline boarding, enhance security screening, and meet international travel security standards.[51] Nigeria is installing forty e-gates at five airports, while South Africa is adding twenty-four to King Shaka and OR Tambo International Airports.[52] Other countries on the continent are also in various stages of implementing this technology, but specific figures for the entire continent are not available in the available data.[53] While these measures can speed up passenger processing, they also add to the volume of personal biometric data being collected, raising questions about cross-border data sharing and alignment with global privacy regulations.

50. Bulelani Jili, "The Spread of Surveillance Technology in Africa Stirs Security Concerns," Africa Center for Strategic Studies, December 11, 2020, https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/.
51. E-gates to be installed at all international airports in Nigeria. PT World. February 21, 2024. https://www.passengerterminaltoday.com/news/security/e-gates-to-be-installed-at-all-international-airports-in-nigeria.html
52. South Africa's Airport Authority Begins Biometric Upgrade. ID Tech. June 15, 2024. https://idtechwire.com/south-africas-airport-authority-begins-biometric-upgrade/
53. ""ABC eGates: Making Travel Easy as 1-2-3," Valour Consultancy Newsletter, April 9, 2024, https://valourconsultancy.com/abc-egates-making-travel-easy-as-1-2-3/.

Human rights standards in biometric deployment

Biometric and digital identity adoption follows clear regional patterns or clusters, shaped by shared political histories, economic structures, and external funding sources. For instance, West African states, including Ghana, Nigeria, Sierra Leone, and Senegal, have been at the forefront of biometric deployment, often driven by regional trends and harmonization efforts. This push has been heavily influenced by donor-supported initiatives, with major backing from organizations such as the United Nations Development Programme (UNDP), the European Union, the World Bank, and emerging frameworks like GovStack, which promote interoperable, open-source solutions for digital public infrastructure.[54] These external actors provide not only technical expertise and funding but also policy blueprints, meaning that West African states often adopt similar system designs and standards, facilitating cross-border coordination for issues such as migration management, trade, and regional elections. ECOWAS has also played a role in encouraging convergence, particularly around civil registration and voter management systems.

In contrast, Southern African countries, such as Botswana, Namibia, and Lesotho, have tended to adopt biometric systems more gradually, relying primarily on domestic resources and political will rather than external funding. These states often take a more incremental approach, piloting smaller-scale projects before committing to full-scale rollouts. The focus in this region is frequently on service delivery modernization, such as improving access to health care, social welfare, and civil registration, rather than rapid, large-scale electoral or migration-focused deployments.

It is a clear pattern that African states are outsourcing core identification infrastructure to foreign entities while simultaneously granting them privileged access to sensitive biometric datasets, which enables governments to expand surveillance capacities. Many contracts for biometric systems are awarded through opaque procurement processes, often shielded from public scrutiny under the guise of national security. These arrangements facilitate rent-seeking by elites and prevent citizens from holding either governments or corporations accountable.

The findings from the ICT Works study reveal a significant transparency gap in how African governments procure advanced digital technologies such as biometric systems, artificial intelligence (AI), and facial recognition tools.[55] With only 38 percent of survey participants reporting knowledge of government purchases of these technologies, the majority of citizens remain uninformed about critical decisions that have profound implications for privacy, civil liberties, and democratic governance. The regional disparities among respondents are particularly striking. In Nigeria, where 80 percent of respondents were aware of government procurement, there appears to be a relatively higher level of public engagement and discourse, potentially due to more active civil society groups and media coverage. By contrast, Uganda and Liberia reflect stark deficits in transparency, with 70 percent and 88 percent of respondents respectively unaware of whether their governments have acquired these technologies. These findings align with broader concerns about opaque procurement practices, where contracts are often negotiated behind closed doors with foreign vendors and financed through donor funding or loans. Such secrecy erodes digital sovereignty, leaving citizens unaware of how their personal data will be collected, stored, and potentially shared across borders. Moreover, the lack of informed public debate allows governments and corporations to expand surveillance infrastructures unchecked, deepening the potential for rights abuses.

The deployment of digital ID systems has been met with both optimism and concern in the continent. On the one hand, these systems are hailed for their potential to improve service delivery, streamline governance, and enable secure transactions. On the other hand, their implementation has raised critical human rights questions, especially regarding the storage and handling of sensitive personal information. Because digital ID systems store highly personal and sensitive data, privacy must be paramount. Cyberattacks, data leaks, or intentional misuse of information can have severe consequences for individuals, particularly in authoritarian or politically unstable contexts. Without strong legal and technical safeguard mechanisms, state critics, journalists, and members of the political opposition remain especially vulnerable to surveillance, harassment, and repression.

These concerns speak directly to global human rights obligations. International frameworks such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and regional instruments like the African Charter on Human and Peoples' Rights guarantee the rights to privacy, equality before the law, and freedom from discrimination.[56, 57] Likewise, the principles embedded in the EU's General Data Protection Regulation (GDPR), including data minimization, purpose limitation, and informed consent, offer benchmarks for responsible digital ID design and operation.[58] When digital identity systems fail to adhere to these principles, they risk undermining not only individual rights but also the public trust essential for their successful adoption.

To understand the safeguards that ought to guide the design and deployment of digital ID systems, the Centre for Internet and Society (CIS) has developed an evaluation framework anchored on three interlinked tests: risk-based, rights-based, and rule of law-based assessments.[59] Together, these tests provide governments, civil society, and regulators with a structured way to assess whether identity systems are truly serving citizens or exposing them to new layers of vulnerability.

The risk-based test emphasizes whether potential harms associated with digital ID, such as profiling, mass surveillance, or exclusion, are adequately assessed before systems are deployed. Digital ID programs combine biometric technologies, big data processing, and extensive databases of personal and demographic information, all of which carry inherent risks. Laws and governance frameworks must therefore require thorough and continuous risk assessments, not only during design but also throughout the life cycle of the system. Risks such as data breaches, unauthorized use, errors in authentication, and mission creep must be anticipated, with mechanisms for prevention and recovery. Importantly, the framework stresses that exclusions often arise not from poor implementation alone, but from the very design of biometric ID systems: for instance, when elderly citizens, manual laborers, or persons with disabilities are unable to reliably provide fingerprints or other biometrics. The test therefore asks, are there adequate mechanisms to prevent digital ID from becoming a barrier to accessing essential services and entitlements?

The rights-based test situates digital ID within the broader landscape of fundamental rights, particularly the right to privacy, freedom of expression, and access to information. Citizens must be able to know when and how their digital ID is being used. They must also have the right to access their personal data, obtain a copy, and correct inaccuracies. Crucially, the framework demands that restrictions on privacy arising from digital ID be necessary, proportionate, and justified in pursuit of a legitimate aim. Blanket data collection, indefinite storage, or extraneous use of personal information, without informed consent, cannot be justified under this standard. Beyond privacy, the rights-based test also addresses exclusion: do digital ID systems uphold equality and non-discrimination, or do they compound existing marginalizations?

