Global Digital Compact Input Submission (E4E Fellows)

Table of Contents

Submission Letter From E4E
Group 1: Connect All People to the Internet, Including All Schools
Highlights in the African Context
Actionable Policy Recommendations
Individuals
Civil Societies
Private Sector
<u>Governments</u>
Group 2: Avoid Internet Fragmentation
Highlights in the African Context
Actionable Policy Recommendations
Individuals
Civil Societies
Private Sector
Governments
Group 3: Protect data
Highlights in the African Context
Actionable Policy Recommendations
Individuals
Civil Societies
Private Sector
Governments

Group 4: Apply Human Rights Online

Highlights in the African Context

Actionable Policy Recommendations

Individuals

Civil Societies

Private Sector

Governments

Group 5: Introduce Accountability Criteria for Discrimination and Misleading Content

Highlights in the African Context

Actionable Policy Recommendations

Individuals

Civil Societies

Private Sector

Governments

Group 6: Promote Regulation of Artificial Intelligence

Highlights in the African Context

Actionable Policy Recommendations

Individuals

Civil Societies

Private Sector

<u>Governments</u>

Group 7: Digital Commons as a Global Public Good

Highlights in the African Context

Actionable Policy Recommendations

Individuals

Civil Societies

Private Sector

Governments

List of Contributing Fellows

About E4E

Submission Letter From E4E

29 March 2023

Dear GDC,

We are writing to submit our contribution to the Global Digital Compact. E4E is a think tank that contributes to tech policy advocacy in emerging markets using emerging technologies.

For our consultation process for this submission, we held a one-month Fellowship with 34 fellows from different parts of Africa and Europe, themed "Africa's Digital Future". Based on the seven areas listed in the Secretary General's Common Agenda, we divided the Fellows into seven groups, each addressing one of the seven areas. We had four deliberation sessions from February 4th, 2023, to March 4th, 2023. The virtual sessions were 2 hours weekly. Group members met separately from these general sessions to discuss and compile their contributions.

Our conclusions from the sessions are consolidated into this submission to the GDC. We have also submitted a concise version via the survey form on the website. This expanded version will be submitted via email to <u>digitalcompact@un.org</u> as a PDF.

We look forward to hearing from you and are available to provide any additional information or support you may need.

Sincerely,

Faith Obafemi **Executive Director. E4E**

Group 1: Connect All People to the Internet, Including All Schools

Members: Asseh Hannah, Rotimi Owolabi

Highlights in the African Context

Current state of internet accessibility in Africa, including Schools

There is an urgent need to connect everyone, including schools, to the internet, given the significant role that it plays in modern society. In addition to making it possible for people to receive essential services and participate in the global economy, this would also ensure that African students have the same access to educational opportunities as students in other areas of the world.

For schools, in particular, the absence of internet connectivity in Africa is concerning because it has become an essential component of modern education. The COVID-19 epidemic highlighted the value of technological innovation in education and the need for fair access to online learning resources. Yet, many African schools still need internet access, which limits their ability to deliver high-quality instruction and prepare pupils for the digital economy.

The internet availability in African schools varies widely across the continent due to the unequal distribution of internet infrastructure and technology access. Some countries such as South Africa, Kenya, and Nigeria have seen significant improvements in recent years, with many schools having high-speed internet connections and computer labs. However, internet access still needs to be improved in many rural and remote schools in these countries. In other African countries, particularly in sub-Saharan Africa, internet access in schools still needs to be enhanced or might be nonexistent, about 60 per cent of school children in urban areas do not have internet access at home globally, with School children in sub-Saharan Africa and South Asia being the most affected,

according to a 2020 UNICEF-ITU report.¹ Additionally, even in schools with internet access, there may be other obstacles to using it effectively for education, such as insufficient resources or infrastructure. Although progress has been made in improving internet accessibility in African schools, more needs to be done to ensure that all students have access to digital resources and tools required for success in the 21st century. Despite significant advancements, many parts of the world, especially Africa, still need equal internet connectivity.

Progress toward internet access for all in Africa

There are multiple examples of initiatives across the continent being implemented to increase access to the internet, including the following:

- Submarine cable by Google in Togo to introduce fifth-generation mobile services in West Africa.²
- 2. Starlink is being approved and licensed in many countries on the continent.
- 3. Adopting the Digital Transformation Strategy for Africa (2020-2030).
- 4. National internet or broadband strategies.
- 5. The Smart Africa Alliance aims to increase internet penetration rates across Africa.
- 6. Express Wi-Fi initiative by Facebook partners with internet service providers across Africa to offer reliable internet access in underserved areas.³
- 7. The Kenyan government's Digital Literacy Programme provides primary school students nationwide with tablets, internet connectivity, and digital skills training.⁴

www.africanews.com/2022/03/18/google-s-underwater-internet-cable-to-connect-togo-to-europe

¹Two Thirds of the World's School-age Children Have No Internet Access at Home, New UNICEF-ITU Report Says.https://www.unicef.org/press-releases/two-thirds-worlds-school-age-children-have-no-internet-access-home-ne w-unicef-itu

² AfricaNews. "Google & Rsquo;S Underwater Internet Cable to Connect Togo to Europe | Africanews." *Africanews*, 18 Mar. 2022,

³ Eutelsat Partners Facebook to Deliver Affordable Internet in Rural Nigeria | TheCable, 21 May 2021, www.thecable.ng/eutelsat-partners-facebook-to-deliver-affordable-internet-in-rural-nigeria.

⁴ "Bringing the Digital Revolution to All Primary Schools in Kenya - ITU Hub." *ITU Hub*, 29 May 2020, www.itu.int/hub/2020/05/bringing-the-digital-revolution-to-all-primary-schools-in-kenya.

 The eLearning Africa conference connects policymakers, educators, and technology experts from across the continent to discuss innovative approaches to using technology in education, including increasing internet connectivity in schools.

What are the main risks and challenges?

- Unequal access due to rural-urban divide: This discrepancy limits access to the internet for people living in rural areas. They often have to travel long distances to access internet cafes or depend on unreliable and expensive mobile internet services.
- 2. Access and affordability of mobile devices: The prices of devices capable of connecting to the internet remain high across Africa.
- 3. Level of digital literacy: this mainly affects marginalised and disadvantaged groups, such as women, people living in poverty, and people with disabilities. Even if they have access to the internet, the lack of digital skills and knowledge limits their ability to navigate the internet and use online resources effectively.
- 4. Power crisis in many African countries: This is a major problem as internet service providers and digital devices require a stable and reliable power supply to function effectively. Yet, many African countries still experience frequent power outages and unreliable electricity supply.
- 5. **Cost of energy:** This creates a digital divide between those who can afford to pay for internet connectivity and those who cannot.
- 6. **Gender inequalities in access:** Females may have limited access to the internet due to cultural norms or limited educational opportunities. Women and girls fight against exclusion from opportunities in the digital economy and society.
- 7. *Funding challenges:* this can limit the ability of countries to invest in digital skills training programs or the necessary infrastructure and technologies to expand access to the internet.

8. **Online protection of school children:** Schoolchildren with access to the internet face many risks online. However, many African countries lack adequate policies or the resources to enforce those policies to protect them.

Actionable Policy Recommendations

Individuals

- → Individuals can collaborate with civil societies to create awareness among the people and advocate for better internet connectivity regulations.
- → Individuals can contribute to expanding internet access in their communities by patronising community-owned and -operated networks that offer internet connection to underserved areas.
- \rightarrow Invest in personal digital devices such as smartphones, tablets, or laptops.
- → Engage in digital literacy programs such as online courses, workshops, or community-based training programs to learn how to use the internet safely and effectively.
- → Individuals are responsible for using the internet safely and avoiding cyber crimes. It is their responsibility to report perpetrators of such crimes to the proper authorities to prevent the exploitation of others.

Civil Societies

→ Promoting awareness of the significance of internet connectivity and its effects on social inclusion, economic development, and education. This can entail planning campaigns, gatherings, and other events to inform the public and policy-makers about the advantages of internet connectivity.

- → To learn more about the difficulties and possibilities of internet access in Africa, they can also study and gather data. This may include conducting surveys, gathering information on internet usage, and examining policy frameworks to find areas that could want improvement.
- → Civil society organisations can push for stronger internet connectivity regulations, such as those that incentivise investment in broadband infrastructure.

Private Sector

- → They can invest in internet infrastructure and expand internet access, build new network infrastructure such as fibre optic cables, and upgrade existing infrastructure to support faster internet speeds.
- → Private organisations can partner with governments and other organisations to provide internet access in underserved areas. In addition, private sector companies can provide internet services such as broadband internet, mobile data, and Wi-Fi access to improve internet connectivity in Africa.
- → They can support research and development in the telecommunications sector to drive innovation and improve internet technologies. They can invest in new technologies such as 5G, offering faster internet speeds and greater connectivity.
- → Public-private collaborations can be an effective way to fund and develop internet infrastructure projects. Through infrastructure investments, internet services, and technological innovation, private sector companies can help bridge the digital divide and provide more people with access to the benefits of the internet.

- → Schools can provide students, teachers, and parents with digital literacy training. Such training would equip them with the necessary skills to navigate the internet safely and effectively, including using digital resources for learning and creating and sharing digital content. This training should be included in school curriculums to ensure all schools practise it.
- → Schools can promote responsible internet use by setting policies and guidelines for internet users to create a safer and more productive online environment for students.

Governments

- → To ensure widespread access to the internet, especially for school children, African governments can prioritise developing and implementing national broadband plans.
- → They can also work with private sector partners to lower the cost of internet-enabled devices.
- → Promote public-private partnerships to fund and develop internet infrastructure projects.
- → Encouraging the establishment of community networks, investing and promoting open access policies.
- → Harmonising laws and regulations related to telecommunications and the internet at the sub-regional level can also improve internet connectivity.
- → Governments can increase funding for internet infrastructure projects in underserved areas through grants, loans, and other financial incentives. African governments can eliminate or reduce taxes and tariffs on ICT equipment such as

smartphones, laptops, and tablets. This will make these devices more affordable for schools and families.

- → Provide digital literacy training to students, teachers, and parents. This training should cover how to use digital resources for learning, navigate the internet safely, and create and share digital content.
- → African governments can establish and enforce laws and policies safeguarding children's online privacy and security. This includes measures to prevent cyberbullying, online harassment, and exploitation.
- → The government can establish public internet access centres, such as community centres, libraries, and internet cafes, where people can access the internet for free or at a reduced cost. There should also be personnel available to assist the aged or unskilled.

