accountabilitylab NIGERIA

2025

BEYOND THE CONSUMER:

Shaping Africa's Voice in Tech Accountability and Human Rights

Policy Brief

Beyond the Consumer: Shaping Africa's Voice in Tech Accountability and Human Rights

By

Jake Okechukwu Effoduh
Assistant Professor, Lincoln Alexander School of Law.

Odeh Friday
Country Director, Accountability Lab Nigeria.

Ehi Idakwo
Programs and Learning Manager, Accountability Lab Nigeria.

Table of Contents

Table of Contents....4
Executive Summary....5
Introduction....6
Government-Tech Company Partnerships....8
Freedom, Digital Rights, and the Hidden Costs of Africa's Digital Ecosystem....11
Limitations of Human Rights Laws....14
Challenges in Tech Accountability....16
Pathways to Accountability....18
Recommendations....20
Conclusion....22
Works cited....23

Executive Summary

The growing integration of technology into daily life presents significant challenges for accountability, especially as governments and tech companies navigate the complex task of balancing freedom of speech with ethical practices. One of the primary challenges is how government-tech partnerships in Africa, often framed as tools for development or security, frequently operate with a lack of transparency and accountability. However, these partnerships frequently operate without adequate oversight, creating fertile ground for human rights abuses, particularly in contexts where regulatory frameworks are weak and civil society organizations (CSOs) have limited influence to demand greater transparency, equity, and justice. To address this, this policy brief examines the systemic obstacles to achieving tech accountability, focusing on

the impact of government-tech company collaborations and the ways that this can contribute to Africa's relegation to the role of a consumer market rather than an active participant in innovation.

It calls for a reimagined approach to tech accountability, one rooted in human rights, inclusive governance, and ethical principles. This can be achieved by emphasizing the need for co-creation processes involving government, CSOs, tech companies, and local communities to design and develop technologies that serve the region's needs and values, not just the market.

Introduction

Technology's dual role as an enabler and inhibitor of rights has become starkly evident.

Emerging technologies like artificial intelligence (AI), algorithmic governance systems, and content moderation frameworks have reignited critical debates about their impact on civil liberties. In Africa, where digital access is growing but remains uneven, approximately 73 percent of the population is still offline, and digital literacy levels vary greatly across regions. This gap worsens existing inequalities, leaving large segments of the population without the skills or resources to fully engage with and benefit from technological advancements.

Freedom of speech, a cornerstone of democratic governance, is increasingly threatened by opaque algorithmic decisions and the absence of meaningful oversight.

Government-tech company partnerships have become increasingly common, aiming to address various societal challenges and improve public services.

In Africa, all too often, ***CSO's role as a watchdog is stifled by restrictive laws, surveillance, and a lack of access to decision-making processes dominated by powerful government-tech alliances***

In 2020, during the #EndSARS protests, the Nigerian government deployed spyware technology to track and suppress dissenting voices, according to a report by the University of Toronto's cyber research unit, Citizen Lab, to actively spy on citizens, significantly undermining free expression and privacy. This marginalization of local participants from technological co-creation exacerbates systemic challenges, undermining both human rights and the continent's potential as an innovator. For example, in several East African countries, content moderation policies enforced by tech

companies have disproportionately targeted local media outlets, leading to widespread censorship and a narrowing of public discourse.

This not only ***reduces Africa to the role of a passive consumer of imported technologies*** but also limits the ability of CSOs to advocate for rights-based approaches to technological development.

Without local input, technologies often fail to address the region's specific needs, perpetuate inequities, and overlook critical human rights considerations,

such as data privacy, freedom of expression, and access to information.

01

Government-Tech Company Partnerships

There is a rise in government-technology company partnerships in Africa, which reflects an ongoing effort to accelerate digital transformation and improve public service delivery. These collaborations are often presented as solutions to enhance government efficiency, transparency, and innovation, but they are not without significant challenges and controversies, particularly regarding data privacy, human rights, accountability, and equity. CSOs are uniquely positioned to advocate for transparency and ethical practices, yet their voices are often drowned out by powerful alliances between governments and tech companies.