Finally, the rule of law-based tests underscores the institutional and legal safeguards that should accompany any digital ID system. This includes clear legal backing for all purposes of ID use, explicit definition of the state and private actors that are permitted to handle ID data, and the principle of purpose limitation, which requires that each new use of data must obtain fresh, informed consent. Robust grievance redress mechanisms are central to this test, ensuring accountability, transparency, and user-friendliness. Individuals should have avenues to challenge misuse, obtain remedies, and hold both state and private actors to account. Strong penalties for civil and criminal violations must also be embedded in law as a deterrence. Equally important is the independence of oversight bodies, without which regulatory capture or political interference can hollow out protections.

Uganda offers a telling case study. According to CIPESA, its digital ID system collects an extensive range of personal data, including "name, date of birth, gender, information on citizenship, place of birth, details of parents, clan, tribe, ethnicity, spouse, education, tax information, personal biometrics information… as well as any other information as may be required."[60] This approach directly conflicts with the principle of data minimization, a key standard in responsible digital ID implementation. Beyond privacy concerns, such extensive data collection raises the risk of ethnic profiling and increased state surveillance. These risks are further amplified by the fact that Uganda's Ndaga Muntu ID is set to become the sole valid method of identification for accessing both public and private services, potentially excluding individuals who cannot or choose not to enroll in the system.[61]

Moreover, the growing biometric economy extends beyond governance into the politics of mobility and migration. For migrants and displaced people, compulsory fingerprinting or facial recognition can lead to political exclusion or conditional inclusion, what some describe as "inclusive exclusion." In fragile democratic contexts, these technologies are not only

54. Melody Musoni, Ennatu Domingo, and Elvis Ogah, "Digital ID systems in Africa: Challenges, risks and opportunities", ECDPM, December 2023,https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-ECDPM-Discussion-Paper-360-2023.pdf.
55. "What Digital Technology Systems Are Procured by African Governments?" ICT Works, October 14, 2021,https://www.ictworks.org/digital-technology-systems-procured-african-governments/.
56. The Universal Declaration of Human Rights outlines fundamental rights and freedoms that belong to every person. It emphasizes the inherent dignity and equal rights of all individuals, including the right to life, liberty, and security of person.
57. "UN International Covenant on Civil and Political Rights," UNOCHR, December 16, 1966, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.
58. "GDPR Article 98: Review of other Union legal acts on data protection," Official Journal of the European Union, April 5, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.
59. "Governing ID: Introducing our Evaluation Framework," Centre for Internet and Society, March 2, 2020, https://cis-india.org/internet-governance/blog/governing-id-introducing-our-evaluation-framework.
60. Alice Aparo, "Uganda's Digital ID System Hinders Citizens' Access to Social Services," CIPESA, October 10, 2023, https://cipesa.org/2023/10/ugandas-digital-id-system-hinders-citizens-access-to-social-services/.
61. Ibid.

Officials assist a voter with biometric registration during national elections in Côte d'Ivoire, part of efforts to enhance transparency and voter authentication.

Source: REUTERS/Virginie Nguyen Hoang /Hans Lucas

tools of service delivery but also instruments of surveillance and control, making the question of who owns, manages, and secures identity data a deeply political one.

Reports have revealed that "smart city" initiatives, which integrate technologies like CCTV and license plate recognition, are being used for unauthorized surveillance of individuals, with a notable absence of oversight.[62] This practice directly infringes upon the fundamental human right to privacy, as codified in the Universal Declaration of Human Rights.[63] A clear example is the Huawei Safe City Project in Kampala, Uganda, a $126 million initiative that deployed 1,800 CCTV cameras equipped with facial recognition capabilities, all connected to a national police command center.[64]

62. "Surveillance/Spyware: An Impediment to Civil Society, HRDs and Journalists in East & Southern Africa," Unwanted Witness, June 2025, https://www.unwantedwitness.org/wp-content/uploads/2025/06/Report-06.06.2025-FINAL.pdf.
63. UN Human Rights Office. Spyware and surveillance: Threats to privacy and human rights growing, UN report warns. September 16, 2022. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.
64. Frank Kisakye, "New report exposes African 'smart cities' as hubs for digital surveillance," The Observer, August 13, 2025, https://observer.ug/technology/new-report-exposes-african-smart-cities-as-hubs-for-digital-surveillance/.

Unbundling the supply chain

The vendors that make up Africa's biometric and digital ID ecosystem can broadly be categorized into three interlinked tiers. At the top are the core technology providers, usually large multinational firms that develop and control biometric matching engines, credential issuance platforms, and large-scale data systems that underpin national ID projects. The second tier consists of specialized hardware suppliers and system integrators, which provide enrollment kits, biometric devices, and software integration necessary for deployment on the ground. Finally, there are local and regional intermediaries, often African companies, which handle field operations, adapt imported technologies to local realities, and manage enrollment processes. Together, these three tiers illustrate a layered ecosystem where global expertise, technical infrastructure, and local execution intersect to deliver biometric identity systems across the continent.

Most African biometric and digital ID systems typically rely on automated fingerprint identification systems (AFIS).These systems are capable of searching over a billion fingerprint records in a second with near-perfect accuracy.[65] When combined with other modalities such as iris and facial recognition, these platforms become automated *biometric* identification systems—powerful engines that enable everything from voter verification to border control. In countries where paper-based registries are unreliable or incomplete, these systems provide a degree of certainty that traditional methods cannot, ensuring individual uniqueness and reducing duplication.[66]

Enrollment typically involves capturing fingerprints, facial photographs, and sometimes iris scans, which are then stored as mathematical templates instead of images.[67] This approach enables faster, more secure matching in large national databases and allows the same infrastructure to be used across sectors such as elections, healthcare, SIM card registration, and digital banking.

The deployment of biometric and digital identity systems across Africa is far from a simple technological rollout. It is a multi-layered, transnational enterprise that stretches from corporate research labs in Europe and Asia to enrollment centers in rural African communities. Each fingerprint scan, facial recognition capture, or digital ID issuance is the culmination of a complex network of technology developers, local contractors, infrastructure operators, and international partners, each operating under distinct objectives and commercial incentives. Surrounding core technologies is a diverse ecosystem of actors. The market is heavily influenced by large, primarily European, vendors who supply the core biometric matching engines, credential issuance systems, and large-scale data infrastructure. Alongside them are also Chinese manufacturers supplying hardware components, and a smaller tier of African firms that serve as intermediaries or subcontractors providing equipment, software integration, and on-the-ground enrollment teams.

Global technology providers

The foundation of Africa's biometric systems rests on international technology companies that develop core algorithms, secure chips, and specialized hardware. Prominent suppliers include Idemia (France), Thales (France), Veridos (Germany), Semlex (Belgium), and Huawei (China). These companies determine the accuracy, speed, and security of biometric applications, and their dominance means most governments rely heavily on their intellectual property. The technical specifications set by these firms often shape the architecture of national ID systems, influencing not just performance but also policy decisions related to data management and security.