Group 2: Avoid Internet Fragmentation

Group Leader: Carolyne Tarus

Members: Carolyne Tarus, Eric Muhia, Majiuzu Daniel Moses, Alice Ndung'u, Adekunle Falola

Highlights in the African Context

The Internet's evolution into a worldwide societal phenomenon lends much credit to the content and services that have taken advantage of the network's unique architecture. Entire economies depend on cross-border content flows, and the Internet is now a critical part of democratic processes and policy discussions. According to estimates,⁵ In 2020, Global Internet traffic was estimated to be equivalent to 95 times the volume of the entire global Internet in 2005. The number of devices connected to Internet Protocol (IP) networks is expected to be more than three times as high as the worldwide population in 2023.⁶

Internet fragmentation is implementing any technical, governmental, or commercial activity that would interfere with the perception of an equal access, open and unified network. At the conception of the Internet, it assumed universal connectivity was a primary benefit. One could not know when such connectivity might prove helpful, and to exclude any seemed self-defeating.

Each user on the internet would have equal access and unlimited freedom to express ideas and information. However, any action interfering with or impeding this accessible data flow between Internet users is qualified as fragmentation.

⁵ Cisco Visual Networking Index available

http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-w hite-paper-c11-481360.html Accessed 24th February 2023

Types of Internet Fragmentation

There are three main types of internet fragmentation: technical, governmental, and commercial.

1. GOVERNMENTAL FRAGMENTATION

Governmental fragmentation is the barrier between nations or national segmentation that could create obstacles in how the Internet functions.⁷ They are sovereign governmental policies and actions that interfere with or limit the creation, access, or distribution of certain information by dividing it into digitally bordered national interests.⁸ The main elements of governmental fragmentation include; content and censorship; e-commerce and trade; national security; privacy and data protection; data localisation; and fragmentation as an overarching national strategy.

Most Governments mainly implement internet fragmentation for political censorship, protection of local industries and markets, and protection of national interests. The main advantage of internet fragmentation is that governments can promote local industry and talent and preserve national cultural and religious values. However, it may restrict access to information provided under Article 19 of the Universal Declaration of Human Rights and inhibits global innovation and cooperation.

The free online information flow is now threatened by growing fragmentation across national borders. It is worth noting that several strides have been taken to champion the avoidance of internet fragmentation. The Internet Governance Forum established a Policy Network on Internet Fragmentation (PN-IF)⁹ to develop a framework that captures a range of fragmentation concerns and to show recommendations and codes of conduct that prevent fragmentation.

⁹ Internet Governance Forum IGF, *IGF 2022 Policy Network on Internet Fragmentation* <u>https://www.intgovforum.org/en/filedepot_download/256/24127</u>

⁷ ibid

⁸ William J. Drake, Vinton G. Cerf, Wolfgang KleinWatcher, 'Internet Fragmentation: An overview, World Economic Forum' (January 2016).

African countries have also taken part in promoting the avoidance of internet fragmentation. In 2019, Zimbabwe's high court ordered the country's government to restore the internet in full, ruling that the security minister did not have the power to order restrictions.¹⁰

i. Content Censorship/ Internet Censorship

Most African countries experienced censorship from their respective governments in the post-independence period. More robust national approaches to limiting access to the global Internet have emerged as comprehensive constraints and network shutdowns targeting specific events across Africa.¹¹ Governments are using their coercive power to block websites and social media platforms and control the provision of Internet services through governmental control or monopolising existing telecommunications services.

Mandated by states and implemented by private intermediaries, content controls reveal new ways of cyberspace policing through automation and machine-learning tools. This bid to control the internet impedes equal access and free flow of information and threatens the established principles of freedom of expression.

A recent case of censorship occurred in Nigeria in 2021, where the government "suspended, indefinitely, the operations of the micro-blogging and social networking service, Twitter". The suspension was after the platform deleted a tweet by President Muhammadu Buhari based on allegedly violating Twitter rules. The government, after that, announced the suspension citing the continued use of the platform for activities capable of undermining Nigeria's corporate existence.¹²

¹⁰ The Guardian, *Zimbabwe high court orders government to restore full internet* <u>https://www.theguardian.com/world/2019/jan/21/zimbabwe-high-court-orders-government-to-restore-full-in</u> <u>ternet</u>

¹¹ Geneva Graduate Institute, *Global Internet Governance: Is Fragmentation Avoidable?* <u>https://globalchallenges.ch/issue/7/global-internet-governance-is-fragmentation-avoidable/</u>

¹² Internet Society, *Internet Fragmentation: The Impact of Technical Blocking on the Economy of Africa* <u>https://www.internetsociety.org/events/internet-fragmentation/</u>

Another case of censorship happened in the same year in Uganda, where Facebook and Twitter announced that they had taken down a network in Uganda linked to the country's Ministry for Information for posting using fake and duplicate accounts. The platforms contended that the fake accounts participated in "coordinated inauthentic behaviour" to target public discourse before the election. The Uganda Communications Commission swiftly followed up by shutting down the internet, including all messaging apps and social media platforms.¹³

Internet censorship impedes the right to freedom of expression and access to information, both fundamental for democracy and the enjoyment of all other rights.

ii. Data localisation

Data localisation is collecting, processing, and storing data within a region where it originated before it is transferred internationally. Such data is usually transferred only after meeting local privacy or data protection laws, such as giving the user notice of how the information will be used and obtaining their consent.¹⁴

There are divergent views on data localisation. Many cite the need to protect national security, promote the local digital economy and ensure adequate data security and users' privacy.¹⁵ Critics argue that data localisation can undermine data privacy, including by facilitating government agencies access to citizens' data, including for conducting state surveillance. It is contended that "data localisation policies are causing more harm than good" as "they are ineffective at improving security, do little to

 ¹³ Quartz, Uganda's election is a key moment for the splinternet in Africa
<u>https://qz.com/africa/1970547/ugandas-election-is-a-key-moment-for-africas-internet-fragmentation</u>
¹⁴ Jurist, Data Localization Laws: An Emerging Global Trend

https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/

¹⁵ How Surveillance, Collection of Biometric Data and Limitation of Encryption are Undermining Privacy Rights in Africa, https://tinyurl.com/4ptmxy43

simplify the regulatory landscape, and are causing economic harms to the markets where they are imposed."¹⁶

In light of the divergent views on data localisation, African countries have adopted differing approaches to cross-border data restrictions. Many have enacted laws requiring data to be stored locally and forbidding cross-border transfers of personal data unless authorised by the data protection authorities.

However, data localisation laws may expose citizens to government surveillance, breaches of privacy, and cybercrime. On the one hand, access to this data allows law enforcement to investigate and prosecute crime without hindrance, and intelligence services can detect any activity contrary to national security interests. On the other hand, this access may readily be misused by government agencies through surveillance without citizens' knowledge or consent.

In July 2018, Ugandan security agents from the Internal Security Organization (ISO) stormed the Data Centre of leading telecom service provider MTN Uganda without a search warrant, a court order, or a request for information served to the telco, and reportedly accessed sensitive and confidential data, including call data records.¹⁷ There were unconfirmed reports that the security agents were investigating MTN Uganda for assisting Rwandan intelligence to spy on Ugandans when the two countries were trading accusations of supporting each other's enemies. In a complaint to the regulator, MTN Uganda stated that the incident posed a severe security risk to its telecommunications infrastructure and customer data, adding that "some data may have been tampered with or illegally accessed and taken from the premises."¹⁸ Uganda's laws permit police officers to access users' data mainly if a court order backs their

¹⁶ Emily Wu, *Sovereignty and Data Localization*, <u>https://www.belfercenter.org/publication/sovereignty-and-data-localization</u>

¹⁷ Nobody is above the law! ISO boss justifies raid on MTN data centre,

https://www.pmldaily.com/news/2018/07/nobody-is-above-the-law-iso-boss-justifies-raid-on-mtn-data-cent re.html

¹⁸ MTN Uganda says government security personnel raided its data centre,

https://www.reuters.com/article/us-uganda-mtn-group-idUSKBN1JW1Q5

requests. However, with or without court backing, it is easier for security agencies to access locally stored data than data stored abroad.

If such a trend toward data localisation continues, it will lead to a more constricted and less resilient network with suboptimal performance, modified to comply with national borders. Businesses will have to narrow their choices and capabilities, and network operators may be forced to use costly and less resilient ways to route traffic. Cybersecurity may suffer as organisations cannot store data outside borders to increase reliability and mitigate various risks, including cyber-attacks and national disasters.

Countries trying to localise data forcibly will impede the openness and accessibility of the global Internet. Data will not be able to flow uninterrupted based on network efficiency; instead, special arrangements will need to be put in place for that data to stay within the confines of a jurisdiction. The result will be increased barriers to entry, to the detriment of users, businesses, and governments seeking to access the Internet. Ultimately, forced data localisation makes the Internet less resilient, less global, and costlier.

iii. Data Localisation and Trade

Data flow is essential for expanding international trade and cooperation. Cross-border data flows and internet openness has led to increased economic efficiency and productivity, thereby improving international trade. For example, trans-border data flow has facilitated real-time customer interaction through business communication. It has caused disaggregation in the supply chain of businesses in many nations.¹⁹

¹⁹ Economic Impact of Data Localization in 5 selected African Countries, an empirical study<u>https://pic.strathmore.edu/wp-content/uploads/2019/03/PIC_RANITP_Economic_Impact_of_Data_L</u>ocalization_in_5_selected_African_Countries.pdf

However, data localisation results in marginal gains for a few local enterprises and workers while causing significant economy-wide harm. Currently, the majority of Africa's data centres are privately owned.²⁰ The domestic benefits of data localisation would accrue to the few owners and employees of data centres and the few companies that service these centres locally. On the other hand, small, medium, and large businesses will suffer the negative consequences of limited or lack of access to data.²¹

Data stored locally due to data localisation requirements would only result in economic growth with the necessary open data and data access policies. In addition, local data processors would also be similarly constrained by the domestic data transfer requirements to comply with, for example, data protection requirements.²²

Overall, restricting data flows would significantly undermine Africa's efforts to exploit the opportunities presented by e-commerce, which also relies on maintaining real-time data connectivity across the economy. With improved logistical infrastructure, African countries could experience a boom in cross-border trade enabled by the internet. However, these restrictions could pose a threat to those aspirations.

2. TECHNICAL FRAGMENTATION

Technical fragmentation impedes the internet's infrastructure from efficiently inter-operating and exchanging information as designed. There are various ways in which the original concept of a fully connected Internet has been eroded throughout the Internet's over 30 years of operation. And this includes technical fragmentation of the underlying physical and logical infrastructure, a complex evolutionary process that has

²⁰ Mandela Institute, The Impact of Data Localization Laws on Trade In Africa

https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/resea rch-entities/mandela-institute/documents/research-publications/PB%2008%20Data%20localisation%20la ws%20and%20trade.pdf

²¹Chander and Lê, 'Data Nationalism', p. 722–723.

²² Supra note 16

unfolded slowly but is gathering pockets of steam in the contemporary era.²³ Some of it has been intentional and motivated by operational and other concerns. Some of it has been the unintended by-product of actions with different objectives. Moreover, how such fragmentation occurs also varies in technical terms. To capture these realities, we survey key trends regarding interconnection, naming and security on the Internet in this section.

