Africa Tech For Development Initiative

27TH MAY 2025

AFRICA TECH FOR DEVELOPMENT INITIATIVE (AFRICA4DEV) SUBMISSION TO THE OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS (OHCHR) CALL FOR INPUT ON DISCRIMINATION AND UNEQUAL ENJOYMENT OF THE RIGHT TO PRIVACY IN THE CONTEXT OF DATA COLLECTION AND PROCESSING.

Introduction

Africa Tech for Development Initiative (Africa4Dev) is a Pan-African nonprofit organization committed to leveraging responsible technology, especially Artificial Intelligence (AI), to address systemic inequalities, promote youth and women empowerment, and build inclusive digital futures. Our organization works at the intersection of ethics, innovation, governance, and rights, with a strong focus on equitable digital transformation across the continent.

Summary of Input:

Africa4Dev welcomes the opportunity to contribute to the OHCHR report and shares deep concerns regarding the discriminatory and unequal enjoyment of the right to privacy arising from biased data collection and processing practices. Our submission is informed by community-based research, regional consultations with civil society and digital rights actors, and case studies from public service sectors, digital platforms, and AI governance ecosystems across Sub-Saharan Africa.

A. DISCRIMINATORY DATA PRACTICES

1. Public Services

In Nigeria national ID systems such as the NIMC[1] collect biometric and personal data to facilitate access to welfare, healthcare, and education. However, many marginalized populations, including women in rural areas and undocumented migrants, face barriers in registration, often due to limited documentation or digital illiteracy. This results in discriminatory exclusion from basic services, economic and social benefits. Also in distributing government economic empowerment, those without digital ID are deprived from accessing government grants such as loans to farmers and business owners, education grants, health waivers etc.

Kenya has taken a significant step forward in its identity management with the introduction of the Maisha Namba and the accompanying Maisha Card in 2023. This new digital ID system aims to simplify how Kenyans access essential services by providing a unique identifier assigned at birth, linked to a secure ID card and a digital counterpart[2].

The implementation of the third-generation ID, also known as the Maisha Namba, has faced criticism for not adequately addressing the identification and registration of historically marginalised groups in Kenya. Civil society organisations in Kenya have consistently raised concerns through media briefings and the courts regarding the implementation of third-generation IDs. They are calling for legislative measures to protect data privacy, ensure meaningful public engagement, and prioritize the registration of historically marginalised groups[3].

Members of stateless communities in Kenya also face significant challenges due to their lack of nationality documents. While some individuals from the Pemba, Makonde, and Shona communities were granted citizenship, many did not register or identify as Kenyans during the process. Although this initiative initially showed promise in addressing statelessness in the country, it has since stagnated, lacking documented guidelines and any plans for registering individuals who were excluded from the initial process. This situation represents a profound injustice, as a growing population of stateless individuals of Burundian, Congolese, and Rwandan descent face citizenship discrimination and marginalisation, despite having lived in the country for close to fifty years[4].

---

[1] NIMC, 'About Us' https://nimc.gov.ng/about-nimc accessed 13th May 2025
[2] Aratek, 'The New Kenyan ID Card: Maisha Namba Explained' (November 25th 2024) https://www.aratek.co/news/the-new-kenyan-id-card-maisha-namba-explained accessed 13th May 2025
[3] Fred Nasubo, 'Maisha Namba: Third-Gen ID Excludes the Historically Marginalised' (The Elephant December 5th, 2024), https://www.theelephant.info/analysis/2024/12/05/maisha-namba-third-gen-id-excludes-the-historically-marginalised/ accessed 13th May 2025
[4] ibid

Digital systems used in public service delivery may use exclusionary algorithms that deny access to certain groups For instance employment systems used in a highly tribalized state may exclude those from particular tribes or regions from having equal employment opportunity like other favoured tribes. This system could also unjustly exclude CVs submitted from certain tribes since the system alone determines who gets employed without public scrutiny of the employment process.

2. Limited Informed Consent and Data Exploitation

Marginalized groups often lack awareness of their data rights or how their information is used, leading to exploitation by digital platforms, government systems, or commercial apps.

In schools, children are often victims of data harvesting. The introduction of digital technologies into learning, as in children's lives overall, brings with it new risks and new pathways to familiar risks. Risks may be introduced simply because the EdTech products and their terms and conditions have not been designed with children's rights in mind[5].