In this landscape, French company Idemia is perhaps the dominant player, operating in twenty-five African countries and managing the continent's largest biometric database in Nigeria.[68] Its platforms have been used for both electoral and national ID systems. Belgium's Semlex operates Côte d'Ivoire's national register and identity card program, while Germany's Veridos has been active in Uganda, Zambia, and Morocco. France's IN Groupe and Germany's Mühlbauer have also delivered national projects, including Mozambique's ID system.[69] These companies often win contracts backed by loans from multilateral institutions such as the World Bank, allowing governments, sometimes in severe fiscal distress, to undertake large-scale identity programs.

65. Craig Watson, Gregory Fiumara, Elham Tabassi, Su Lan Cheng, Patricia Flanagan, and Wayne Salamon, "Fingerprint Vendor Technology Evaluation," NISTIR 8034, December 18, 2014, https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8034.pdf.
66. "Biometric Data," World Bank ID4D, https://id4d.worldbank.org/guide/biometric-data.
67. ,"Proprietary Fingerprint Template Evaluations (PFT) Overview," National Institute of Standard Technology (NIST), March 26, 2025,https://www.nist.gov/programs-projects/proprietary-fingerprint-template-evaluations-pft-overview.
68. "Biometric identification a coveted African market," The Africa Report, June 22, 2020, https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/.
69. Ibid.

An individual's fingerprint is scanned using biometric equipment during an election process in Côte d'Ivoire.

Source: REUTERS/Thierry Gouegnon

Local intermediaries and regional contractors

Yet the ecosystem is not entirely foreign-dominated. South Africa's BioRugged, Secure ID, and Ideco, Nigeria's Seamfix, and Ghana's Margins Group have built reputations supplying biometric kits, integrating systems, and managing field enrollments. Their role is often to adapt global technology to local conditions, navigating logistical and cultural challenges that outsiders might overlook. South Africa's Waymark was successful in 2010 in managing Guinea's electoral register but has been criticized for its lack of experience in the field.[70] However, several companies are gradually expanding their market presence, especially as subcontractors to larger and more internationalized groups.[71] Still, the market has yet to see an African firm capable of matching the scale, R&D capacity, and political leverage of the major European providers.

Following the delivery of core technologies, local and regional actors integrate these systems into national projects. Companies such as BioRugged, Seamfix, and Margins Group manage logistics, train operators, and coordinate large-scale registration exercises. These intermediaries are crucial in bridging global technology with local implementation, yet their involvement sometimes introduces political influence and elite capture into ostensibly neutral technical projects. In Mozambique, for instance, the politically connected printing firm Artes Gráficas, owned by the Sidat family, partnered with Laxton (South Africa–China) to supply biometric voter kits ahead of the 2018 elections.[72]

Laxton played a key role in this project by providing a complete range of solutions to support voter registration. This included supplying voter ID printer kits that enable on-the-spot production and issuance of voter ID cards, along with essential accessories such as solar panels and photo backdrops to ensure operations continue smoothly in areas without reliable electricity. Laxton also delivered advanced identity registration software to securely manage and protect voter data, as well as a central server and software for streamlined, centralized data management and integration. To build local capacity, the company conducted in-country training programs to equip teams with the knowledge and skills needed to operate and maintain the systems. In addition, nationwide technical support and warranty services were provided to ensure ongoing assistance and long-term system reliability, creating a sustainable voter registration infrastructure.[73]

70. "Guinea Electoral Body appoints South African Firm" Associated Press, February 15, 2013, , https://www.washingtonexaminer.com/?p=2332138.
71. "Biometric identification a coveted African market," The Africa Report, June 22, 2020, https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/.
72. Olivia Solon, Tomas Statius, Beatriz Ramalho da Silva, Nalinee Maleeyakul, Jessica Loudis, Tom Giles, Crofton Black, and Daniel Howden. "False Promise of Biometrics," Lighthouse Reports, June 5, 2024, https://www.lighthousereports.com/investigation/false-promise-of-biometrics/.
73. Laxton Election Solution has partnered with Mozambique's Technical Secretariat of the Electoral Administration (STAE) to register sixteen million and eight hundred thousand voters ahead of the countries election, see "Record-Breaking 16.8 Million Voters Registered for Mozambique's 2024 Elections," Laxton, https://www.laxton.com/case-studies/mozambiques-elections-2024.

Risks and complexities in Africa's biometric expansion

Infrastructure and data hosting

The deployment of biometric systems requires robust hosting and secure digital infrastructure. Companies such as Huawei have become prominent in building national data centers across Africa. For instance, in Malawi, Huawei developed the National Data Center to support both governmental and private sector applications.[74] Similar infrastructure projects exist in Uganda, Zambia, South Africa, Mozambique, and Senegal, creating regional hubs for identity data management. While these facilities enhance operational capability, reliance on external providers raises questions of national sovereignty, as control over critical identity data remains partially in the hands of foreign companies.

Africa's biometric and digital ID ecosystems are built through a deeply interconnected global supply chain that combines international technology expertise with local implementation. At the top are powerful multinational companies, mostly European and Chinese, which design and control the core technologies, such as biometric matching engines and large-scale data management platforms, influencing not only the technical architecture but also policy decisions around data management and security. Beneath them are regional and local companies that integrate these imported systems, manage enrollment processes, and adapt technologies to local realities. While these local actors are essential for field operations, they remain dependent on foreign vendors for the critical technologies that drive the systems.

This arrangement allows governments to deploy advanced identity systems quickly, supporting sectors like elections, healthcare, telecommunications, and digital finance. However, it also creates structural dependencies and political risks. Reliance on foreign providers means that sensitive biometric data, fingerprints, facial scans, and other personal information, is often stored or managed externally, raising serious concerns about data sovereignty and national security. Moreover, the integration of politically connected local contractors introduces opportunities for corruption and elite capture, as seen in cases where voter registration projects became vehicles for patronage. The result is a system that delivers technical efficiency while leaving governments vulnerable to external influence, limited autonomy over their citizens' data, and growing public distrust in how these identity systems are governed.

This section examines the key issues arising in the deployment of Africa's biometric systems: their proliferation, the integration of security cooperation projects, strategic risks from private sector dominance, and illustrative cases that highlight the political and commercial intricacies of deployment.

Several incidents demonstrate how foreign vendors, when left unchecked, can create long-term structural dependencies that compromise data sovereignty, human rights, and national security. These vendors often control critical infrastructure, software, and even access to raw biometric data, giving them significant leverage over governments. This dynamic can lead to situations where states are locked into expensive proprietary systems, unable to transition to alternative providers without major disruptions to essential services such as voting, civil registration, or border management. It can also result in opaque data-sharing agreements where sensitive citizen information is stored or processed abroad, beyond the reach of domestic laws. For African states, this underscores the urgent need to rethink procurement strategies, strengthen regulatory safeguards, and demand transparency and independent auditing in all digital ID projects to prevent corporate interests and foreign political agendas from undermining national autonomy and public trust.