The Internet's original design used 32-bit numerical identifiers, analogous to telephone numbers, to designate endpoints on the Internet. Unlike the telephone numbering plan, however, IP addresses were not nationally-based.²⁴ Their structure was related to how the networks of the Internet were connected. Each network was made up of a collection of IP addresses associated with an autonomous system number. An endpoint on a given autonomous system or network could be anywhere globally, but a particular autonomous system's endpoints are interconnected through that network.²⁵

A guiding vision of the Internet's conception was that every device on the Internet should be able to exchange packets with any other device²⁶. Universal connectivity was assumed to be a primary benefit. But there are various ways in which the original concept has been eroded through a complex evolutionary process that has unfolded slowly but is gathering pockets of steam in the contemporary era.²⁷ Four issue areas are reviewed: Internet addressing, interconnection, naming and security. Below are 12 kinds of fragmentation of varying degrees.

- 1. Network Address Translation
- 2. IPv4 and IPv6 incompatibility and the dual-stack requirement

 ²³ William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter Internet Fragmentation: An Overview https://www.wef_Fii_Internet_Fragmentation_An_Overview_2016.pdf Accessed 24th February 2023
²⁴ ibid

²⁵ ibid

²⁶ World Economic Forum Internet Fragmentation: An Overview being the Future of the Internet Initiative White Paper https://www.Internet%20fragmenta/Wef_Fii_Internet_Fragmentation_An_Overview_2016.pdf Accessed 27th February 2023

- 3. Routing corruption
- 4. Firewall protections
- 5. Virtual private network isolation and blocking
- 6. TOR "onion space" and the "dark web"
- 7. Internationalized Domain Name technical errors
- 8. Blocking of new gTLDs
- 9. Private name servers and the split-horizon DNS
- 10. Segmented Wi-Fi services in hotels, restaurants, etc.
- 11. Possibility of significant alternate DNS roots
- 12. Certificate authorities producing false certificates²⁸

3. COMMERCIAL FRAGMENTATION

Commercial fragmentation separates internet content and services into separate markets. Commercial fragmentation refers to dividing or separating the internet into different commercial markets or economic zones when commercial entities, such as e-commerce companies, digital service providers, or advertisers, tailor their services and content to specific geographic or cultural markets. As the internet has become more globalised in recent years, the issue of commercial fragmentation has become more prominent.

A good example of internet fragmentation in Africa is the online entertainment business. Most African countries need access to western entertainment websites such as HBO, Hulu, Paramount Plus, and Disney Plus. Kenyan citizens could only access Netflix in 2016 despite launching in 2007 and Spotify in 2018 despite being established in 2006. The lack of access to these online entertainment platforms for Africans has contributed to the lack of global promotion of local entertainment worldwide. Since the launch of Netflix Africa and Spotify Africa, we have seen a rise in the worldwide appreciation of African talent. We have seen movies and series such as the South African series 'Queen Sono' and Nigerian Series 'Blood Sisters', which have gained global recognition.

Commercial fragmentation can be seen in how countries and regions use the internet. For example, some areas of the world have more developed e-commerce markets than others; there is a higher level of digital literacy in some nations than others. In addition, there are differences in how people from different regions consume content on social media networks.

Factors Contributing to Internet Fragmentation in Africa

- National internet backbones: Many African countries have built their own national internet backbones, which act as the country's main channels for internet traffic. These backbones are often disconnected from each other, creating islands of internet connectivity isolated from the rest of the world.
- Mobile Network Operator (MNO) Walled Gardens: Some MNOs in Africa offer limited internet services, often through their proprietary platforms, creating a "walled garden" of services only accessible to subscribers of that particular network, further fragmenting the internet.
- Content blocking and censorship: Some African governments have been known to block access to certain websites or platforms for political reasons or to protect local industries.
- 4. Lack of infrastructure: In many parts of Africa, more infrastructure is needed to support high-speed internet connectivity.

Actionable Policy Recommendations

Recommendations for Avoiding Internet Fragmentation: Roles and Responsibilities of Individuals, Civil Societies, Private Sector, and Governments.

Individuals

Individuals play a crucial role in promoting the responsible use of digital technologies and ensuring the internet remains an open and inclusive platform. They can contribute by being mindful of their online behaviour, such as not spreading false information, supporting privacy rights, and respecting others online. Individuals should take proactive steps to protect their online freedom and privacy. These steps can include educating themselves on internet laws and regulations in their country and advocating for internet freedom in their community. Supporting organisations that protect online freedom of expression, privacy, and access to information is also essential. Individuals should consider using virtual private networks (VPNs) to ensure secure and private internet access. Additionally, open-source software such as the Linux operating system and the Mozilla Firefox web browser can help avoid proprietary software subject to restrictions or regulations. Supporting net neutrality, the principle that all internet traffic should be treated equally without discrimination or interference by ISPs or governments, is another way individuals can promote online freedom and protect their rights.

Civil Societies

Civil society organisations can raise awareness about the importance of avoiding internet fragmentation and promote the adoption of shared principles for a more inclusive and equitable internet. They can also advocate for the protection of internet freedom and human rights, as well as contribute to the development of alternative technologies that are more accessible and affordable.

Civil societies play a vital role in protecting digital rights and promoting an open and accessible internet. Civil society organisations can contribute to this cause by

advocating for net neutrality laws and regulations that ensure equal access to the internet. Additionally, they can support digital literacy programs that help people understand how to use the internet effectively and safely. Advocating for digital rights such as privacy, freedom of expression, and access to information is another crucial step civil societies can take to protect individuals' online rights. To foster cross-border collaborations, civil society organisations can work with other countries in Africa to promote a unified approach to internet governance and address issues of internet fragmentation, ultimately enabling a more connected and accessible world.

Private Sector

The private sector significantly impacts the direction and development of digital technologies and the internet. Companies can contribute to avoiding internet fragmentation by being transparent about their data collection and usage practices, supporting the development of open standards, and investing in technologies that promote inclusion and access. Private sector companies are essential in promoting an open and accessible internet. Investing in building and expanding internet infrastructure, such as Elon Musk's Space X plans to launch Starlink satellites, can help deliver high-speed internet to more people, bypassing the limitations of traditional infrastructure. Supporting the development and use of open standards like blockchain for internet technologies and protocols can ensure that the internet remains interoperable and accessible across different regions and countries. Engaging with policymakers at all levels to promote policies that support an open and accessible internet, including net neutrality and data protection, is also crucial. By being transparent about their data collection and usage practices, companies can contribute to avoiding internet fragmentation and promoting a more connected world.

Alongside several possibilities to prevent internet fragmentation, blockchain technology offers a viable solution with its decentralised network model, interoperability and security. Blockchain technology has the potential to support decentralisation and promote an open, accessible, and interoperable internet. Some ways blockchain

technology can help internet defragmentation is through solutions that decentralise domain name systems (DNS), content delivery networks (CDNs), identification using zero-knowledge proofs (ZKPs), interoperability protocols and open data standards.

Governments

Governments play a critical role in shaping the future of the internet and avoiding internet fragmentation. They can do so by supporting the development of regulations that promote a free and open internet, protecting citizens' rights online, and investing in digital infrastructure and access for all. African governments can benefit from developing regional standards promoting interoperability between networks and platforms. This will make it easier for businesses to operate across different countries and reduce business costs.

Governments have a crucial role in promoting and protecting digital rights and internet freedom. They should defend freedom of expression and resist the temptation to censor online content or restrict access to the internet. Governments can help promote a more informed and engaged citizenry and foster democratic values. Additionally, governments should develop digital rights policies and net neutrality regulations that incorporate the need to unite the global internet where content, services, and applications are not unjustifiably blocked or restricted. Any necessary restrictions should be justified and proportionate on public interest grounds.

Fostering cross-border collaborations with other governments and organisations is another crucial step that African governments can take to promote a unified approach to internet governance and address issues of internet fragmentation. By working together, they can develop policies and regulations that promote a more connected and accessible internet for all. Governments should also promote fair competition and create a level playing field for all market players, whether foreign or local, to avoid commercial fragmentation. Governments can achieve this through implementing regulations and policies encouraging transparency and ensuring that all companies operate on a level playing field. By doing so, governments can promote a more vibrant and competitive marketplace, driving innovation and collaboration, lowering costs, developing standardisation and increasing investment.

Government should move faster towards policy harmonisation across African countries using the Malabo Convention and African Union Data Policy Framework, among other regional instruments, as a blueprint to improve data flows across countries while ensuring data privacy. Governments should move faster towards policy harmonisation and work together to develop policies and regulations that promote a more connected and accessible internet for all, including developing consistent data protection, privacy, and security standards across all African countries. By doing so, governments can create a more favourable environment for businesses to operate and promote regional innovation and investment.

Additionally, promoting policy harmonisation can help address the issue of internet fragmentation by creating a more consistent regulatory environment that encourages cross-border data flows and avoids unnecessary restrictions on the free flow of information. By working together, African governments can promote a more united and integrated digital ecosystem that benefits all citizens and supports economic growth and development in the region.

Governments should develop digital rights policies that will incorporate the need to have unity of the global internet where content, services and application are not unjustifiably blocked or restricted. States should also ensure that where there is a need for a limitation on the unity of the internet, the limit ought to be justified and proportionate on the grounds of public interests.^{29 30}

²⁹ European Parliamentary Research Service, 'Splinternets' Addressing the renewed debate on internet fragmentation, July 2022.

³⁰ Internet Fragmentation and Content Blocking available at

https://www.Internet%20fragmenta/ContentBlockingOverview.pdf Accessed 27th February 2023 Internet Fragmentation: The Impacts of Technical Blocking on the Economy of Africa available at https://www.internetsociety.org/events/internet-fragmentation/ Accessed 28th February 2023

Group 3: Protect data

Group Leader: Gilbert Ogolla

Members: Jacqueline Simpson, Stella Nalwoga, Wangari Njaathi, Doreen Abiero

Highlights in the African Context

As of the present, many African countries have enacted data protection legislation. Thirty-three (33) out of fifty-four (54) countries have a data protection framework. Forty-four (44) have a cybersecurity framework, while only 13 have ratified the Malabo Convention that envisions Africa as a single entity regarding data and privacy protection. The Malabo Convention is the only existing Data Protection Policy framework at a regional level in Africa and calls for a harmonised and independent legal framework which protects all stakeholders including data subjects, processors and data controllers.

More than just providing data protection frameworks, some African countries have gone beyond to provide supporting mechanisms for protecting data. Kenya for instance had its Data Protection Act 2019 establishing the Office of the Data Protection Commissioner (ODPC) that has since focused on the enforcement of the Act. ODPC is handling cases such as the use of blackmail by rogue money lending platforms threatening to expose customer data for failure to comply with their terms.