Human Rights Watch reviewed 165 EdTech products, of which 89% engaged in data practices that put children's rights at risk, undermined or actively violated them[6]. Companies monitored children without their consent and knowledge, harvested data on what they do, who they are, where they live or study, and who their family and friends are, to the extent that the only way to protect themselves from this invasion is by throwing "the device away in the trash," the report concluded.

The majority of the learning platforms sent or allowed access to children's data to advertising technology (AdTech) companies, many of which belong to whole supply chains owned by the most powerful companies like Amazon, Facebook, Google and Microsoft. From there, advancing algorithms analyse and profile children, piece together more data from other public or private sources to create detailed profiles that are sold to advertisers, data brokers and anyone else who may be interested to target groups of people with similar characteristics online. Such inferred profiles of children can then be used to enable behavioural manipulation, over time[7].

In contexts like social protection or refugee registration, access to vital services is sometimes made conditional on consent to data collection thereby making refusal practically impossible for vulnerable individuals. This coercive data practices places marginalized groups in a position where they have no other choice but to succumb to the terms and conditions.

---

[5] United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, January 2023 <https://www.unicef.org/media/134131/file/Child%20Protection%20in%20Digital%20Education%20Technical%20Note.pdf> accessed 15th May 2025

[6] Velis Lava, 'Many EdTech companies exploit children's data, says Human Rights Watch report' (May 26, 2022) <https://www.edds-education.org/post/many-edtech-companies-exploit-children-s-data-says-human-rights-watch-report> accessed 15th May 2025

[7] ibid

3. Gender-Specific Harms

Women and girls are subjects of frequent risks of online abuse, cyberstalking, and unauthorized data exposure, which discourage their digital participation. Cyberviolence harms women and girls by curtailing their rights to freedom of expression and lowering their confidence and self-esteem. A report from Plan International shows that 50 percent of girls said they face more online harassment than street harassment[8].

Cyber violence is not gender neutral: women and girls are exposed to online violence more frequently than men. Globally, 38 percent of women have directly experienced online abuse. Women aged 18 to 24, in particular, are deemed at greater risk of being exposed to every form of cyber violence[9]. Sadly, this trend has also been increasing across Europe and Central Asia, in various forms such as online harassment, cyberbullying, cyberstalking, grooming for sexual purposes, sex trolling and physical threats.

Due to systemic gender gaps in access to smartphones, internet, and tech education, women are both underrepresented in the digital labor force and overexposed to exploitative platforms such as data-for-cash schemes or predatory gig work.

4. Surveillance and Repression

Governments often fail to adequately inform the public about their surveillance activities, and even where surveillance tools are initially rolled out for legitimate goals, they can easily be repurposed, often serving ends for which they were not originally intended.

Targeting of human rights defenders and minority groups has become somewhat prevalent. Governments and private actors in some African countries use digital surveillance to monitor civil society, particularly Human Rights, LGBTQ+ activists, ethnic minorities, and Equality advocates. Data is sometimes shared across state agencies without proper safeguards, leading to harassment or legal persecution.

The invasive nature of surveillance can lead to a chilling effect on free expression and association. Marginalized groups may hesitate to engage in political activities or community organizing due to fear of being monitored. This self-censorship undermines their ability to advocate for their rights and express dissent.

---

[8] Hyeonsoo Jeon and Umutai Dauletova, 'Cyberviolence disempowers women and girls and threatens their fundamental rights' (UNDP November 25th, 2021), <https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights> accessed 16th May 2025

[9] ibid

Moreover, surveillance technologies can create a false narrative about individuals, resulting in profiling based on race, ethnicity, or socio-economic status. The misapplication of surveillance data can lead to unjust scrutiny, reinforcing stereotypes while compounding the socio-political challenges faced by these communities.

Another notable case is the treatment of Black activists during the Black Lives Matter movement. Law enforcement agencies employed surveillance tactics, such as facial recognition technology, to monitor protests. This has raised concerns regarding racial profiling and the excessive targeting of African American individuals, undermining their right to dissent and assemble peacefully[10].

In the United Kingdom, the impact of surveillance has been evident among the LGBTQ+ community, particularly during the enactment of the Investigatory Powers Act. Increased monitoring of online communications has fostered anxiety surrounding privacy rights, discouraging individuals from expressing their identities openly[11]. These case studies collectively highlight the disproportionate impact of surveillance on marginalized groups, revealing systemic biases that persist within national security frameworks.