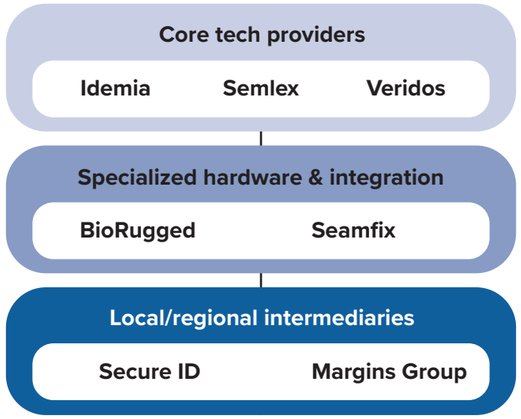
Proliferation and fragmentation of biometric systems

At least thirty-seven African countries now operate multiple biometric systems spanning voter registration, national IDs, e-passports, SIM registration, and sector-specific programs.[75] In several cases, countries manage five or more parallel applications, often with overlapping mandates and partial coverage. For example, in Nigeria, the National Identity Number, Bank Verification Number enrollment, drivers license, travel passport, and voter registration involve separate data collection processes.

Voter registration initiatives and national ID programs represent the bulk of deployments in the continent, but many remain incomplete or in the enrollment phase.[76] The lack of integration compels citizens to repeatedly provide biometric data to different agencies, increasing operational costs, duplication of effort, and the potential for human rights and data violations. This fragmentation highlights the challenges of achieving a single, authoritative source of identity while maintaining operational efficiency across multiple sectors.

74. Thapelo Ndlovu, "SADC's Rocky Path: The Challenges of Biometric and Digital Identity Systems," Digital Southern Africa, Issue 3, April 2024, https://africaninternetrights.org/sites/default/files/Digital%20Rights%20Southern%20Africa_ED3-2.pdf.
75. "Where and How in Africa Is Biometrics Being Used?" Use of Biometrics within Sub-Saharan Refugee Communities, Dec. 1, 2013, https://www.jstor.org/stable/resrep23612.5.
76. Ibid.

Fig. 1: Biometric and digital ID ecosystem in Africa



A pictorial representation of the biometric and digital ID ecosystem in Africa based on the research findings.

Security cooperation and cross-border programs

In some cases, biometric deployments are closely linked to international security initiatives. The West African Police Information System (WAPIS), supported by European partners, enables cross-border sharing of criminal data. Similarly, the EU has funded biometric civil registries in Senegal and Mali, often implemented by Civipol, the French Ministry of Interior's development arm.[77]

These initiatives enhance regional security coordination, but they also underscore the interplay between development objectives and security agendas, raising considerations about data sovereignty and the influence of external actors in shaping domestic biometric systems. The erosion of data sovereignty is not just a technical issue; it has deep political, economic, and social consequences. When foreign governments, international organizations, or private companies control or influence how a country's biometric data is collected, stored, and used, it creates structural dependencies that can limit national autonomy and harm citizens.

First, foreign control over data can shift decision-making power away from domestic institutions. For example, when biometric registries are tied to international security initiatives, external actors may dictate how the data is used or shared, even if it conflicts with local priorities. This can undermine national policies on law enforcement, border management, or even voting processes, leaving a country unable to fully govern its own population data.

Second, it creates risks of misuse and surveillance. Biometric databases contain highly sensitive information like fingerprints, facial scans, and demographic details. If managed externally, there is a danger that this data could be exploited for geopolitical purposes, commercial gain, or intelligence gathering without the knowledge or consent of the country or its citizens. This turns biometric systems into tools of control rather than public service.

Third, economic dependency deepens when core biometric systems are built and maintained by foreign companies or donors. Countries may become locked into costly contracts for technology upgrades and maintenance, while losing opportunities to build local capacity or tech industries. Worse still, the data itself, a valuable economic resource, is effectively owned or monetized by others, preventing the country from leveraging it for domestic innovation or digital economy growth.

Finally, the public's trust is eroded. When citizens suspect that their personal data is vulnerable to foreign interference or misuse, they are less likely to engage with government programs, from voting to accessing social services. This can exacerbate inequalities and undermine the legitimacy of state institutions.

Strategic risks of private sector dominance

Private sector participation brings advanced technology, operational efficiency, and rapid deployment capabilities. Yet it also introduces strategic vulnerabilities. Companies that build, integrate, and maintain biometric systems often retain leverage over governments, creating opportunities for long-term dependency.

77. Victor Chidubem, "European Biometric ID Program in West Africa: Between European External Border Securitization and ECOWAS Free Movement," African Security, Volume 18, Issue 3, May 4, 2025, https://doi.org/10.1080/19392206.2025.2491206.

A particular risk is "data ransom," where private companies controlling critical biometric databases can leverage this access to negotiate more favorable contract terms.[78] Governments dependent on these systems for essential services have limited alternatives, increasing their susceptibility to vendor pressure and reducing bargaining power.

An illustrative case of political and commercial complexities

The fragility of government–corporate relationships can disrupt even well-funded projects. In South Africa, Idemia is currently embroiled in a high-profile lawsuit over a multimillion-dollar biometric security contract that was to supply biometric and facial recognition systems for the country's airports. Valued at 380 million rand (approximately US $20.8 million), the project aimed to introduce automated border control, electronic gates, and a "single token" passenger identification system across South Africa's airport network. In its announcement, Airports Company South Africa (ACSA) provided no detailed explanation for the cancellation, stating only that the termination was in accordance with the terms of the service-level agreement, which permits a sixty-day notice period.[79] Idemia will be allowed to complete any work already underway before its full withdrawal. The deal was initially awarded in August 2023 to a joint partnership between Idemia South Africa and Infoverge Solutions, with ambitious plans to roll out Idemia's ID2Travel biometric passenger flow system nationwide. However, by July 2024, tensions between the two companies became public when Infoverge filed a court petition to have the contract annulled. These internal disputes, combined with mounting scrutiny, ultimately contributed to the project's collapse.[80]

This case underscores that while government corporate relationships often appear unified, they can fracture under competing interests, exposing vulnerabilities in procurement processes and raising concerns about transparency and accountability. It also highlights how biometric infrastructure projects carry not only technological risks but also political and commercial complexities that can undermine public trust.