In Benin, the government partnered with Estonia to develop an e-government framework aimed at enhancing data interoperability and creating a centralized online portal for public services. The collaboration is claimed to have facilitated access to over 200 public services online, introduced innovative features like electronic driver's license exams, and implemented advanced data exchange solutions. Similarly, Rwanda's partnership with the private company *Irembo* is said to have led to the digitization of

more than 100 public services, processing millions of transactions through the *IremboGov* platform. While these initiatives promise to improve service delivery and reduce corruption, concerns about data privacy, security, and the transparency of long-term agreements persist. Rwanda's 25-year contract with *Irembo*, for instance, has raised questions about the accountability of such extensive public-private arrangements and the risks of government over-reliance on a single private entity.

Despite their potential, these partnerships often exacerbate systemic inequalities. To tackle these challenges, it is important for governments to implement strategies that guarantee equitable access to digital services, including the enhancement of internet infrastructure and digital literacy plans, particularly for marginalized communities. The rapid digitization of government services highlights the issue of the digital divide, as not all citizens have equal access to technology or the digital literacy required to benefit from these services. This exclusion disproportionately affects marginalized populations, raising concerns about equitable access to essential public services. Moreover, the centralization of sensitive data on digital platforms increases the risk of breaches and misuse, especially in contexts where strong data protection frameworks are lacking. To reduce these risks, independent oversight bodies should be instituted to oversee the execution of digital services and ensure compliance with international data protection standards.

In more controversial cases, government-tech alliances have facilitated digital repression and surveillance.

In Zimbabwe, partnerships with Chinese technology firms have provided the government with surveillance tools reportedly used to monitor opposition leaders and activists. This has led to the intimidation and arrest of dissenters, significantly undermining CSO's ability to hold the government accountable. Similarly, Ethiopia's collaboration with state-controlled telecom providers during the Tigray conflict enabled widespread internet shutdowns, silencing dissenting voices and obstructing humanitarian efforts. These actions highlight how such partnerships can be used to suppress freedom of expression and limit the ability of CSOs to advocate for human rights. In such contexts, it is important for international human rights organizations to intervene and advocate for the establishment of safeguards that prevent the misuse of technology for authoritarian purposes.

Uganda presents another concerning example, where partnerships with social media companies and telecom providers have supported initiatives like the controversial social media tax and digital surveillance measures. These actions have stifled online dissent, restricted access to information, and created a chilling effect on free expression.

Reports of targeted censorship further show the risks posed by opaque and unaccountable collaborations between governments and technology firms. To improve accountability, governments and tech companies must work together with CSOs to ensure that these partnerships are transparent, inclusive, and uphold fundamental human rights.

These examples illustrate the dual-edged nature of government-tech partnerships in Africa. While they hold significant potential to enhance governance and public service delivery, their lack of suitable oversight often enables abuses of power, suppresses civil liberties, and marginalizes CSOs. To strengthen the positive potential of these partnerships, independent monitoring bodies must be established, transparent contracting processes implemented, and CSOs should be involved in decision-making. The erosion of CSO's role is particularly damaging, as it weakens a critical counterbalance to unchecked government authority and diminishes advocacy for transparency, equity, and human rights.

02

Freedom, Digital Rights, and the Hidden Costs of Africa's Digital Ecosystem

Freedom of expression and digital rights are essential to building a tech ecosystem in Africa that promotes accountability, transparency, and social justice. These rights empower citizens to access and share information freely, participate in civic and political discourse, and hold governments and corporations accountable. In Africa, digital platforms are vital for democratization and civic engagement, making it essential to protect these rights so that technology becomes a tool for empowerment rather than repression. The #EndSARS movement in Nigeria exemplifies this potential, as social media platforms like X (then Twitter) were used to expose police brutality, mobilize protests, and amplify marginalized voices. The movement showcased the indispensable role of digital rights in fostering public accountability by drawing national and international attention.

Despite their importance, digital rights across Africa face numerous challenges, often undermining efforts to build accountable tech ecosystems.

Governments frequently resort to censorship and internet shutdowns to suppress dissent and limit political engagement. These restrictions negatively affect political autonomy and worsen pre-existing disparities in education, healthcare, and economic opportunities.

In areas with limited digital access, marginalized communities are negatively impacted, losing access to essential information, including online education and employment opportunities.

As noted earlier, in Ethiopia, internet blackouts during the Tigray conflict isolated millions from critical information and hindered reporting on human rights abuses. Similarly, Uganda's internet shutdown during the 2021 elections silenced political discourse and curtailed civic participation. These shutdowns, justified as security measures, suppress civic engagement and weaken democratic processes while simultaneously undermining public trust.