On October 15, 2021, Rwanda's Data Protection and Privacy law went into force. The National Cyber Security Authority (NCSA) was established and tasked with ensuring compliance with the Act. Africa is moving in the right direction as far as working towards Data Protection is concerned, with a majority of the states having in place certain frameworks for data protection.

The challenges relating to Africa as concerns Data Protection are more similar than they are different. All regions seem to have difficulty progressing with certain aspects that hamper robust Data Protection frameworks.

First is the lack of a unified framework that caters to Africa's specific needs, while appreciating Africa's unique situations, our values and systems , rather than what is a generic copy and paste framework that may not serve Africa effectively. Most of the present data protection legislation borrows heavily from the European General Data Protection Regulation (GDPR). The GDPR reflects the values of the EU it seeks to protect, advancing the ownership and suitability to the EU region. This is unlike the prevailing situation in Africa in which our values are not brought forth clearly in our Data Protection laws. Most African states seem to have blindly transferred and applied external data protection frameworks without substantial consideration of their shortcomings in their home origins, and those that may develop in the blanket application to the unique situation in Africa.

Second, Africa is struggling to present a united front regarding a robust regional framework for Data Protection. Only thirteen (13) countries out of a possible fifty four (54) have ratified the Malabo Convention. Twenty-four countries (24) have no data protection framework. They are therefore not progressive at the national level, nor are they progressive at the regional level as they are yet to ratify the Malabo Convention.

Third, the fairly effective legislation that some African countries has enacted, fall short in their enforcement. Very few Data Protection frameworks at the national level established independent bodies charged with enforcement, and most are still grappling with some inconsistencies in the provisions and thus find enforcing such provisions cumbersome. In Equatorial Guinea, for instance, the Organo Rector de Protección de Datos Personales (ORPDP) is statutorily mandated to investigate infractions of data protection rights and issue fines up to CAF 15,000,000. The agency has not been set up since 2016; hence there are no records of its activities. As such, what we have is largely procedural rather than substantive.

Last, there seems to be a myriad of interrelated issues that are hurdles to data protection, among them the presence of outdated laws such as the Data Protection Act passed in Ghana in 2012. There is also the high cost of implementing strategies and solutions to these issues.

Actionable Policy Recommendations

First, we should consider the culture, context and socio-cultural dynamics in Africa that present unique situations. We ought to design data protection frameworks that incorporate local cultural values and norms which could make them more relevant and effective. For example, in some African cultures, the concept of privacy may be viewed differently than in Western cultures. Addressing this would make data protection frameworks representative of Africa's complex social, economic, political, and cultural issues. This could be pursued through the Malabo Convention or similar fora that have the potential to present a united front for Africa. Further, the ratification of the Malabo protocol by all African states could prevent non protected states at a regional level. We also should promote international cooperation on data protection by working with international organizations and other countries to share best practices, coordinate enforcement efforts, and establish global data protection standards that reflect the diversity of African perspectives. In this, Africa should seek to take a participatory and inclusive approach that engages diverse stakeholders on international fora to ensure that they consider a range of perspectives and take the needs and concerns of different groups into account.

Second, African states should endeavor to design dynamic policies that are adaptive to tech advancement alongside strong advocacy to promote stronger data protection legislation and review to keep pace with new technology developments. Digital Currency, for instance, is a focus many African Central Banks. Several regulatory policies on issues surrounding privacy, tax, anonymity and other factors need to be grappled with if at all confidence and security can be built around these systems. Ideally, it is difficult to create policy on what is non-existent, as most advancements always precede policies. This notwithstanding, policy needs to be flexible and adaptive such that we do not have to uproot whole systems to instill new ones everytime.

Third, governments must invest in the resources and capacity of enforcement mechanisms, such as establishing specialized data protection authorities or commissions to enforce data protection regulations and investigate data breaches, training for law enforcement agencies, and imposing reasonably stringent sanctions on data controllers and processors who fail to comply. Moreover, public and commercial institutions should be urged to undertake transparency and accountability measures such as posting data protection policies, performing regular audits, and putting in place independent oversight mechanisms. Monitoring and reporting on data protection procedures in the public and private sectors should be promoted by civil society groups. We should also encourage cross-sector collaboration, such as public-private partnerships or dialogues, to establish data protection standards and recommendations.

Fourth is the need to create more sensitisation on the importance of data protection in this digital age. This can be done through collaboration with local authorities through barazas (informal gatherings called by village chiefs or community elders), whereby data protection authority officials can educate the public on the importance of data protection. On top of this, we should address economic disparities, especially in marginalised communities, design data protection frameworks that address those disparities, and ensure that data protection measures are accessible to all, regardless of economic status. Data protection education can also be incorporated into school curricula, given the great presence of the young generation from an early age on the internet and online social platforms operating on the exchange of data and information.

This is to inform students about their data protection rights and the risks associated with personal data misuse and breaches. African Data Protection Officers or Ministry of IT officials can also organise training for organisations to reach out to corporate-level citizens and institutions, including training and education for data protection authorities and the judiciary, to strengthen the enforcement of data protection laws. To allow the enforcement of all these, Individuals and institutions should be empowered to exercise their data protection rights. For example, by providing resources and support for individuals to access their personal data, file complaints, and seek redress for data protection breaches.

Finally, collaboration and harmonisation will be necessary to promote consistency and reduce confusion for businesses and individuals operating across borders. Legislations should also be unified such that they are not scattered across multiple legal instruments that make these laws difficult to correlate. In addition, cybersecurity measures should be effected through tools such as firewalls, encryption, and multi-factor authentication to protect personal data against cyber attacks.

Individuals

Awareness of their data protection rights, comprehending the dangers inherent in data abuse and breaches, and taking proper precautions to safeguard their data are some ways individuals can contribute to data protection in Africa. Some institutions do not have the investigative capacity to act during data breaches and violations. This calls for proactiveness at an individual level which again is impossible without the knowledge of the existence and application of these rights. This also calls for personal responsibility and reasonable effort to protect one's data by use of strong passwords, careful sharing of sensitive information online where unavoidable, and reporting any data breaches or suspected data protection violations.

Civil Societies

Promotion of greater awareness and understanding of data protection and invest in the power of unison to tap into resources and human resources for capacity building are some actions civil societies can take. They could tap into areas of research on data protection and advocacy for data protection laws and offer training to businesses, governments, and individuals to ensure that they are aware of the risks and best practices for data protection.

Private Sector

Businesses and most private sectors may contribute to data protection initiatives by having stringent policies and procedures. Organisations should also be honest about their data collecting and processing activities, as is required by administrative law, and notify individuals about how their data is being used.

Governments

Governments should seek to champion the foundational process by driving the creation and implementation of comprehensive legal data protection frameworks through legislative and judicial instruments. They should also seek to empower independent instruments charged with certain aspects of data protection to perform their mandate, invest in cybersecurity measures, launch awareness campaigns, and ensure accountability and enforcement of data protection regulations.

Group 4: Apply Human Rights Online

Group Leader: Adedeji Ajani Members: Nelson Otieno, Immaculate Were

Highlights in the African Context

Digital transformation has earnestly taken off in Africa. The African Union has documented its digital transformation agenda in The Digital Transformation Strategy for Africa 2020-2030.³¹ Besides the actual and prospective developmental benefits associated with the digital transformation, the African normative frameworks which includes the Malabo Convention 2014³² and the Personal Data Protection Guidelines for Africa 2018³³ recognizes that the achievements can only be sustainable if they are achieved in an environment that encourages participation and respects human rights.

In particular, The Personal Data Protection Guidelines for Africa 2018 recognises the protection of the right to privacy in Kenya and reaffirms the position in Malabo Convention on the need to ensure that individuals enjoy equivalent online and offline rights. The Guidelines refer to this as an 'important principle'.³⁴ This principle both forms the basis of and has been reemphasised in other related African human rights instruments such as the African Resolution on the Right to Freedom of Information and Expression on the Internet in Africa 2016³⁵ and the Declaration on Principles on Freedom of Expression and Access to Information in Africa 2019.³⁶ The declaration of

³¹ https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

³²https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_securit y_and_personal_data_protection_e.pdf

³³ https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf

³⁴ The Personal Data Protection Guidelines for Africa 2018, p 11.

³⁵ African Commission on Human and Peoples' Rights (ACHPR) Resolution 362 (LIX) on the Right to Freedom of Information and Expression on the Internet in Africa 2016

³⁶ African Commission on Human and Peoples' Rights (ACHPR) Declaration on Principles on Freedom of Expression and Access to Information in Africa 2019

this principle as applying to Africa reflects the position in developing court jurisprudence across Africa and the recognition under the UN human rights system.³⁷

African States have taken legislative measures to address the protection of human rights online with 35 African States now having data protection legislations in place. This, coupled with ratification of the Malabo Convention by some States represent a good step since it seeks to protect cyberspace and provide a framework for protection of personal data. Some notable State initiatives include Ghana which has a joint Cybersecurity Committee whose membership draws from institutions responsible for critical security formations in Africa. In Kenya, the courts now allowed defamation suits to arise from misuse of online platforms. There have been prominent figures who have gotten orders in defamation suits.³⁸ Another example is Nigeria, where citizens successfully challenged a Twitter ban by the Government.³⁹

Africans continue to suffer exclusion in the roll-out of emerging technologies subjecting Africans to discrimination and inequalities either by design or as a spill-over.⁴⁰ It is vital to advance the promise of new technologies, which can only be realised if local communities are involved in decisions for both design and deployment of emerging technologies.⁴¹

Western technology companies have capitalised on data mining in Africa, which makes them sidestep human rights considerations or breach them without due regard to the rule of law just so that they can make profit. Numerous reports such as manipulation of

³⁷ The Resolutions and Declarations of the UN human rights bodies apply to African legal systems by dint of Article 61 of the African Charter on Human and Peoples Rights 1981.

³⁸ "Kenya: Excessive Defamation Damages Violate the Right to Media Freedom - ARTICLE 19." *ARTICLE 19*, 6 Aug. 2021, www.article19.org/resources/kenya-inordinate-damages-violate-media-freedom.

³⁹ Why ECOWAS court declared Twitter ban by Nigerian government illegal

https://www.premiumtimesng.com/news/headlines/542696-why-ecowas-court-declared-twitter-ban-by-nigerian-govt -illegal.html

⁴⁰ https://www.sciencedirect.com/science/article/pii/S2666389922000423

⁴¹ Landry Signé, Njuguna Ndung'u and. "The Fourth Industrial Revolution and Digitization Will Transform Africa Into a Global Powerhouse." *Brookings*, 8 Jan. 2020,

www.brookings.edu/research/the-fourth-industrial-revolution-and-digitization-will-transform-africa-into-a-gl obal-powerhouse.

elections in some African States not only continues colonial tendencies but are also a huge threat to protection of human rights online.