While this ecosystem promises efficiency, it also embeds asymmetries. The reliance on foreign providers raises questions about data governance and the long-term cost of maintaining proprietary systems.[81]

A recent example illustrates this multi-tiered system in action. Under the World Bank's Madagascar Digital Governance and Identification Management System Project known as PRODIGY, Madagascar chose Idemia and Thales as preferred technology partners for a new national biometric identity system, awarding a contract worth just over €18 million. According to procurement details reported by Africa Business, hardware provider Laxton[82] will receive €12.2 million of the total for biometric enrollment equipment and related software.[83]

The biometric upgrade forms a key work package under PRODIGY, a US $140 million initiative launched in 2020 to modernize civil registration, establish a unique identifier from birth, and streamline government service delivery. Earlier procurement records show that several international suppliers, including Thales, Idemia, Veridos, Semlex, and newer entrant Augentic, had competed for different PRODIGY lots as far back as late 2021[84]. The new award indicates that Idemia and Thales will provide the core biometric matching and credential-issuance platforms, while Laxton supplies the enrollment kits used in field registration campaigns across Madagascar's twenty-three regions.[85]

Kenya illustrates the risks of rolling out biometric systems without strong governance. In January 2023, the country's High Court halted the launch of Huduma Namba, a national biometric ID that collected fingerprints, contact details, and occupational data, citing the lack of a clear regulatory framework to protect citizens' privacy.[86] This was not the first sign of concern. Back in 2019, when questioned about the program, then–ICT Principal Secretary Jerome Ochieng stated, "Data is the new oil."[87] His remark captured both the economic potential and

78. "False Promise of Biometrics," Light House Reports, June 5, 2024, https://www.lighthousereports.com/investigation/false-promise-of-biometrics/.
79. Idemia contract with South Africa airport authority terminated. BiometricUpdate. August 27, 2024. https://www.biometricupdate.com/202408/idemia-contract-with-south-africa-airport-authority-terminated
80. Ibid.
81. Alpondith, "IDEMIA: A Tech Giant with Hidden Risks," Forward Sight, March 16, 2025,https://medium.com/forward-sight/idemia-a-tech-giant-with-hidden-risks-8838851c640e.
82. "Laxton: Empowering Citizens Advancing Nations," Laxton, https://www.laxton.com/.
83. "Madagascar Awards €18M Biometric ID Contract to Idemia, Thales Partnership," ID Tech Wire, May 15, 2025 https://idtechwire.com/madagascar-awards-e18m-biometric-id-contract-to-idemia-thales-partnership/
84. Newcomers flourishing on African market worry biometrics leaders. Africa Intelligence. November 22, 2021. https://www.africaintelligence.com/the-continent/2021/11/22/newcomers-flourishing-on-african-market-worry-biometrics-leaders,109706283-ge0
85. Ibid.
86. Madeleine Speed, "Activists sound alarm over African biometric ID projects," Al Jazeera, December 10, 2020, https://www.aljazeera.com/economy/2020/12/10/activists-sound-alarm-over-african-biometric-id-projects.
87. Christine Mungai, "Kenya's Huduma: Data commodification and government tyranny", Al Jazeera, August 6, 2019, https://www.aljazeera.com/opinions/2019/8/6/kenyas-huduma-data-commodification-and-government-tyranny

Kenyan President Mwai Kibaki launches Kenya's biometric voter registration exercise, registering himself as a voter.

Source: REUTERS/Thomas Mukoya

the political stakes of biometric data: while it can drive innovation and economic growth, without proper safeguards it can just as easily become a tool for exploitation, surveillance, and loss of citizen trust.[88]

Meanwhile, the UN Human Rights Committee concluded found that Mauritius's 2013 National Identity Card Act violates its citizens' privacy rights, as there are no sufficient guarantees that the fingerprints and other biometric data stored on the identity card will be securely protected.[89] The committee's decision responded to a complaint filed by a Mauritian national who claimed that the country's smart identity card system has contravened his privacy right under Mauritius's constitution and the International Covenant on Civil and Political Rights.[90]

Mauritius launched its first identity card scheme back in 1995. In order to prevent multiple applications for an identity card with falsified names or information, the authority amended its legislation in 2009 with additional biometric data requirements and increased penalties for noncompliance. A new smart identity card was subsequently launched in 2013 to replace the old one. In addition to the printed information such as name, date of birth, and gender, the new electronic ID card also contained a microchip storing data including fingerprints that can be read by an e-reader. The government stated that the fingerprint requirement was essential to tackle identity fraud.[91]

The rollout of biometric identity systems across Africa highlights a recurring pattern: ambitious modernization projects are being driven by foreign technology providers and international financing, while governance and privacy safeguards lag behind. Cases from Kenya and Mauritius reveal the risks when such systems are deployed without adequate oversight. Together, these examples show that while biometric systems can drive efficiency and modernization, without robust legal safeguards, independent oversight, and clear data governance frameworks, they risk becoming tools of surveillance and control rather than instruments of empowerment.

88. Ibid.
89. "Mauritius: Storing biometric data on identity cards violates privacy," UN Human Rights Committee, July 22, 2021, https://www.ohchr.org/en/press-releases/2021/07/mauritius-storing-biometric-data-identity-cards-violates-privacy-un-human.
90. "International Covenant on Civil and Political Rights," UN Human Rights Committee, September 16, 2021, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=PdKcxTJ93MIiikF7I5IZPFOERSDX0gclWmO8xVJnZOhI9vFD9VEA4YiVMHSrvc56bBRVrkgWuuI2RnGqhlbatClyub1vI3Z6X%2B4EJ3JUmrl%3D.
91. "Prime Minister Launches New National Identity Card", NewsGov, September 17, 2013, https://govmu.org/EN/newsgov/SitePages/2013/Prime-Minister-Launches-New-National-Identity-Card.aspx.

Legal and oversight frameworks across Africa

The expansion of digital ID and biometric systems across Africa is unfolding against a patchwork of legal and regulatory frameworks. While these systems promise efficiency and inclusivity, their deployment often outpaces the development of clear, enforceable data governance rules. This misalignment exposes citizens to heightened risks of surveillance, exclusion, and misuse of personal information.

In their current state, many programs operate in fragile legal contexts. Of Africa's fifty-five states, only thirty-seven have enacted national data protection laws, and many of these lack robust safeguards such as truly independent oversight bodies.[92] Eighteen countries have yet to pass comprehensive privacy and data protection legislation at all. Even where laws exist, regulatory oversight remains inconsistent, and the governance of biometric processing is often handled through scattered provisions rather than integrated, coherent frameworks. This leaves gaps in regulating how biometric data is collected, processed, stored, and shared, whether in SIM card registration, voter rolls, or national ID systems.

These shortcomings are particularly problematic given the sensitivity of biometric identifiers. Without stringent safeguards, the same infrastructure that enables efficient service delivery can also facilitate mass surveillance, data breaches, identity theft, and discriminatory exclusion. The risks are amplified in contexts where political opposition and civil society operate under restrictive conditions.

At the continental level, the African Union Convention on Cybersecurity and Personal Data Protection, widely known as the Malabo Convention, represents the most comprehensive regional effort to address these challenges. Adopted in 2014 but only entering into force in June 2023 after Mauritania's ratification, the convention obliges its state parties to implement protective measures at the national level. Article 8 enshrines the principle that "any form of data processing respects the fundamental freedoms and rights of natural persons," while Article 10(4) specifically restricts the processing of biometric data unless authorized by a legally established protection agency, such as a data protection office.[93] Equally significant is Article 14(6)(a), which prohibits transferring personal data to a non–African Union member state unless that state guarantees an adequate level of privacy protection. These provisions aim to establish a continent-wide baseline for ethical data practices, addressing both domestic and cross-border risks. The Malabo Convention has been ratified by Angola, Cape Verde, Congo, Ghana, Guinea, Mauritania, Mauritius, Mozambique, Namibia, Niger, Rwanda, Senegal, São Tomé and Príncipe, Togo, and Zambia.