These threats extend to CSOs, journalists, and human rights defenders who rely on digital platforms to expose corruption, advocate for change, and document abuses. In Zimbabwe, activists have faced state-led surveillance and digital harassment, undermining their work and threatening their safety. Advanced surveillance technologies, often acquired from foreign companies, are increasingly used across Africa to monitor citizens under the guise of national security. Rwanda's reported surveillance of dissidents abroad highlights the transnational dangers of such practices, which stifle free speech and endanger critics.

The role of tech companies in content moderation significantly impacts digital rights, accountability, and the lives of the workers who sustain these systems. Algorithms designed to address harmful content often fail to consider Africa's cultural and political contexts. Disinformation and hate speech targeting African users frequently go unchecked, while culturally specific content is disproportionately censored due to algorithmic biases.

Moreover, the human cost of these moderation practices is often overlooked. Social media companies increasingly rely on human moderators in some of the world's poorest regions, including Africa, to screen and remove graphic and harmful content. These workers are frequently exposed to deeply disturbing material, including violence, abuse, and exploitation, to protect other users from such content. The psychological toll on moderators is severe, with many reporting post-traumatic stress disorder (PTSD),

depression, and burnout. The human cost extends to the refinement of large language models, which rely on human reviewers to label data and train AI systems.

In Africa, companies have outsourced such labour-intensive tasks to workers earning minimal wages, exposing them to harmful content and long hours without proper safeguards. For instance, it has since been reported how Kenyan workers earned less than $2 USD per hour to moderate content or refine AI systems like large language models, enduring immense emotional distress in the process. These practices highlight a critical gap in accountability; to wit, while tech companies profit from increasingly sophisticated moderation and AI systems, the burden of maintaining these systems disproportionately falls on vulnerable workers in African communities.

03

Limitations of Human Rights Laws

Human rights laws in Africa serve as a fundamental framework for accountability for various forms of social interactions, providing legal standards that address issues like freedom of expression, privacy, and non-discrimination. These laws, often embedded in national constitutions and regional instruments such as the African Charter on Human and Peoples' Rights, have the potential to hold both governments and private tech companies accountable if implemented and enforced adequately. For example, constitutional guarantees of privacy and free expression have been invoked to successfully challenge government overreach and data misuse, as seen in Kenya's High Court ruling in 2020, which determined that the *Huduma Namba digital ID* rollout violated privacy rights. In 2022, South Africa's Competition Commission ruled against Facebook, expressing the capacity of human rights legislation to tackle data misuse and anti-competitive behaviours. The 2019 ruling by Tanzania's High Court annulled restrictive online content regulations, illustrating the significance of judicial independence in protecting freedom of expression.

However, despite this potential, human rights laws in Africa face several critical limitations in effectively addressing tech-related challenges. A major issue is that many of these laws predate modern digital technologies, limiting their applicability to contemporary concerns such as algorithmic discrimination, AI bias, or mass surveillance. African governments must implement comprehensive data protection laws specifically designed for AI-related challenges, guarantee transparency in algorithmic decision-making, and perform regular reviews to revise legislation in accordance with

technological progress. For instance, while South Africa's constitutional privacy protections have been applied to tech cases, the absence of detailed regulatory mechanisms specific to emerging technologies, such as AI-driven surveillance tools, remains challenging from the standpoint of meaningful regulation. This highlights the necessity of creating specialized regulatory entities tasked with supervising AI applications, encompassing the formulation of ethical standards, data management protocols, and privacy protections.

Another significant limitation is the inconsistency in enforcement mechanisms. In many countries, legal protections exist on paper but are poorly enforced in practice. For example, Uganda's digital rights laws, meant to protect freedom of expression, have often been selectively applied, with the government resorting to internet shutdowns and imposing social media taxes to curb dissent and public participation. This gap between legal protections and their enforcement weakens public trust and renders accountability mechanisms ineffective. Governments need to ensure consistent and equitable application of digital rights legislation.

Government overreach and abuse of power further undermine human rights laws. States often invoke broad national security laws to justify surveillance, data access, and censorship, sidestepping constitutional protections. A prominent example is the earlier stated Ethiopia's use of surveillance technology during political unrest, which allowed the government to bypass privacy protections under the pretext of national security. Such practices illustrate how human rights frameworks can be subverted, limiting their ability to hold governments accountable. Reforms need to establish clear legal restrictions on national security claims in order to prevent the abuse of surveillance technologies, to assess the necessity and proportionality of these actions.