Actionable Policy Recommendations

Individuals

- Observing laws which govern interactions on social media platforms. A study conducted in Kenya noted that one in 5 women suffer from cyberbullying on online platforms. The most common forms of bullying on social media platforms include sexual harassment, unwanted trolling, and doxing. The Kenyan Computer Misuse and Cybercrimes Act punishes crimes on online platforms, for instance, cyber harassment, under Section 27 and Section 22 on false publications. We, therefore, recommend that individuals adhere to laws that govern interactions on social media in online spaces.⁴²
- 2. Individuals are also encouraged to invest in technology and internet service infrastructure so that Africans can slowly regain digital sovereignty.

Civil Societies

- 1. Develop priorities to advocate for a digital development model that balances economic, cultural and social benefits for the people.
- 2. Hold governments accountable through public interest or class actions to enforce the protection of human rights online.
- 3. Actively engage in public participation for a while contributing to developing online regulations and related law reform processes.
- Make valuable research initiatives and contributions in the ongoing search for an appropriate African approach to digital rights and hence the protection of rights online.

⁴²https://www.researchgate.net/publication/348121824_Communication_on_Social_Network_Sites_Asses sing_Cyberbullying_Among_Young_Women_in_Nairobi_Kenya_-_Case_of_Facebook_Platform

Private Sector

- 1. Prioritize human rights in the design of new innovative or emerging technologies.
- Embrace the corporate responsibility to respect all the relevant corporate governance structures to protect human rights in the design and roll-out of its processes.
- 3. Prioritise the emerging insurance opportunities to ensure adequate remedies for persons injured by the actions of others.
- 4. Prioritise consumer trust in corporate processes and products.

Governments

If Africa is to strengthen its digital sovereignty, it is imperative that internet platforms used by Africans are founded, managed and run by Africans. Governments, therefore, ought to:

- 1. Financially support African startups to establish businesses that deal with internet provision.⁴³
- 2. Create conducive legal environments for the set-up and growth of African startups that seek to supply internet and other technological services.
- 3. Judiciaries to strictly enforce laws against cybercrimes on online platforms.
- 4. Operationalizing entities that are mandated with enforcing laws on the internet.

⁴³

https://www.investmentmonitor.ai/tech/why-investors-should-get-behind-africas-emerging-tech-talent/

Group 5: Introduce Accountability Criteria for Discrimination and Misleading Content

Group Leader: Faith Amatika

Members: Joshua Ogwu, Ochieng Ogango, David Gitonga

Highlights in the African Context

Examples of misleading and discriminating content in the African context.

- → Misinformation and disinformation during the 2022 electioneering period in Kenya, such as the conflicting transmission of election results by different media houses.
- → Kenya High Court case calling for Facebook to be accountable for not stopping the spread of hate speech against individuals in Ethiopia and Kenya.⁴⁴
- → Misinformation about the Ebola outbreak in DRC alleging that the government's suspension of the elections due to Ebola was a ploy to postpone the election so as to continue being in power.
- → Misinformation about the Gambia's president Ali Bongo's death leading to an attempted coup in January 2019.⁴⁵
- → Misinformation about presidential candidate Hon. Raila Odinga dancing with musician Moya David with former president Uhuru Kenyatta looking on.⁴⁶
- → Airbnb hosts and guests from African American backgrounds faced some discrimination on the platform.⁴⁷
- → Amazon is not shipping goods to Africa. Purchasers in Africa have to go through MyUS.com.⁴⁸

⁴⁴<u>https://www.amnesty.org/en/latest/news/2022/12/kenya-meta-sued-for-1-6-billion-usd-for-fueling-ethiopia-ethn</u> <u>ic-violence/</u>

⁴⁵ <u>https://www.youtube.com/watch?v=F5vzKs4z1dc</u>

⁴⁶https://pesacheck.org/altered-this-image-claiming-to-show-entertainer-moya-david-surprising-raila-oding a-with-the-da60723a861e

⁴⁷ https://hbswk.hbs.edu/item/racism-and-digital-design-how-online-platforms-can-thwart-discrimination

⁴⁸https://borderoo.com/pages/does-amazon-ship-to-africa-yes-heres-the-solution/

- → Denying people access to certain services based on their country or region; for example, Paypal and Amazon offer very limited services to customers from Asia and Africa besides the stipulation of many restrictive measures.⁴⁹
- → Denying people access to certain services based on their online activities or profiles.⁵⁰
- → Charging people different product or service prices based on their digital footprint.⁵¹
- → Excluding people from certain activities or events based on their online presence.⁵²
- → Segregating people based on their online activities or profile.⁵³
- → Targeting people with advertising or content based on their online activities or profile.⁵⁴
- → Using algorithms to screen out certain applicants for jobs or other opportunities based on their online activities or profile.⁵⁵
- → Discriminating against people based on their online activities or profile in hiring, promotion, or other employment decisions.⁵⁶
- → Limiting people's access to information or resources based on personal features.⁵⁷
- → Cyberbullying for instance, the case of Jimmy Gait who was trolled and vilified for a song he authored and released.⁵⁸
- → Misinformation when it comes to reporting on credible data about Africa to drive investments or focus on Africa in specific industries.

Causes of misleading information and discrimination

1. Unprofessional Journalism: The central narrative surrounding fake and misleading information is the desire for journalists and media influencers to gain traction and make quick profits off fake news. Research by the BBC conducted in Kenya and Nigeria proved that social media users surveyed in both countries believe fake stories are spread purely to make money.⁵⁹

- ⁵⁴ ibid
- 55 ibid
- 56 ibid
- 57 ibid

⁴⁹https://www.linkedin.com/pulse/what-digital-discrimination-chris-ezeh/

⁵⁰ibid

⁵¹ibid ⁵²ibid

⁵³ibid

⁵⁸https://hivisasa.com/posts/kenyans-respond-after-jimmy-gait-cries-on-tv

⁵⁹ https://republic.com.ng/vol3-no3/africa-misinformation-struggles/

- Politicisation of Information: Political associations, groups and parties usually spread fake and misleading information to preserve their varying political interests. Most of this information is classified as propaganda, primarily created to favour a political leaning and to put the opposition in disrepute.
- 3. Political Propaganda: Some States manipulate information to advance their varying interests. Sometimes, this propaganda is usually transboundary, carried out by states to influence positive /negative response to government decisions and policies to safeguard government interests. For instance, Russia has been accused of setting up specific troll farms to influence the media in the Central African Republic.⁶⁰ Also, In 2021, Facebook reportedly pulled down more than 500 accounts, pages and groups from Facebook and Instagram targeting African users with misleading information.⁶¹
- Technological Advancements: This can contribute to enabling people to create fake information without the same being easily recognized as fake. A typical example is Deepfake.⁶²

Effects of misleading and discriminating content

- → Violent Crisis, e.g. Rwanda genocide in 1994. Kenya Post Election Violence in 2007-2008.
- → Public disorder and political instability.
- → Social instability because of mental stress from trolling and online discrimination.

Risks and Challenges

- → Low digital literacy skills.
- → Regulation is tricky because technology advances faster than the law.⁶³
- → Limited resources for training forensic experts.

 ⁶⁰ https://www.info-res.org/post/russian-disinformation-in-the-central-african-republic
⁶¹ https://qz.com/africa/1947174/facebook-pulls-russian-and-french-disinformation-trolls-in-africa
⁶²Faith Amatika-Omondi, 'The Regulation of Deepfakes in Kenya' (2022) 2(1) JIPIT 155

<<u>https://journal.strathmore.edu/index.php/jipit/article/view/208/227</u> > accessed 20 February 2023

Actionable Policy Recommendations

Individuals

Individuals are significant propagators of discriminatory or misleading information. Some do it out of ignorance, spreading misinformation, while others do it intentionally. Civic education should be emphasised to enlighten ordinary citizens on 'not forwarding a message unless they are sure'. It still falls on the government to educate the public. That notwithstanding, individuals are responsible for stopping the spread of misinformation and disinformation. Individuals should be able to educate themselves and know that not all information is genuine and that they should be able to sieve through it. Considering the source is also a way to help individuals not to believe the information in question. For instance, if information comes from a suspicious website, it is likely fake.

Civil Societies

Several civil society groups have been established in various parts of Africa to combat the spread of misinformation. Their efforts should be lauded and replicated. They include the following organisations.

In Kenya, there is the Africa Uncensored,⁶⁴ an independent media house set up by 'Kenya's finest investigative journalists'.⁶⁵ Their goal is to investigate, expose and empower and this resonates quite well with their editorial policy, which is just two words, 'THE TRUTH'.⁶⁶

Another fact-checker is known as 'Piga firimbi' (translated as 'blow the whistle'). Piga Firimbi is an offshoot of Africa Uncensored whose aim is 'to provide readers and the general public with access to factual information on the validity of claims being made in news/media reports and on social media.'⁶⁷

⁶⁴https://africauncensored.online/about/ ⁶⁵ibid

⁶⁶ ibid

⁶⁷https://pigafirimbi.africauncensored.online/about/

Another fact-checker in Kenya is Pesacheck,⁶⁸ which also sieves through information and alerts consumers of information on whether it is authentic or doctored. Pesacheck prides itself in being 'Africa's largest indigenous fact-checking organisation, debunking misleading claims and deciphering the often-confusing numbers quoted by public figures in 15 African countries'.

However, some challenges bedevil Civil Society Organizations (CSOs), which may impair their objectivity and efficiency in calling out discriminatory and misleading content. They include the following:

- Lack of access to social media data⁶⁹ unequal or insufficient access to data and metadata impedes CSOs' ability to analyse and give their findings on its authenticity. This is caused by private companies' (social media) unwillingness to share the relevant data with the CSOs.
- Duplicative programming⁷⁰ Using the same tools by different CSOs to analyse data means the same results will be obtained over the same data by different CSOs. This means that some information may not be adequately analysed thus posing a threat of leaving out crucial information.
- 3. Varying relationships with tech giants/platforms across regions⁷¹ some tech giants deal preferentially with some CSOs including in areas of funding, raising questions as to independence and objectivity. It was also observed that CSOs in the Global South countries and in Eastern Europe have challenges accessing some tech giant's data.
- 4. Regional divides in capacity affect the type of responses pursued by CSOs⁷²- where CSOs are driven only by the desire to debunk any lies but still lack the technical know-how of how to go about it, the result is half-baked information. Therefore, investors must invest in an all-round CSO rich in journalism skills, human rights, law, data protection, software engineering, data analysis, artificial intelligence, deep learning, etc., to comprehensively analyse any information and provide a comprehensive approach.

72 ibid

⁶⁸ https://pesacheck.org/

⁶⁹ https://www.ned.org/mapping-civil-society-responses-to-disinformation-international-forum/

⁷⁰ ibid

⁷¹ ibid

Private Sector

The private sector includes several players in the information ecosystem. They include broadcasting houses and big tech companies. They bear the heaviest burden because they control what goes out to the public for consumption.