Another prominent initiative is the Smart Africa Alliance (SAA), which unites thirty-nine African heads of state and government under the goal of accelerating economic development through ICT.[94] Its Smart Africa Digital ID Blueprint (Smart Africa 2020), led by Benin, sets out governance structures, principles, procedures, and technical standards to build trusted digital ID systems. A core proposal of this blueprint is the Smart Africa Trust Alliance (SATA), a public-private partnership aimed at fostering interoperable digital ID systems among SAA members. SATA's purpose is to establish mutual trust between governments, enabling smoother cross-border transactions and ultimately increasing intra-African trade. Ghana, Zimbabwe, Gabon, Rwanda, Tunisia, and Guinea formally signed SATA during the Transform Africa Summit in early 2023. While SATA aspires to break down trust barriers and address interoperability challenges, awareness campaigns remain essential to explain its added value amid overlapping initiatives such as the World Bank's West Africa Unique Identification for Regional Integration and Inclusion project.[95] Clarification is also needed on how SATA aligns with the continental digital interoperability framework being developed under the African Union.

Complementing these efforts, the United Nations Economic Commission for Africa (UNECA) and its partners launched the Digital Identity, Digital Trade, and Digital Economy (DITE) initiative.[96] DITE established the Center of Excellence on Digital Identity, Trade, and Economy to provide technical advice, promote minimum standards, and safeguard inclusion, trust, and harmonization between civil registration and digital ID systems

92. ,"Biometrics and Digital Identity in Africa," Cipesa, April 2024, https://cipesa.org/wp-content/files/Biometrics_and_Digital_Identity_in_Africa_Brief.pdf.
93. Kebene Wodajo, "Societal and Structural Risks of Biometric ID: Towards People's Right to Privacy," *Science, Technology and Society*, October 17, 2024, https://journals.sagepub.com/doi/10.1177/09717218241281941?int.sj-abstract.similar-articles.8#fn4-09717218241281941.
94. "Smart Africa Board brings together the thirty-one heads of state and government along with the International Telecommunication Union, the African Union Commission as well as Smart Africa's Platinum members, with one common goal: to transform Africa into a single digital market." Smart Africa, https://www.wipo.int/edocs/mdocs/africa/en/wipo_webinar_rba_2021_1/wipo_webinar_rba_2021_1_p6.pdf.
95. Samia Melhem, "WEST AFRICA UNIQUE IDENTITY FOR REGIONAL INTEGRATION AND INCLUSION (WURI) – P161329,"iD4Africa, 2018, https://www.id4africa.com/2018_event/Presentations/InF4/2-4-0_The_World_Bank_Samia_Melhen.pdf.
96. "What is Digital Identity, Digital Trade and Digital Economy for Africa?" UNECA, https://www.uneca.org/dite-for-africa/what-is-digital-identity%2C-digital-trade-and-digital-economy-for-africa%3F.

across the continent. The center intends to serve as a go-to source for technical advice, assisting countries with their digital ID and digital economy initiatives. It will also conduct research on the many aspects of the digital economy and coordinate related work across the Commission. Specifically, the center will promote the harmonization of standards across member states, support the creation of regulations to ensure security, and encourage increased investment in infrastructure. It will also focus on building the capacity and skills of key players, including the private sector, so they can take advantage of the innovation and job creation opportunities that digitalization offers. The center will also support the creation of a digital common market under the African Continental Free Trade Area (AfCFTA). This initiative is designed to help African countries, ICT operators, and citizens benefit from a continent-wide digital market

A primary goal for the center is to define and support the implementation of minimum standards for digital ID systems to ensure they are inclusive, trustworthy, and interoperable. It will also work on harmonizing civil registration and digital ID systems. Furthermore, following a mandate from the African Union Specialized Technical Committee on Trade, Industry, and Minerals (STC-TIM), the center will collaborate with the African Union Commission and other partners to develop and implement a comprehensive strategy for digital ID, trade, and economy for Africa.

Complementary frameworks such as 2022's African Union Data Policy Framework reinforce these commitments.[97] By recognizing not only individual privacy but also collective privacy rights, the framework widens the scope of data protection in the African context. Other AU initiatives including the Digital Transformation Strategy for Africa and AfCFTA have also underscored that ethical processing of biometric digital identities is central to building trust in Africa's digital economy.[98]

While thirty-seven African countries have enacted standalone data protection laws, only twenty-nine have operationalized data protection authorities, and many of these authorities lack the political and financial independence needed to function effectively.[99] Simply having data protection laws or other legal instruments in place is only the first step toward governing biometric deployment. To truly safeguard citizens and ensure accountability, stronger mechanisms for oversight and redress must be established. These include independent regulatory bodies with enforcement powers, clear pathways for individuals to challenge misuse of their data, and mandatory impact assessments to evaluate risks before biometric systems are rolled out

97. Kebene Wodajo, "Societal and Structural Risks of Biometric ID: Towards People's Right to Privacy," *Science, Technology and Society*, October 17, 2024, https://journals.sagepub.com/doi/10.1177/09717218241281941?int.sj-abstract.similar-articles.8#fn4-09717218241281941.
98. Ibid.
99. Olumide Babalola, 'Gbenga Sesan,Steven Akomian, Jackline Akello, Tsandzana Dercio and Bonface Witaba, "Data Protection Authorities in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of their Existence on the Continent," Paradigm Initiative, July 2021, https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf.

Policy recommendations

The rapid deployment of biometric and digital identity systems across Africa requires governance models that prioritize human rights, privacy, and democratic accountability. Without strong safeguards, these systems risk increasing surveillance, entrenching exclusion, and eroding public trust. The following recommendations outline what should be done, the issues they aim to address, the actors responsible for implementation, and the ultimate purpose of these actions.

1. Establish independent oversight bodies

Independent oversight agencies with full autonomy over budget allocation, enforcement decisions, and regulatory revisions should be created and strengthened. This responds to the problem of political interference and regulatory capture in the management of biometric systems, where oversight bodies are often controlled by ministries or dominant political elites.

The main actors responsible are national governments and legislators, who must introduce legal reforms to ensure agency independence. The purpose is to safeguard individuals against unlawful surveillance, build public trust, and guarantee that biometric systems are used lawfully and transparently.

2. Enact comprehensive and enforceable legal frameworks

Robust legislation should be adopted to govern the entire lifecycle of biometric data, including collection, storage, processing, retention, sharing, and deletion. This addresses the lack of clear regulations, which leaves biometric data vulnerable to misuse, unauthorized sharing, and "function creep," where data collected for one purpose is used for unrelated activities such as policing or surveillance.

Legislators, supported by national data protection authorities and regional organizations such as the African Union, are the key actors. The goal is to align national laws with instruments like the AU's Malabo Convention and international standards such as Convention 108+, ensuring that biometric data use remains lawful, necessary, proportional, and subject to public accountability.