Judicial capacity also presents a challenge. Courts across the continent often lack the technological expertise, resources, and independence needed to adjudicate complex tech-related cases. This has led to delays, ineffective enforcement, and susceptibility to political influence. Efforts to challenge government actions, such as internet shutdowns or mass surveillance, have frequently stalled due to these constraints. In Nigeria, for example, the government's suspension of Twitter in 2021 highlighted this challenge. While human rights laws provided a basis for contesting the ban on the grounds of free expression, enforcement was slow, and broad executive powers ultimately delayed meaningful redress. Judiciary systems need to invest in training judges and legal practitioners on digital rights and emerging technologies, while augmenting resources and independence to handle technology-related cases.

04

Challenges in Tech Accountability

Tech accountability faces significant obstacles, particularly in safeguarding freedom of speech, ensuring CSOs engagement, and addressing systemic inequities in global innovation. The monopolization of digital spaces by tech giants like Meta, Google, and X (formerly Twitter) has created platforms that serve as both enablers of free expression and tools for its suppression. Algorithms designed to maximize user engagement often amplify divisive content, disinformation, and harmful speech, undermining the very democratic values these platforms claim to support. For instance, Facebook has been criticized for its role in amplifying hate speech during the Rohingya crisis in Myanmar, where algorithmic recommendations facilitated the spread of inflammatory content that fueled violence against the minority group. This case shows how opaque decision-making in content moderation can have catastrophic consequences, particularly in politically fragile contexts.

Government partnerships with tech companies can drive innovation but also enable state overreach and suppress dissent.

A prominent example is the Pegasus spyware scandal, in which governments used technology developed to monitor journalists, activists, and political opponents. These surveillance practices not only violate fundamental human rights but also erode public trust in both state institutions and tech companies. CSOs, which traditionally play a vital role in advocating for transparency and accountability, find themselves increasingly sidelined. Collaborative advocacy efforts and public awareness campaigns may

reinforce their impact by building partnerships with governments and tech companies to improve accountability. Emerging technologies should integrate diverse perspectives, especially from under-represented groups, with CSO efforts that advocate for inclusive design and ethical practices aligned with local values. Restricted access to policymaking processes, limited resources, and fear of reprisal have significantly curtailed their ability to hold power to account.

The design of emerging technologies, such as AI systems, often reflects inherent biases due to the under-representation of African data sets and perspectives. The facial recognition systems developed by leading tech companies have been shown to exhibit accuracy disparities across different racial groups, with notably higher error rates for darker-skinned individuals. This lack of inclusion in the design and testing phases not only reinforces systemic discrimination but also limits Africa's ability to shape AI's ethical parameters in a manner that reflects regional values and needs. The young people of Africa have the capacity to lead digital rights advocacy, harnessing their skills in technology to shape policy and push on accountability. Youth-led campaigns opposing digital censorship reflect their vital contribution to advancing inclusive digital governance.

Building power for young people through digital literacy programmes and policy discussions guarantee their influence in formulating inclusive, technologically viable policies.

Africa's experience within this global context illustrates another critical dimension of tech accountability. The continent's tendency to openly and uncritically adopt digital products has fostered a culture that significantly boosts the consumer base for tech companies, yet Africa remains a marginal player in global technology development.

Tech companies often treat Africa as a lucrative market rather than an innovation partner.

For example, initiatives like Facebook's *Free Basics*, which provided limited internet access to African users, were criticized for prioritizing corporate interests over genuine digital inclusion and, in some cases, even enabling dictatorship. Free Basics restricted access to a curated selection of websites, creating a digital divide that entrenched unequal access to information. Moreover, technologies developed without input from African participants frequently fail to address the continent's specific challenges.

05

Pathways to Accountability

When structured equitably, tech-government partnerships can be powerful tools for addressing social challenges and driving innovation. However, such partnerships must be designed to prioritize public interest, uphold human rights, and ensure accountability. Far from being inherently skewed, partnerships can thrive under conditions of transparency, inclusivity, and appropriate oversight.

One successful example is Rwanda's partnership with Zipline to deliver medical supplies using drones. This collaboration uses advanced technology to solve a pressing local challenge: access to essential medical supplies in remote areas. The success of this initiative may have rested on a clear alignment between public health goals and technological innovation and supported community engagement. Similarly, Estonia's e-governance model, built through a partnership between the government, private tech companies, and academic institutions, has contributed significantly to positioning the country as a leader in e-governance. This model highlights how collaborative partnerships can transform public services when guided by clear objectives and inclusive policies.