In Africa, Big tech companies such as Facebook, TikTok and Twitter are responsible for moderating information that could be misleading or discriminatory. Content moderation has been both a success and a failure. It failed when Facebook failed to moderate misleading content about an Ethiopian activist leading to his death due to mob calls for his death on social media.⁷³ However, a success story is seen in Twitter policies that prescribe ways to help individuals identify whether the information is fake or genuine.

Further, in a bid to 'make lying wrong again,' social media should up the standards of truthfulness by rewarding those social media users who disseminate authentic information and vice-versa.⁷⁴

For broadcasting houses, it is necessary for them to invest in fact-checking.⁷⁵ This is where journalists should be able to interact with the public. They should be able to point out to the public the authentic sources of their information. Media houses should also invest in teaching children and the elderly about misinformation and what to be on the look-out for.⁷⁶ This is part of their Corporate Social Responsibility.

It is further suggested that instead of working in silos and as competitors, media houses should collaborate and work as partners to weed out the infodemic that has plagued society today.⁷⁷

Governments

We have identified that most Tech giants such as Facebook and Twitter, have remained relatively inactive in the moderation of African content. From existing literature on

⁷³https://www.amnesty.org/en/latest/news/2022/12/kenya-meta-sued-for-1-6-billion-usd-for-fueling-ethiopia -ethnic-violence/

⁷⁴https://ijnet.org/en/story/strategies-countering-spread-misinformation

⁷⁵https://ijnet.org/en/story/strategies-countering-spread-misinformation

⁷⁶ibid

⁷⁷ibid

disinformation across Africa, we identified two major approaches the government could take in dealing with misleading content.⁷⁸

- → The technological approach.
- → The legal approach.

The technological approach involves censoring or blocking access to content to prevent the spread of fake news or hate speech. As noted, most tech giants do not regulate content in Africa. For instance, the infamous Kenyan High Court Case against Facebook for failing to censor hate speech content.

Most governments employ content blocking where social media platforms are shut down, or the internet is generally interrupted. The blocking of certain social media platforms has been experienced in countries such as Central African Republic, Ethiopia and Cameroon. This approach might not prove effective as it is often draconian and causes the interruption of otherwise essential services.

The legal approach involves legislation. Constitutions of most countries guarantee freedom of expression, but freedom is not absolute. It is subject to limitations based on a just and democratic society. It can be limited in cases where the expression is likely to result in hate speech, incitement to violence, propaganda for war or advocacy for hatred.⁷⁹

Other laws are also in place; for instance, Kenya has the Computer Misuse and Cybercrimes Act No. 5 of 2018, the Penal Code, etc. In Nigeria, there is the Cybercrimes Act and the Anti-terrorism Act.

In Nigeria, the National Information Technology Development Agency (NITDA) has issued a Code known as the draft Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries ("the Code").⁸⁰ Under this code, the government has the power to take down content that is misleading or discriminatory within 24 hours. The challenge is that there is no

⁷⁸https://blogs.lse.ac.uk/africaatlse/2021/11/25/how-african-countries-respond-fake-news-and-hate-speec h-tech-regulation/

⁷⁹ Article 33(2) Kenyan Constitution.

⁸⁰https://www.mondaq.com/nigeria/social-media/1206270/exploring-the-nitda-code-of-practice-and-its-pot ential-impact-on-social-media-and-online-platforms

accountability mechanism to determine what misleading content is. The government may hide behind this to censor content that paints it in a bad light even if it is true. This is therefore a call to governments to ensure that enacted laws do not conflict with human rights.

The government should also invest in training law enforcement officers and forensic experts on distinguishing between fake and genuine information on digital platforms.⁸¹ This will go a long way in ensuring that only fake and misleading information is pulled down instead of any information that appears to be calling out the government on its wrongdoings or failures. The training of forensic experts will also go a long way in ensuring that photo and video evidence that is tendered in court is of probative value.⁸²

 ⁸¹ Faith Amatika-Omondi, 'The Regulation of Deepfakes in Kenya' (2022) 2(1) JIPIT 155
<<u>https://journal.strathmore.edu/index.php/jipit/article/view/208/227</u> > accessed 20 February 2023
⁸²ibid

Group 6: Promote Regulation of Artificial Intelligence

Group Leader: Chinasa T. Okolo

Members: Clarisse Mideva, Nancy Gacheru, Joel Adefidipe, Cynthia Chepkemoi

Highlights in the African Context

Regulation of Artificial Intelligence within the African continent is beginning to emerge. According to the 2021 Government AI Readiness Index by Oxford Insights, countries from Sub-Saharan Africa rank the lowest on average, with a readiness score of 31.61/100 compared to a global average of 47.42⁸³. Only 3 African countries rank above the global average: Mauritius (52.71), Egypt (49.75), and South Africa (48.24).

While no African country has formally enacted national AI legislation, much work is in progress. 30 African countries have data protection legislation, and four countries have a national AI strategy, one country (Tunisia) has a draft policy or a white/green paper on AI, and 13 countries have established an expert commission or task force on AI. Presently, six countries prioritise AI in their National Development Plans, while the plans of 4 other countries partially mention AI.

Work is also being done on a continental level with the African Union (AU) Development Agency drafting the first continental strategy for Africa⁸⁴. This strategy aims to guide AU Member States in harnessing AI technologies responsibly for socioeconomic growth. While regulation is a great step, African countries have a long way to go in terms of building the necessary capacity to support active AI ecosystems. Methods to build AI capacity include strengthening internet access, establishing research centres, improving STEM curricula, and supporting native AI startups.

The efforts put in by African countries to make progress towards regulating AI are promising, however, there exist some barriers that could hamper the effective adoption and promotion of such policies. While some African countries have national AI strategies, they may not have the legal and regulatory frameworks to implement them effectively compared to other regions. For example, the EU and the United States have comprehensive regulatory frameworks that touch on the development and use of AI. There is also a limited capacity for oversight and

⁸³ https://www.oxfordinsights.com/government-ai-readiness-index2021

⁸⁴ https://www.nepad.org/news/african-union-artificial-intelligence-continental-strategy-africa

enforcement of AI regulation. Most African countries lack the technical and human resources to implement effective oversight and enforcement mechanisms.

African countries and governing bodies could mirror initiatives such as the EU's High-Level Expert Group on AI⁸⁵ to build this capacity. African countries may not have established mechanisms for public engagement and participation in AI Policy and regulation, limiting the potential for AI regulation to be passed and for the general public to understand and take these measures seriously. Unlike the EU⁸⁶ and the US, which have ethical guidelines, many African countries lack transparency and accountability requirements or do not have sufficient ethical guidelines for AI systems. Many African countries also have limited capacity to engage effectively in discussions and negotiations on AI regulations. The EU, US, and countries within Asia, Latin America, and Oceania actively engage in these discussions through forums such as OECD.AI⁸⁷ and Global Partnership on AI⁸⁸.

One of the most important factors limiting the promotion and development of AI regulation within Africa is the limited resources for AI research and development. Many African countries lack the financial and technical resources to invest in AI Research and Development (R&D), thus limiting their ability to keep up with global AI developments and develop solutions that address their specific challenges and needs.

Challenges and risks associated with promoting the regulation of AI in Africa

Currently, a major concern is the deployment of AI systems without robust regulatory and legal frameworks within the continent⁸⁹. Additionally, a lack of inclusivity in the generation of AI systems has resulted in unprecedented bias against people of African descent⁹⁰. The innovation and development of AI should take an all-inclusive approach to avoid such bias. Another concern is the reliance on foreign AI technologies. Although Africa has great innovators and inventors, it's unfortunate that most don't work for home-based entities. Talent export has stifled

⁸⁵ https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai

⁸⁶ https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

⁸⁷ https://oecd.ai/en/wonk/oecd-and-g7-artificial-intelligence-initiatives-side-by-side-for-responsible-ai ⁸⁸ https://gpai.ai/

⁸⁹ https://afripoli.org/ai-in-africa-key-concerns-and-policy-considerations-for-the-future-of-the-continent

⁹⁰ https://paradigmhq.org/algorithmic-apartheid-african-lives-matter-in-responsible-ai-discourse/

Africa's capacity to have local solutions that are fit for the economic status of most African countries.

Some challenges include a lack of technical expertise in the continent across the research, development, and legal processes, which hampers the policy development process that is more inclined to ICTs. Additionally, the existence of unfair labour practices, especially in regards to remote data labelling and content moderation jobs, often known as 'click work'. Large foreign tech companies seek cheaper labour in Africa⁹¹ and other regions within the Global South to label the data needed to train their massive AI systems, often not inclusive of consumers from these regions.

Multi-stakeholder engagement is also a challenge slowing the regulation of AI within Africa. Overall, there is a lack of collaboration among stakeholders at the local, regional, and state levels in the policy development process.

There are also several risks that African governments should be concerned with regarding the adoption and regulation of AI technologies. In as much as there are several benefits of using Digital ID to curb identity theft, money laundering, and fraud, research shows that most African countries adopt it without first conducting impact assessments. AI-driven digital identification powered by facial recognition systems and other verification systems poses a high risk to the rights of users⁹². Given the challenges seen in facial recognition systems in the United States and other Western contexts⁹³, there is a high likelihood of bias and discrimination that may affect minority populations within Africa. AI technologies like facial recognition also pose a high risk of unnecessary surveillance in general, which could result in the infringement of fundamental human rights such as the right to privacy⁹⁴. AI also poses many risks to labour laws for employment protection in cases where AI replaces humans, such as in application screening, performing managerial duties, and conducting employee performance reviews. AI used for these tasks could lead to unequal treatment in the workplace and cause both direct and indirect discrimination. AI technologies also have the potential to negatively impact the health and safety of human employees working alongside robots for more manual labour roles.

93 http://gendershades.org/

⁹¹ https://time.com/6247678/openai-chatgpt-kenya-workers/

⁹² https://www.refinitiv.com/perspectives/financial-crime/digital-id-in-africa-leading-the-fraud-fight

⁹⁴ https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa-part-5-of-6/

Actionable Policy Recommendations

Individuals

As members of society, individuals are vital in shaping the regulation of AI in Africa. They can contribute to this process in many ways, i.e.

- → By creating awareness on AI development, governance, accountability, use and responsibility through healthy debates with policymakers, their peers, fellow social media & AI users and colleagues.
- → By supporting the efforts of the government to educate the public on AI-related topics to create a skilled workforce that can support the development and regulation of AI.
- → By advocating for transparency, accountability and human-centred design in AI development and deployment. This will, in turn, promote ethical practices.
- → By being active in public participation to ensure their effective representation in all stages of the AI lifecycle and the development of AI legislative frameworks.
- → By advocating for diversity and inclusion and the participation of underrepresented people in developing and deploying AI systems.
- → By ensuring that AI systems are transparent on the kinds of data they are collecting and how the data is being used by encouraging data protection and privacy.
- → By educating themselves on the technical aspects of AI to stay informed on AI developments and advocate for AI regulation.
- → Through sharing how using AI has positively or negatively impacted their lives. This will create a conversation and an open space for people to share their experiences.