3. Ensure transparent and inclusive procurement processes

Procurement practices for biometric and surveillance technologies must become transparent, competitive, and inclusive of public participation. This addresses the problem of opaque procurement processes that foster corruption, dependence on foreign monopolies, and poor system design while excluding affected communities.

National governments, regional bodies, and civil society organizations are the responsible actors. They should work together to monitor procurement and advocate for disclosure of contracts and technical specifications. The aim is to prevent power concentration among a few state agencies or private vendors, ensure procurement serves the public interest, and preserve analogue alternatives for individuals unable to enroll in biometric systems.

4. Integrate human rights due diligence for all contracts

Human rights due diligence should be made a binding requirement for corporations, international technology providers, and donors involved in biometric projects. This responds to the issue of unregulated private sector involvement and donor-funded initiatives that may unintentionally harm vulnerable communities or exacerbate systemic discrimination. Corporations, international donors, and national governments must collaborate to enforce due diligence as part of contracts and project planning. The purpose is to minimize harm, respect individual rights, and ensure that systems evolve based on the feedback of affected populations and continuous assessment.

5. Create continuous oversight and remedy mechanisms

Ongoing monitoring should be established through independent audits, user feedback systems, and transparent public reporting. This would address the lack of accountability mechanisms after deployment, where violations often go unresolved and structural problems remain hidden. The key actors are national governments, civil society organizations, and judicial bodies, which must work together to design and enforce oversight frameworks. The aim is to provide both individual and collective remedies for rights violations, compensate affected individuals, and drive systemic reforms in governance and technical design.

6. Safeguard electoral integrity and prevent over-integration

Strict separation between biometric voter registration systems and national ID databases should be maintained, with clear legal controls over data sharing. This addresses the risk of over-integration, where combining electoral and foundational ID systems increases state surveillance capabilities and excludes citizens without national IDs from voting. Legislators, election management bodies, and data protection authorities are the primary actors responsible. The goal is to protect electoral integrity, prevent misuse of electoral data, and ensure that all citizens can exercise their voting rights without unnecessary barriers.

7. Embed a rights-based governance model

Biometric systems should be anchored in a governance model that prioritizes privacy, equality, and non-discrimination. This addresses the problem of biometric deployments being driven by efficiency and modernization goals without adequate consideration of human rights and democratic freedoms. The actors involved include national governments, civil society groups, regional bodies, and the media, who should promote public debate and consultation before large-scale rollouts. The aim is to ensure that biometric technologies serve the public good, protect fundamental rights, and foster inclusive, accountable governance.

8. Promote regional cooperation and harmonization

Regional cooperation should be strengthened through the African Union and subregional bodies such as ECOWAS, EAC, and SADC to develop shared standards for biometric systems. This would address the issue of fragmented, country-specific deployments that hinder cross-border services like migration management, regional elections, and trade facilitation. Smart Africa and the Digital Identity, Trade, and Economy (DITE) initiative can serve as accelerators by coordinating efforts, providing technical support, and fostering collaboration among countries. The key actors are regional organizations and national governments working collaboratively. The purpose is to reduce costs through collective bargaining, enable interoperability, and prevent cross-border surveillance abuses by establishing consistent privacy and data protection safeguards.

9. Build domestic technical capacity and reduce foreign dependency

Investment in local technical expertise and innovation ecosystems should be prioritized to design, manage, and secure biometric systems. This addresses the problem of heavy reliance on foreign technology providers, which threatens national sovereignty and limits the ability to tailor systems to local needs. National governments, supported by development partners, universities, and private sector stakeholders, are responsible for implementing this recommendation through training programs and funding for local companies. The goal is to increase national ownership of biometric infrastructure, develop context-specific solutions, create jobs in the technology sector, and reduce vulnerability to foreign influence or exploitation.

Conclusion

The rise of biometric and digital identification systems across Africa represents both a tremendous opportunity and a grave challenge. These technologies have the potential to improve service delivery, enhance electoral credibility, and create more efficient governance structures. However, without strong legal protections, independent oversight, and transparent governance, they also risk eroding privacy, undermining civil liberties, and exacerbating social inequalities.

This research highlights the central role of foreign vendors in shaping Africa's biometric landscape. The heavy reliance on external technology providers has created a vendor-driven ecosystem, where national sovereignty over data and identity infrastructure is increasingly compromised. This means that when critical national datasets are stored on foreign platforms or managed by external companies, countries become dependent on foreign technology providers. This dependency can lead to high costs for maintenance and upgrades, limited bargaining power, and the loss of opportunities to develop local tech industries. Other risks include disruption of democratic processes like elections, national security risks due to the sensitivity of the data, and weakening legal and policy authority. The convergence of electoral and national ID systems further amplifies these risks, expanding state surveillance capacities and disenfranchising vulnerable populations.

To safeguard human rights and democratic accountability, African states must prioritize the creation of rights-based governance frameworks. This includes harmonizing national laws with continental standards such as the Malabo Convention, empowering independent regulators, and fostering meaningful public participation. Governments, civil society, and development partners must work collaboratively to ensure that biometric systems are designed and deployed in ways that prioritize privacy, consent, non-discrimination, and transparency.

Ultimately, the future of biometric and digital identification in Africa hinges on political will. If left unchecked, these systems could become tools of control and exclusion. But with proper governance and accountability mechanisms, they can be harnessed to build more inclusive, transparent, and rights-respecting societies. The choice lies not in the technology itself, but in how it is governed and whose interests it serves.

Appendix

1: Data protection legislation and complementary laws affecting biometric data processing across Africa

Country	Data protection and complementary legislation
Angola	Data Protection Law (Law no. 22/11, 17 June 2011)
Botswana	Data Protection Law 2018
Cameroon	Law No. 2024/017 on the Protection of Personal Data
Comoros	2019 Personal Data Protection Law
Eswatini	
Lesotho	Data Protection Act (2013)
Madagascar	Madagascar's Law No. 2014-038, 2014.
Malawi	Draft
Mauritius	Data Protection Act 2004 (DPA 2004)
Mozambique	No
Seychelles	
Zambia	Data Protection Act No. 3 of 2021
Zimbabwe	Data Protection Act gazetted on the 3rd of December 2021
East Africa	
Burundi	No
Djibouti	No
DRC	No
Eritrea	No
Ethiopia	Draft
Kenya	Kenya's Data Protection Act 2019
Tanzania	Personal Information Protection Act 11, 2022
Rwanda	Law No. 058/2021 Relating to the Protection of Personal Data and Privacy (the Law) 15 October 2021.
Somalia	Data Protection Act 005, passed in March 2023
South Sudan	No
Sudan	No
Uganda	Data Protection and Privacy Act of 2019