Certain foundational structures are necessary for such partnerships to succeed.

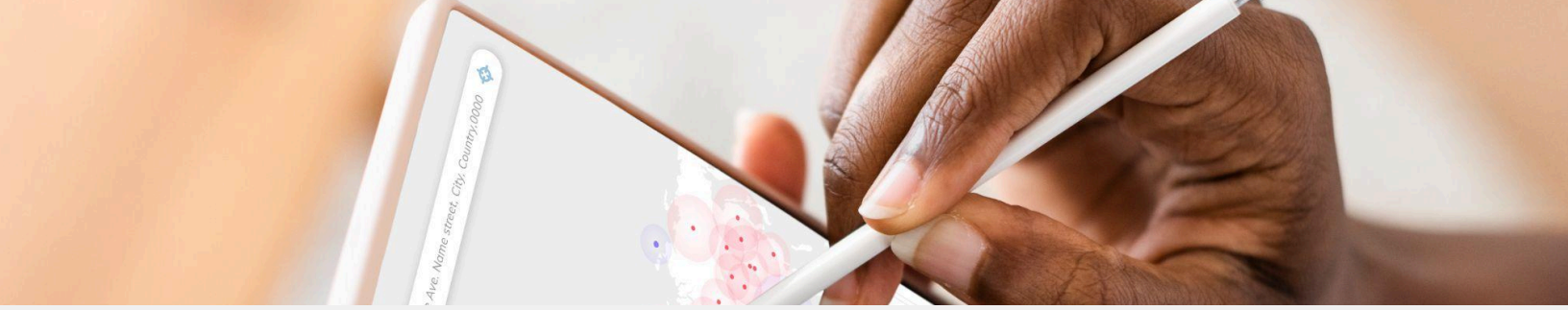
Transparency is paramount; agreements between governments and tech companies must be made public, including details about data-sharing practices and accountability mechanisms.

Clear legal frameworks should define the roles and responsibilities of each party, ensuring that partnerships prioritize public welfare over corporate or state interests. Independent oversight bodies involving representatives from CSOs, academia, and the private sector can provide critical checks and balances to prevent abuses of power or misalignment with public needs.

CSOs play a pivotal role in shaping and monitoring these partnerships. Their involvement ensures that diverse perspectives, particularly those of marginalized communities, are represented in decision-making processes. In India, for instance, CSOs advocacy has been crucial in highlighting the potential overreach of the government's 2021 IT rules, which mandate rapid content takedowns. While these rules were intended to curb harmful content, they have raised concerns about censorship and the stifling of dissent. CSOs have actively engaged in public discourse, pushing for more significant safeguards to protect freedom of expression and digital rights.

In Africa, however, many CSOs often face significant barriers to fulfilling this role. Restrictive regulations, such as Tanzania's requirements on international funding for NGOs, curtail their operations and reduce their influence. Furthermore, a lack of access to open government data and limited technological capacity undermines their ability to monitor and critique tech-government partnerships effectively.

Ultimately, the role of CSOs is not just to critique but to co-create solutions. CSOs can act as intermediaries, bridging the gap between governments, tech companies, and communities to ensure that partnerships are equitable and sustainable. Their involvement helps embed human rights and ethical considerations into the design and implementation of technologies, ensuring that innovation benefits society.



Recommendations

- Addressing the skewed dynamics in tech-government partnerships and the limitations of CSOs in Africa requires a focused effort to prioritize transparency, accountability, and inclusivity in the continent's digital ecosystem. Tech-government collaborations have often prioritized corporate and state interests over the public good, undermining digital rights and freedoms. To rebalance these relationships, governments must establish regulatory frameworks that ensure transparency in partnerships with tech companies. This includes public disclosure of agreements, independent oversight of data-sharing arrangements, and safeguards against the misuse of technologies for censorship or mass surveillance.