Ultimately, the impact of surveillance on privacy rights illustrates a critical tension between national security interests and individual liberties. Marginalized migrants and internally displaced persons are often subjected to biometric data collection without transparency or recourse mechanisms. These datasets may be shared with third-party vendors or governments with minimal oversight.

5. Digital Colonialism and Extractive Data Practices

Most international tech companies often gather extensive behavioral and biometric data from Africans particularly amongst low-income users using free or subsidized platforms but repatriate the economic value to global North markets without reinvesting in local communities.

Kenya's High Court had ordered Worldcoin, the biometric cryptocurrency initiative co-founded by OpenAI's Sam Altman, to delete all biometric data collected from Kenyan citizens who were promised USD50. The court found that Worldcoin's data collection practices violated Kenya's Data Protection Act of 2019[12]. It is likely the promised USD50 formed a nonnegotiable part of the terms and conditions for processing, therefore vitiating any potential consent obtained from the iris providers.

---

[10] Just Law Editorial, 'The Impact of Surveillance on Marginalized Groups and Society' (January 2, 2025), <https://thejustlaws.com/impact-of-surveillance-on-marginalized-groups/> accessed 18th May 2025

[11] ibid

[12] Techpoint Africa, 'Kenya orders Worldcoin to delete biometric data in landmark privacy ruling' (May 7, 2025), <https://techpoint.africa/news/worldcoin-delete-biometric-data-kenya/> accessed 19th May 2025

The capacity of those data subjects to whom USD50 was paid by Worldcoin and Tools for Humanity is contestable, as less than 4% of Kenyan's primary language is English. Worldcoin's Privacy Notice is not in Kiswahili, or any other indigenous language of Kenya's people, but in English[13].

Many African countries lack robust data protection laws or enforcement capacity, leaving communities exposed to corporate and state misuse without recourse. Many countries in the Global South lack the institutional capacity and regulatory frameworks needed to support digital innovation and protect users' rights particularly in a dynamic era of Artificial intelligence and other emerging technologies. In particular, the absence of strong data protection and privacy laws poses a serious risk to these vulnerable populations and groups.

Only about 48% of LDCs have implemented data protection legislation, compared to 74 per cent of countries in the Americas[14]. Without strong data protection laws, personal data can be collected, processed, and even sold without users' consent or knowledge. Secondly, weak or non-existent data protection makes countries more susceptible to cyberattacks, as unregulated digital environments provide easy targets for cybercriminals. This could lead to breaches of sensitive information, such as health or financial data, causing both economic and social harm.

Digital platforms and Social media algorithms unjustly suppress or flag content by African creators and activists, especially women and LGBTQ+ persons. A case in Ghana documented how AI-driven moderation mistakenly flagged posts advocating for reproductive rights as "harmful content," silencing critical voices.

6. Language and cultural barriers

Marginalized communities with low resource languages speaking indigenous or local languages may be excluded from platforms or services built only in dominant national or international languages. This often results in discriminatory exclusion and non-accessibility to public services such as welfare, education, and health care). The design and operation of such digital platforms creates a huge digital exclusion of marginalized groups from accessing certain services.

[13] Amit Gadhia, 'Worldcoin case a 'watershed moment' for data protection in Kenya' (September 15th 2023) <https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya/> accessed 19th May 2025

[14] Hany Besada, 'South-South cooperation can power the Global South's digital future' (LSE Blog November 8, 2024), <https://blogs.lse.ac.uk/africaatlse/2024/11/08/south-south-cooperation-can-power-the-global-souths-digital-future/> accessed 25th May 2025

B. CONTRIBUTING FACTORS

There are several factors that contribute to discrimination and unequal enjoyment of the right to privacy in the context of data collection and processing. These factors are technological, institutional or social and economic factors.

i. Data sets used to train AI systems are largely sourced from Global North populations, lacking African representation.
ii. Inadequate consideration of local languages, cultures, and dialects in algorithm design.
iii. Digital inequalities persist across gender, geography, and income.
iv. Social norms and patriarchal structures that deprioritize women's digital inclusion further exacerbate data marginalization.
v. Weak enforcement of data protection laws.
vi. Absence of human rights-centered digital governance mechanisms.
vii. Lack of ethical review processes in tech innovation by private and public institutions.