Civil Societies

Undoubtedly, civil society organisations (CSOs) are important in promoting AI regulation and governance. Since they are considered closer to the public, they are well-positioned to influence AI policy and regulation based on public opinion. CSOs could carry out this role in the following ways:

→ Advocacy: CSOs can be at the forefront of pushing for people-centric AI laws. They can make recommendations on how laws and policies can be framed to ensure that the rights and interests of the public are protected. They could also act as a watchdog that monitors the implementation and enforcement of AI policies and laws.

- → Education and awareness: In Africa, many are not tech-savvy, and probably do not know when they are interfacing with AI. CSOs could remedy this. CSOs, through education and raising awareness, can arm Africans with the ability to identify unethical AI and their rights when AI infringes them. Education and awareness can also position Africans to hold other stakeholders in the AI industry and the government accountable for ensuring that the technology is deployed ethically in Africa.
- → Collaboration with other stakeholders: CSOs can collaborate with the academia, private sector, government and international bodies to build AI systems compliant with ethics. This could involve conducting surveys or research on how AI can potentially impact the rights and freedoms of Africans. They could also help develop ways that these stakeholders can mitigate or eliminate risks in using AI by the government and the private sector. CSOs could also give feedback to these stakeholders on their systems' effectiveness and policies' efficiency. Furthermore, CSOs could collaborate with the government in AI policy-making to ensure that the perspective and interests of the public are duly represented and considered.
- → Public Interest Litigation: To promote AI governance and ethics and ensure redress when the public is unduly exposed to the risk of AI, CSOs can take legal action when an injury is occasioned to the public by AI. By taking legal action, CSOs can ensure that the public is protected from potential harm and that the responsible parties are held accountable for their actions.

Private Sector

- → Private institutions should carry out a review and assessment of existing data protection and Intellectual Property laws to determine whether they sufficiently protect the right to respect for private life, the right to data protection and Intellectual Property rights in the context of AI systems. And institute legal reform where they do not.
- → In order to avoid discrimination, private institutions should apply the highest level of scrutiny when using AI systems in law enforcement, especially to avoid profiling individuals belonging to specific groups. An example is where banks use AI to draw data from the past to make future predictions when making lending decisions for individuals.
- → Research indicates that private corporate entities tend to put profits before human rights. To curb this non-compliance with human rights laws, private institutions should

enforce existing laws where necessary to meet the state's duty to protect the human rights of individuals against violations by AI actors.

→ Private Institutions should introduce laws and regulations requiring HRIAs (Human Rights Impact Assessments) to be conducted about AI systems that have been or may be acquired, developed or deployed by public authorities.

Governments

African governments play a critical role in promoting and controlling the use and development of AI to enable them to reap the benefits of AI and unlock economic benefits while also ensuring its citizens are protected from the negative impacts of AI. Governments must take a proactive multi-stakeholder approach by

- → Establishing technical expert groups consisting of national, regional and international experts to help establish regulatory frameworks and ethical guidelines that will encourage the development and use of AI technologies. While doing this, governments should also be wary of over-regulation, which could stifle innovation within the respective countries.
- → Enhancing public engagement and participation. This includes engaging with the private sector, academia, CSOs, individuals and other stakeholders to ensure that their concerns and perspectives are incorporated into the development and regulation of AI and warrant their involvement in decisions around the development and deployment of AI systems that may affect them.
- → Fostering collaboration with regional and international organisations to harmonise regulations and standards and to ensure that AI is used and developed in a manner that aligns with global ethical and regulatory standards.
- → Engaging in international initiatives such as the Global Partnership on AI, OECD.ai, etc, to share best practices and gain a global perspective and presence within AI governance. This will ensure that African countries are not left behind in the global AI race.
- → Supporting AI research and development through funding research institutions/AI research centres and supporting startups to drive innovation and ensure that African countries develop solutions that address their specific challenges and needs. Governments can also initiate AI projects that will benefit citizens in areas such as transportation, security, healthcare etc.

- → Investing in AI education and skills development to create a skilled workforce that can support the development and regulation of AI.
- → Governments must refrain from using AI Systems that may lead to or cause bias or discriminatory outcomes. Discrimination risks can be prevented and mitigated with special attention to the minorities such as women, children, the elderly, people with disabilities as well as members of the LGBTIQ community. This should be done by applying the highest level of scrutiny when using AI systems.

Promotion of regulation of AI in Africa is essential for the region's sustainable growth. While AI presents tremendous potential for innovation, economic development, and social advancement, it poses risks if unregulated. As a result, African countries must take a proactive stance towards AI regulation, building on existing international frameworks and tailoring them to fit local contexts. AI can be a force for good in Africa, helping address some of the continent's most pressing challenges and paving the way for a better future for all if the right policies and practices are put in place.

Group 7: Digital Commons as a Global Public Good

Group Leader: Kingsley Owadara Members: Odette Bester, Marco Grieco

Highlights in the African Context

Executive Summary

The United Nations Digital Strategy (2022-2025) defines digital as "an ever-evolving range of technologies (like mobile technologies, artificial intelligence, machine learning, blockchain, Internet of Things, and robotics, to name a few) that impact all aspects of our world.... a mindset, which translates into a new way of working that enables people and institutions to innovate with technology."

From the preceding definition of digital, the continuously evolving nature of technology would influence our traditional way of interpreting, developing and deploying shared values from one form to another and from one person to another in society. To properly put this into perspective, commons are cultural and natural resources held, managed and accessed by community members in which everyone has a common interest. In other words, it is called a "Shared resource". The "digital" and "common" meeting together breeds the concept of Digital Common.

This report advocates the use of Digital Common for the public Good. Since there is variance in what constitutes "public good" from society to society, this report adopts Article 19 of the Universal Declaration of Human Rights (UDHR) and the United Nations Sustainable Goal as a yardstick to an end of reaching a widely accepted concept of the public Good. Sustainable Development Goals such as Good health and well-being (Goal 3), quality education (Goal 4), Industry, innovation and infrastructure (Goal 9) are critically considered as a channel to reaching the public good.

Using case studies of open-source software, open-source data, copyrighting and Intellectual Property, the report concludes with a multi-stakeholder recommendation and a conclusion.

Introduction

Digital commons refer to several resources such as data, information and other sources of knowledge which are created and kept online, and on which the community of people building them can intervene in the processes and interactions of the shared resources. Digital commons represent an essential source of information to which the community can easily access and contribute directly.

This analysis aims to define general guidelines to leverage the power of these ecosystems for the Public Good. The definition of Public Good that will be taken into consideration is in line with the UN Secretary General's Roadmap for Digital Cooperation, which defined Digital Assets with the purpose of Public Good as: "open source software, open data, open AI models, open standards and open content that adheres to privacy and other applicable laws and best practices, such as do no harm, and help attain the Sustainable Development Goals."

The analysis will consider three specific technology verticals within Digital Commons. Each one will be streamlined from the challenges it represents in the continent to the solutions that African governments can implement. The first one is open data which can help communities to enhance public oversight of governments and helps reduce corruption by providing greater transparency. Second, if appropriately leveraged, Open Source Software Development can generate responsive and flexible ecosystems to build and deploy the technology. Finally, we propose a balanced approach towards copyright which can benefit both authors and communities, drawing inspiration from Article 19 of the Universal Declaration of Human Rights. Article 19 provides that everyone has the right to freedom of opinion and expression, including the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Case Study 1: Open-Source Software

Africa is thinking big about digital development. Increased digitalisation and technology adoption have fueled the African economy and created numerous jobs and opportunities throughout the continent, advancing financial inclusion and making technology a key sector for several African countries' Gross Domestic Product (GDP).

Open-source refers to making source code freely available to the Public, allowing anyone to view, modify and distribute the code. In computer science and software development, open source is essential for several reasons, as it promotes collaboration among individuals, innovation, accessibility and inclusion in the tech space. The economic benefits of open source technologies have recently attracted a growing move towards adopting open source software (OSS) options in developing countries. The developing world is now overtaking the developed world in open-source adoption.

Over time, Africa has increased the number of people connected to the internet. Researchers have estimated that at least a quarter of the population of Africa has internet access, with some perspective that three-quarters of residents will be connected by 2030. Due to this growing adoption of digital technologies, open-source software has become a key trend in Africa in recent years.

In this regard, the phenomenon became increasingly relevant in the early 2000s, being included in African regulations for the first time. In 2002 and 2003, the South African Cabinet noted and adopted policy recommendations from the Government IT Officer's Council (GITOC) about Free & Open Source Software (FOSS), establishing the government criteria for implementing Free and Open Source Software over proprietary software.

In 2006, Zambia included in its Information and Communication Technology Policy the possibility of adopting open-source software in developing E-Government solutions. In 2012, Nigeria, in its National ICT Policy, promoted the use and development of Free Open Source Software throughout the country. In 2014, Egypt's Ministry of Communication and Information Technology became the third largest country in 2020 for the number of contributing users of Open Software Development according to GitHub.⁹⁵ Egypt released a document explaining Egypt's National Free and Open Source Software strategy, which introduced the concept of a multi-stakeholder approach towards adopting emerging technology.

In 2019, Kenya proposed harmonising ICT policy and legal and regulatory frameworks with the other East African Community member states in its National ICT Policy. Local data protection

⁹⁵ GitHub is a public repository for open source software.

laws came into force recently as South Africa's Protection of Personal Information Act (PoPI), effective from 2021. The Act aims to influence every organisation that manages a large amount of data to comply with specific security standards by appointing Information Officers and starting Data Asset Registers.

The Risk and Challenges in Africa

Some initiatives have succeeded, others moderately, while several failed due to their significant dependency on licensing, ease of system integration within the ecosystem and stakeholders' resistance to change.

The ecosystem's orchestrator has a crucial role in its design, development and support over others' stakeholders (e.g. 24/7 technical support, training and maintenance) and a clear goal towards the public Good. Mostly, orchestrators are private entities due to the technical complexity and capacity needed to ensure the ecosystem works, which, however, can sometimes be reluctant to change and profit-driven.

Moreover, orchestrators have to deal with licensing issues and terms that present little protection to licensees in the case of open software due to the numerous opportunities for contributors to introduce infringing codes. Meanwhile, it creates the risk of a possible intellectual property infringement claim. It may be difficult for licensors to recover anything against the parties involved, especially those with small financial/capital substance. Africa should consider a regional approach towards framework licensing systems, making creating standards to regulate Open Source Software projects easier.

Case Study 2: Open Data

Open-source data plays a pivotal role in modelling African database technologies. These include the codebase of applications, software, or algorithms that can be viewed, downloaded, modified, distributed, and reused. The intersection of database technologies and traditional commons created the Digital Commons concept. The aim is to make it accessible to all community members.