- CSOs are pivotal in holding governments and corporations accountable, yet they face significant challenges, including restrictive laws, limited funding, and inadequate technical capacity. Strengthening CSO's role in tech accountability involves providing legal protections for their operations, such as laws safeguarding whistleblowers and activists who expose digital rights violations. CSOs can deploy creative and innovative pathways for their advocacy, such as using data analytics and open-source intelligence tools to monitor and expose violations. Other strategies like digital storytelling and social media campaigns can also yield positive results. For example, the Lab has creatively advocated for environmental remediation through music. Also, instead of "naming and shaming" corrupt actors, the Lab "names and fames" people who lead by example instead, reinforcing trust in the public sector and normalizing integrity in public service. Targeted investments in capacity-building initiatives can also equip CSOs with the resources and technical expertise needed to monitor and advocate against issues like algorithmic bias, privacy breaches, and surveillance abuses.

Collaborative engagements that bring together governments, tech firms, and CSO representatives are also essential for ensuring that diverse voices shape the policies and practices governing Africa's digital future.

Dedicated media channels like the AccountabiliTea Podcast and AccountabiliTea Show can further raise awareness and empower citizens to demand accountability.

- Promoting locally driven innovation is critical for addressing the marginalization of African voices in the global tech landscape. Governments and regional organizations must incentivize local startups, researchers, and tech hubs to develop solutions tailored to Africa's unique challenges, such as improving access to healthcare, education, and financial services. This requires investments in local innovation ecosystems and the establishment of regional platforms for cross-border collaboration on shared challenges, such as climate resilience or digital literacy. Africans have demonstrated the capacity for building high-tech technologies that also reflect the socio-economic and cultural realities of the region while protecting the rights of citizens.

- Accountability mechanisms must also be embedded within Africa's tech ecosystem to ensure human and digital rights are upheld. Tech companies should be required to conduct human rights and digital rights impact assessments before deploying their technologies in African markets. The African Union (AU), through decades of policy development and collaboration, has articulated a clear and inclusive vision for the continent's AI future. This vision resulted in the African Continental AI Strategy, endorsed in 2024, which outlines a roadmap for ethical and sustainable AI deployment across the continent. Governments must also champion these ethical guidelines for emerging technologies, such as AI systems, that prioritize equity and non-discrimination. Moreso, public education campaigns can further empower citizens to understand and assert their digital rights, creating a more informed and engaged populace.

Conclusion

Africa has the potential to establish a digital ecosystem that embodies its unique context while upholding human rights, ethics, and accountability.

Success is rooted in transparent, inclusive partnerships that transform technology into a means of building power for people and equitable development.

As stakeholders work to address systemic obstacles to tech accountability, it is fundamental to draw attention to collaborative frameworks established on transparency and co-creation. By doing so, Africa may evolve from a marginal player to a global leader in shaping a digital future that safeguards freedoms, advances equity, and addresses the needs and aspirations of its people.

Stakeholders must also engage in ongoing discourse regarding tech accountability. This ongoing engagement improves collaboration, enables adaptive policymaking, and ensures tech policies are in alignment with the continent's constantly evolving needs. Through deliberate actions and visionary leadership, Africa can effectively leverage technology as a catalyst for inclusive growth and justice.

Works cited

Akuchie, M. (2023, June 7). A review of Irembo: Rwanda's 'impressive' e-government initiative. *Technext.* Retrieved from https://technext24.com/2023/06/07/rwanda-digital-governance-irembo/

Boxell, L., & Steinert-Threlkeld, Z. (2022). Taxing dissent: The impact of a social media tax in Uganda. *World Development, 153*, 105792. https://doi.org/10.1016/j.worlddev.2022.105792

Buyse, A. (2018). Squeezing civic space: Restrictions on civil society organizations and the linkages with human rights. *The International Journal of Human Rights, 22*(8), 966–988. https://doi.org/10.1080/13642987.2018.1492916

Chonka, P., Diepeveen, S., & Haile, Y. (2023). Algorithmic power and African indigenous languages: Search engine autocomplete and the global multilingual Internet. *Media, Culture & Society, 45*(2), 246–265. https://doi.org/10.1177/01634437221104705

Collaboration on International ICT Policy for East and Southern Africa (CIPESA). (2021, September 30). How state surveillance is stifling democratic participation in Africa: State of internet freedom in Africa study findings. *CIPESA.* Retrieved from https://cipesa.org/2021/09/how-state-surveillance-is-stifling-democratic-participation-in-africa-state-of-internet-freedom-in-africa-study-findings/

Effoduh, O. (Jake). (2024) Africa's AI Awakening. KU Leuven, Belgium (AI Summer School) https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/africas-ai-awakening