C. IMPACTS ON RIGHTSHOLDERS

- **Persons from Underrepresented Language Communities**: Unable to access digital platforms where their language is excluded in the design and functionality of such system.
- **Women and Girls**: Excluded from welfare programs due to digital barriers; subjected to online harassment without recourse.
- **LGBTQ+ persons**: Subjected to surveillance and data misuse by state and non-state actors.
- **Children and Youth**: Exposed to privacy-violating ed-tech platforms used in schools without informed consent.
- **Persons with Disabilities**: Underrepresented in digital identity systems, leading to service exclusion.

D. RECOMMENDATIONS AND BEST PRACTICES

a. Legislative and Regulatory Frameworks

- Enact and enforce comprehensive data protection laws aligned with international human rights standards.
- Mandate algorithmic transparency and impact assessments for both private and public actors.

b. Oversight and Remedy Mechanisms

- Establish independent digital rights commissions with investigatory powers.
- Strengthen local ombuds systems to receive and adjudicate digital rights complaints.

c. Business Self-Governance and Due Diligence

- Tech companies operating in Africa must publish transparency reports, including algorithmic bias audits.
- Conduct participatory ethics reviews with civil society and local communities before deploying tech solutions.

d. Data Governance Models

- Promote community-based data governance, emphasizing ownership and consent.
- Develop African-specific AI ethical frameworks, grounded in Ubuntu and Pan-African values.

Conclusion

In Africa, the absence of inclusive, rights-based data governance magnifies the inequalities already facing marginalized communities. Africa4Dev stresses the need for ethical data policies that are intersectional, localized, participatory, and pro-poor. Only then can digital technologies serve as tools of empowerment rather than systems of oppression. Africa4Dev reiterates its support for OHCHR's initiative and emphasizes the urgent need to protect those in the Global South (Africans) and those in the Global North from digital harm while ensuring the transformative potential of technology is equitably realized. We advocate for a globally inclusive and locally grounded framework that protects privacy, mitigates discrimination, and upholds human dignity in the digital age.

REFERENCES

Amit Gadhia, 'Worldcoin case a 'watershed moment' for data protection in Kenya' (September 15th 2023) <https://iapp.org/news/a/worldcoin-case-a-watershed-moment-for-data-protection-in-kenya/> accessed 19th May 2025

Aratek, 'The New Kenyan ID Card: Maisha Namba Explained' (November 25th 2024) <https://www.aratek.co/news/the-new-kenyan-id-card-maisha-namba-explained> accessed 13th May 2025

Fred Nasubo, 'Maisha Namba: Third-Gen ID Excludes the Historically Marginalised' (The Elephant December 5th, 2024), <https://www.theelephant.info/analysis/2024/12/05/maisha-namba-third-gen-id-excludes-the-historically-marginalised/> accessed 13th May 2025

Hany Besada, 'South-South cooperation can power the Global South's digital future' (LSE Blog November 8, 2024), <https://blogs.lse.ac.uk/africaatlse/2024/11/08/south-south-cooperation-can-power-the-global-souths-digital-future/> accessed 25th May 2025

Hyeonsoo Jeon and Umutai Dauletova, 'Cyberviolence disempowers women and girls and threatens their fundamental rights' (UNDP November 25th, 2021), <https://www.undp.org/eurasia/blog/cyberviolence-disempowers-women-and-girls-and-threatens-their-fundamental-rights> accessed 16th May 2025

Just Law Editorial, 'The Impact of Surveillance on Marginalized Groups and Society' (January 2, 2025), <https://thejustlaws.com/impact-of-surveillance-on-marginalized-groups/> accessed 18th May 2025

NIMC, 'About Us', <https://nimc.gov.ng/about-nimc > accessed 13th May 2025

Techpoint Africa, 'Kenya orders Worldcoin to delete biometric data in landmark privacy ruling' (May 7, 2025), <https://techpoint.africa/news/worldcoin-delete-biometric-data-kenya/> accessed 19th May 2025

United Nations Children's Fund, 'Child Protection in Digital Education: Policy Brief', UNICEF, New York, January 2023 <https://www.unicef.org/media/134131/file/Child%20Protection%20in%20Digital%20Education%20Technical%20Note.pdf> accessed 15th May 2025

Velis Lava, 'Many EdTech companies exploit children's data, says Human Rights Watch report' (May 26, 2022) <https://www.edds-education.org/post/many-edtech-companies-exploit-children-s-data-says-human-rights-watch-report> accessed 15th May 2025

Majiuzu Daniel Moses
Executive Director
Africa Tech for Development Initiative - Africa4dev
info@africa4dev.org; mmajiuzu@gmail.com
www.africa4dev.org