When resources are held in common raises the question of ownership and permission of the preceeding owner regarding the manner of usage. Unfortunately, there are instances where the

right to those resources is lost due to the longevity of creation time. In Africa, several laws and policies regulate the usage of the digital commons. It can be either general or sector-specific laws /policies on data protection, Intellectual property laws, cyber security laws, copyrighting laws, property laws, Information technology laws or even sector-specific laws. Open-source licenses allow developers to build new applications using existing database technologies. It makes the process faster, more effective and more robust.

Case Study 3: Copyrighting and Intellectual Property

The Digital Commons in Africa refers to the potential for digital technologies to enable shared knowledge, resources, and tools across the continent. This concept has significant implications for copyrights and intellectual property, as the increasing availability of digital resources poses challenges to protecting intellectual property rights.

One of the key benefits of the digital commons is the potential for knowledge-sharing initiatives. With the increasing availability of digital resources such as online learning platforms, open-access journals, and collaborative tools, Africans can access and share knowledge more efficiently than ever. In addition, it can support education, research, and development initiatives across the continent. This happens across Africa, with ongoing efforts to develop copyright and IP protocols containing guiding principles within this context. This forms an essential role in implementing Africa's digital transformation strategy.

As Article 26 of The Universal Declaration of Human Rights states, 'everyone has the right to education. Education shall be free, at least in the elementary and fundamental stages. Elementary education shall be compulsory. Technical and professional education shall be made generally available, and higher education shall be equally accessible based on merit.' This reinforces Article 19 mentioned above - regarding the right to receive and impart information and ideas.

However, as more information is shared digitally, the risk of intellectual property infringement and theft remains an issue. For example, copyrighting is the process of creating written content that is protected by copyright laws. This can include books, articles, blog posts, and other types of content. However, with the increasing availability of digital resources, it has become easier for individuals to copy and distribute copyrighted material without permission. In addressing this, many African countries are trying to establish legal frameworks for intellectual property protection - including regulations protecting copyright owners' rights and developing technological solutions that help prevent infringement and theft.

Examples include initiatives like

- → The South African National Research and Education Network (SANReN) provides high-speed internet connectivity and advanced digital tools for researchers and educators in South Africa. They have played a critical role in enabling researchers and educators to connect with those in other parts of the world to help build the research capacity in South Africa. However, countries like South Africa are bound by international copyright laws that restrict the use and dissemination of copyrighted materials. This means that researchers who use copyrighted materials may infringe on the copyright owner's rights leading to legal challenges. South Africa has developed policies and guidelines promoting the responsible use of copyright Policy for Higher Education encourages the use of open-access resources and enables institutions to negotiate fair use agreements with copyright owners. In 2019, the Copyright Amendment Bill was introduced, which seeks to introduce provisions for proper use, expand exceptions for educational use, and improve access to copyrighted materials for persons with disabilities.
- → The Nigerian government introduced an open-access policy for all federal universities. The procedure requires all researchers and academics to deposit their research output in institutional repositories within six months of publication, such as the Nigerian Virtual Library (NVL) or other approved repositories. This policy aims to promote access to research output and increase the visibility and impact of Nigerian research.
- → The African Digital Rights Network (ADRN) is a network of civil society organisations and individuals that promotes digital rights and freedoms in Africa, including access to information. The network has advocated for policy and legal reform supporting access to information, such as the passage of the Freedom of Information Act in Nigeria.

→ The Digital Repository of Scientific Information (DRSI) in Kenya is also a national platform that provides open access to research output from Kenyan universities, research institutions, and other organisations. The platform includes a wide range of research output, including journal articles, conference papers, theses and dissertations, and research reports. The DRSI has been instrumental in increasing the visibility and impact of Kenyan research by making it accessible to a global audience. By providing open access to research output, the platform has also helped promote collaboration among researchers and institutions and developed new research partnerships and alliances.

The Risk and Challenge in Africa

- → Law reformation: The Global North and Western states continue to exert enormous influence on African copyright law reform efforts to benefit significant corporate interests. Often this can lead to threats of trade sanctions or aid for African countries, hindering researchers, libraries and archives. However, the balance between access to these resources and the licensing and recognition of those who develop these materials is a continuous challenge. It is vital to ensure credit is attributed to authors and contributors of these sources while shared access is made available. Even when political leaders recognise the importance of addressing copyright and access to information, reform may need to be faster due to bureaucratic processes, political deadlock, or lack of resources.
- → Copyright and access to information: Other obstacles worth noting are the failure of political leadership to address the concerns around copyright and access to information
 with reform and governance needing to be faster to address these issues. Contributing factors include the secrecy culture, low public awareness and institutional barriers.
- → Security Concerns: Many organisations, including governments and private companies, have a security culture that can make accessing information difficult. This is understandable to a certain degree, but the balance between security and access needs to be taken into consideration in order not to hinder efforts to address concerns around copyright and access to information.

- → Lack of awareness: Many people may need to be made aware of the importance of copyright and access to information or may need help understanding this issue which can make building public support for reform challenging.
- → Other institutional barriers include legal frameworks, technical limitations, or resource constraints.

Actionable Policy Recommendations

Individuals

→ Individuals can educate themselves about copyright laws, open access initiatives, and the importance of access to information to help them make informed decisions about using, accessing and sharing information. By supporting open access initiatives, they can advocate for policies that promote open access to information while also promoting the respect of copyright laws that call for permission to use materials, citing sources properly, and avoiding plagiarism.

Civil Societies

- → Civil society should work towards improving individuals' collaboration into Open Source Software projects with a clear purpose towards strengthening the sustainable development of the country in question. Several kinds of research highlight the crucial role of non-coding contributors to OSS projects as moderators, coordinators and people who stimulate debate in the community.
- → Raising public awareness of these issues can help build support for reforms. For example, advocacy campaigns, educational programs and media outreach can drive more awareness so communities can also participate in the discourse of the challenges mentioned above. In addition, encouraging collaboration among civil society, governments, and the private sector can help identify and address access barriers to information access. This includes collaboration on policy development, research and technology developments.

- → Possibility of considering research development as a fundamental human right to support open access to information. Constructing the right to research as an annexe to the right to education can help match the exercise of copyright by copyright owners. The development of criteria when requesting information and research by Individuals and organizations can support and encourage those leveraging this material to seek permission from copyright owners before using their material and qualify the purpose and use of this material so that it can also be appropriately attributed to the original author or creator. A human rights approach can help ensure equality of rights between copyright owners, researchers, libraries and archives.
- → Additionally, platforms and publishers can explore new models for revenue generation, such as advertising or subscription-based models which can provide access and support accountability when giving credit to the author or creator. However, in striking the appropriate balance between authors' private concern and the public interest through a right to research, different considerations must be made depending on the type of research since commercial and noncommercial research will affect the material interests of authors differently.
- → Civil societies can play a dual role, stimulating public debate on the topics to stimulate reflections and awareness on entities' commitment towards public Good and promoting education and skills development among the population to raise general engagement and understanding of the topic. Civil society's historic mission in the relationship with these new entities should be grounded in promoting social Good through accountability, fairness, transparency and trust over all aspects of mutual activities.

Private Sector

→ The private sector is crucial in infrastructure capacity and technical capability to support Open Source Software projects. However, several challenges must be addressed to fully collaborate with governments, individuals and civil societies. One of them is Africa's composition of numerous small and separated markets. Historically, individual governments have integrated neighbouring markets by negotiating trade agreements to create regional economic communities. As a result, conditions throughout much of Africa are starkly different—not only is there a tremendous excess of labour, but many workers are also largely untrained or, at least, under-trained. The high unemployment rates that result from excess labour pose a potential security threat to the quality and stability of the continent's business environment.

- → To leverage private sectors' innovation and funding, governments must bring together private and public sustainable development objectives and offer an opportunity for businesses to rebalance and reduce risk exposure to their proposed undertakings. These types of partnerships can reduce input costs, improve supply chains and benefit the region/country where they are based.
- → It is also essential to track and define accountability criteria for the stakeholders involved when attracting and involving new players. Transparency should be the fundamental criterion to judge the effective contribution towards the public Good.

Governments

- → It is crucial to outline guiding principles in proposed IP and copyright laws to formulate a way to allow African countries some policy space to develop open, flexible and balanced national copyright systems suitable to solving the access challenge. This can help support the updates to legal frameworks and ensure that they help promote access to information that respects IP rights. This includes copyright, data protection, and freedom of information laws.
- → Furthermore, to maximise the benefits of the digital commons while minimising the risks, it will be essential to establish robust legal frameworks for intellectual property protection and promote the responsible use of digital resources through education and awareness-raising efforts.
- → On the other hand, to ensure transparency and software quality, governments should find ways to ensure people's knowledge of the legal and technical aspects of their contributions.
- → Governments adopt OSS policies for various reasons, such as infrastructure modernisation, digitisation, interoperability, e-governments and cutting technology costs relying on external resources. However, the essential thing in policy-making should be to attribute within the governments' roles to represent the good public interest in the ecosystem and project creation, ensuring transparency and accountability criteria for stakeholders' involvement.

- → Government should be responsible for creating clear guidelines, governance, processes and checks to manage potential security, legal, and operational risks for every organisation involved.
- → Currently, in Africa, according to a recent WEF report, 22 of 25 countries analysed had no public policies focused on an ecosystem for innovation, thus creating several difficulties for OSS projects to create excellent outcomes in terms of public Good. From a geographic and sectoral point of view, investing in broad-based digitalisation is crucial to address socioeconomic problems and dealing with peace and security challenges.
- → African institutions must cooperate to uphold Africans' fundamental rights and interests against profit-oriented approaches.

List of Contributing Fellows

Adedeji Ajani Adekunle Falola Alice Ndung'u Carolyne Tarus Chinasa T. Okolo Clarisse Mideva Cynthia Chepkemoi David Gitonga Doreen Abiero Eric Muhia Faith Amatika Gilbert Ogolla Immaculate Were Jacqueline Simpson Joel Adefidipe Joshua Ogwu Kingsley Owadara Majiuzu Daniel Mose Marco Grieco Nancy Gacheru Nelson Otieno Ochieng Ogango Odette Bester Rebecca Asseh Rotimi Owolabi Stella Nalwoga Wangari Njaathi

About E4E

The E4E (Emerging Technology for Emerging Markets) is a think-tank focusing on evidence-based tech policy advocacy to action around emerging technologies for emerging markets.

Our goal is to aid stakeholders, key players, governments, and regulators in making and complying with informed policies and regulations. Often, policymakers and regulators need to understand these frontier technologies, aggravating the risk factor of complying and coping with knee-jerk policies stifling innovation.

Through our policy reports and other activities at E4E, we can enlighten, examine and engage regulators and the governed.

Website: https://et4em.org/