Effoduh, O. (Jake). (2024). *The role and potential of artificial intelligence in extremist-fueled election misinformation in Africa.* Toronto Metropolitan University. https://doi.org/10.32920/25378333.v1

Effoduh, O. (Jake). (2024). A Global South perspective on explainable AI. *Toronto Metropolitan University.* https://doi.org/10.32920/25746738.v1

Gravett, W. H. (2022). Digital neocolonialism: The Chinese surveillance state in Africa. *African Journal of International and Comparative Law, 30*(1), 39–58. https://doi.org/10.3366/ajicl.2022.0393

Hayes, B. (2012). Counter-terrorism, 'policy laundering' and the FATF: Legalising surveillance, regulating civil society. *Transnational Institute / Statewatch.*

Igbinosun, B. (2021, June 19). The suspension of Twitter operations in Nigeria: Beyond free speech. *Penn Carey Law.* Retrieved from https://www.law.upenn.edu/live/blogs/106-the-suspension-of-twitter-operations-in-nigeria

Ilori, T. (2020, June 19). Stemming digital colonialism through reform of cybercrime laws in Africa. *Yale Law School.* Retrieved from https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/stemming-digital-colonialism-through-reform-cybercrime-laws-africa

Jili, B. (2020, December 11). The spread of surveillance technology in Africa stirs security concerns. *Africa Center for Strategic Studies.* Retrieved from https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/

Lauer, D. (2021). Facebook's ethical failures are not accidental; they are part of the business model. *AI Ethics, 1*(4), 395–403. https://doi.org/10.1007/s43681-021-00068-x

Mhlungu, G. (2024, May 16). Africa's internet shutdowns: Where, why, and how do they happen? *Global Citizen.* Retrieved from https://www.globalcitizen.org/en/content/africa-internet-shutdowns-impact-human-rights/

Minko, A. E. (2023). The role of civil society in promoting good governance in Africa: Challenges and opportunities. *International Journal of Research and Innovation in Social Science, 7*(5), 952–958. Retrieved from https://rsisinternational.org/journals/ijriss/articles/the-role-of-civil-society-in-promoting-good-governance-in-africa-challenges-and-opportunities/

Mlambo, V. H., Zubane, S. P., & Mlambo, D. N. (2020). Promoting good governance in Africa: The role of the civil society as a watchdog. *Journal of Public Affairs, 20*(1), e1989. https://doi.org/10.1002/pa.1989

Nanjala, N. (2020, August 19). How African governments use social media to keep citizens in the dark. *Slate.* Retrieved from https://slate.com/technology/2020/08/social-media-content-moderation-african-nations.html

Organization of African Unity. (1981). *African Charter on Human and Peoples' Rights (Banjul Charter).* Adopted June 27, 1981. OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982). Retrieved from https://au.int/en/treaties/african-charter-human-and-peoples-rights

Renieris, E. M. (2021, November 10). Kenyan High Court ruling a watershed moment for digital rights. *Centre for International Governance Innovation.* Retrieved from https://www.cigionline.org/articles/kenyan-high-court-ruling-a-watershed-moment-for-digital-rights/

Soulé, F. (2023, October). Navigating Africa's digital partnerships in a context of global rivalry. *CIGI Policy Brief, 180.* Retrieved from https://www.cigionline.org/static/documents/PB_no.180.pdf

The Economist. (2022, December 5). China is helping Zimbabwe to build a surveillance state. *The Economist.* Retrieved from https://www.economist.com/middle-east-and-africa/2022/12/15/china-is-helping-zimbabwe-to-build-a-surveillance-state

Twizeyimana, J. D., Larsson, H., & Grönlund, Å. (2018). E-government in Rwanda: Implementation, challenges, and reflections. *The Electronic Journal of e-Government, 16*. Retrieved from https://academic-publishing.org/index.php/ejeg/article/download/648/611/644

Umutoni, N. (2024, October 1). Digitisation of government services in Rwanda: Lessons from the data. *Cenfri.* Retrieved from https://cenfri.org/articles/digitisation-of-government-services-in-rwanda-lessons-from-the-data/

Uwazuruike, A. (2021, December 13). #EndSARS: An evaluation of successes and failures one year later. *Georgetown Journal of International Affairs.* Retrieved from https://gjia.georgetown.edu/2021/12/13/endsars-a-evaluation-of-successes-and-failures-one-year-later/