Country	Data protection and complementary legislation
ECOWAS	
Burkina Faso	Law N°010- 2004/AN 2007)
Chad	No
Cabo Verde	Law 133-V-2001 on the Protection of Personal Data
Cote d'Ivoire	Data Protection Law of 2013
Gabon	Law No. 001/2011
Gambia	No
Ghana	The Data Protection Act, 2012 (Act 843)
Guinea	Law No. L/2016/037/AN
Guinea-Bissau	No
Liberia	No
Mali	Law No. 2013/015
Mauritania	Law No. 2017-020 (Adopted by the National Assembly in 2017, but has not yet come into effect)
Niger	
Nigeria	Nigeria Data Protection Act, 2023
Senegal	Law No. 2008-12 on the protection of personal data
Sierra Leone	No
Togo	Law No. 2019-014 (DPA Law
Maghreb	
Algeria	Law No. 18-07of 2018 on the protection of personal data for Algeria
Libya	No
Morocco	The Consumer Protection Law No.31-08; the Cybersecurity Law No.05-20; and the Right of Access to Information Law No.31-13
Tunisia	National Authority for the Protection of Personal Data (INPDP)

2: Comprehensive overview of the vendors and the type of biometrics provided

Country	Adoption of Biometric ID System	Purpose of Biometrics	Type of Biometric	Vendor who deployed
Angola	Yes (2008 elections)	Service delivery	Fingerprint, Facial	ANY Security Printing Company PLC
Botswana	Yes	Service delivery	Fingerprint	Morpho South Africa (which has merged with IDEMIA Smart Identity)
Cameroon	Yes (2013 elections)	Service delivery	Fingerprint	AUGENTIC
Comoros	Yes (2015 elections)	Service delivery	Facial	Belgium's Semlex Group
Eswatini	No			
Lesotho	Yes (2002 elections)	Service delivery	Fingerprint	PRIMES
Madagascar			Fingerprint	Belgium's Semlex Group
Malawi	Yes (2019 elections)	Service delivery	Fingerprint	
Mauritius				
Mozambique	Yes (2008 elections)		Fingerprint, Facial	Belgium's Semlex Group and Mühlbauer
Seychelles				
Zambia	Yes (2011 elections)	Service delivery	Fingerprint, Facial Biometric	Veridos (MOSIP)
Zimbabwe	Yes (2017 elections)	Service delivery, Immigration	Fingerprint, Iris, Facial	Belgium's Semlex Group
Burundi				No information available
Djibouti	No information available	No information available	No information available	No information available
DRC	No information available	No information available	No information available	Belgium's Semlex Group
Eritrea				
Ethiopia	Yes	Service delivery	Fingerprint, Facial	Laxton, Tech5, In Groupe, Idemia, Toppan Security
Kenya	Yes	Service delivery	Fingerprint, Facial, Iris	Idex biometrics, Innovatrics, IB, BioID, Idemia
Tanzania	No information available	Service delivery, Immigration	Fingerprint, Facial	HID Global
Rwanda			Fingerprint, Facial	Belgium's Semlex Group
Somalia				Belgium's Semlex Group
South Sudan				No information available
Sudan	No information available	No information available	Fingerprint, Facial	Smiles, Thales, Uqudo
Tanzania	Yes (2010)	Service delivery		
Uganda	Yes (2011 elections)			Veridos

Country	Adoption of Biometric ID System	Purpose of Biometrics	Type of Biometric	Vendor who deployed
Burkina Faso	Yes (2013)			
Chad	Yes (2016 elections)			Belgium's Semlex Group
Cabo Verde	Yes	Service delivery (security infrastructure)	Facial Biometric	Accura Scan
Cote d'Ivoire	Yes (2010 elections)			Belgium's Semlex Group
Gabon				Belgium's Semlex Group
Gambia	Yes (2011 elections)			
Ghana	Yes (2012 elections)			
Guinea	Yes (2010 elections)	Service delivery	Facial, Fingerprint	M2M (MOSIP)
Guinea-Bissau		Service delivery	Fingerprint	Belgium's Semlex Group
Liberia	Yes (2017 elections)			No information Available
Mali	Yes (2013 elections)	Service delivery, Immigration	Facial, Fingerprint	Oberthur Technologies (Idemia)
Mauritania	Yes (2010)			
Niger	Yes (2016 elections)			No information available
Nigeria	Yes (2007 elections)	Service delivery	Facial, Fingerprint	IDEMIA Smart Identity
Senegal	Yes (2007 elections)	Immigration, elections		Belgium's Semlex Group
Sierra Leone	Yes (2012 elections)			No information available
Togo	Yes (2007 elections)	Service delivery		No information available
Algeria				No information available
Libya	No information available	No information available	No information available	Belgium's Semlex Group
Morocco	Yes (2016 elections)	Service delivery, Election, Immigration	No information available	Veridos & Idemia, Modular Open-Source Identity Platform (MOSIP)
Tunisia	Yes	Service delivery	Fingerprint, Facial	E-Houwiya

Atlantic Council Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Stephen Achilles
Elliot Ackerman
*Gina F. Adams
Timothy D. Adams
*Michael Andersson
Ilker Baburoglu
Alain Bejjani
Colleen Bell
Peter J. Beshar
*Karan Bhatia
Stephen Biegun
Linden P. Blue
Brad Bondi
John Bonsell
Philip M. Breedlove
David L. Caplan
Samantha A. Carl-Yoder
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
George Chopivsky
Wesley K. Clark
Kellyanne Conway
*Helima Croft
Ankit N. Desai
*Lawrence Di Rita
Dante A. Disparte
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Joseph Durso
Richard Edelman
Oren Eisner
Stuart E. Eizenstat
Mark T. Esper
Christopher W.K. Fetzer
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
*Meg Gentle
Thomas H. Glocer
John B. Goodman
Sherri W. Goodman
Marcel Grisnigt
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Robin Hayes
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Keoki Jackson
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Karen Karniol-Tambour
*Andre Kelleners
John E. Klein
Ratko Knežević
C. Jeffrey Knittel
Joseph Konzelmann
Keith J. Krach
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Diane Leopold
Andrew J.P. Levy
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Roger R. Martella Jr.
Judith A. Miller
Dariusz Mioduski
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Mary Claire Murphy
Scott Nathan
Julia Nesheiwat
Edward J. Newberry
Franco Nuschese
Robert O'Brien
*Ahmet M. Ören
Ana I. Palacio
*Kostas Pantazopoulos
David H. Petraeus
Elizabeth Frost Pierson
*Lisa Pollina
Daniel B. Poneman
Robert Portman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Laura J. Richardson
Thomas J. Ridge
Gary Rieschel
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Wendy R. Sherman
Gregg Sherrill
Jeff Shockey
Kris Singh
Varun Sivaram
Walter Slocombe
Christopher Smith
Clifford M. Sobel
Michael S. Steele
Richard J.A. Steele
Mary Streett
Nader Tavakoli
*Gil Tenzer
*Frances F. Townsend
Melanne Verveer
Tyson Voelkel
Kemba Walden
Michael F. Walsh
*Peter Weinberg
Ronald Weiser
*Al Williams
Ben Wilson
Maciej Witucki
Neal S. Wolin
Tod D. Wolters
*Jenny Wood
Alan Yang
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik

*Executive Committee Members

List as of August 15, 2025

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org