



Policy Brief

CURTAILING STATE EXTREMISM IN DATA GOVERNANCE

AFRICAN CONTEXT

Adedeji Adeniran, PhD, Sone Osakwe

SUMMARY

This brief examines the implications of emerging threats to good data governance in Africa, as it relates to restrictive data policies and abuse of state power. Based on our analysis of data regulations/policy documents, studies by industry experts, and consultative workshop with stakeholders, we identify three major examples of these threats - increased cases of government imposed restrictions on online freedoms, mass surveillance of citizens and data protectionism.

While the justification often given for these measures is national security, there are often other underlying motivations that negate the principles of an effective and transparent data governance strategy. The negative impacts of these emerging trends range from human/digital rights violations, huge economic losses, among others. To address this problem, a holistic and systems thinking approach is required, as there is a need to ensure adequate checks and balances for increased transparency, accountability and independent oversight.

● BACKGROUND

There is an increasing level of attention and growing conversations at the national, regional and global levels, around the imperative for a more effective set of rules and regulations to guide the use and sharing of online data and digital footprints of individuals, firms and governments. The rationale is that a framework of policies and strategies is essential to address the inherent risks emerging from the recent data revolution. Emerging threats range from abuse and misuse of technologies and new communication media, lack of accountability from digital platform firms at the core of the data ecosystem, national security concerns, cyber crime, and user privacy issues. Such policies are intended to make digital platform firms accountable for how data is collected and used to generate insights, stored, shared and protected in order to engender trust in the data ecosystem.

In recognizing the importance of data governance, a grave challenge lies in determining the most appropriate approach to adopt, bearing in mind that the goal is not to “over regulate” which could stifle innovation, nor abuse governmental powers on these issues. Several approaches and frameworks for data governance are emerging in this respect on the African continent. While multinational big digital technology corporations are usually viewed as the “bad players” in data governance discourse,

there are emerging threats emanating from government and state led institutions around the world, particularly in African countries, which often go against the tenets of good data governance.

For instance, cases of government imposed controls/restrictions on online freedom and mass surveillance of citizens are rising. Also, data protectionism through data localization laws and similar regulations are becoming commonplace in Africa. We discuss some of these threats below and the implications:

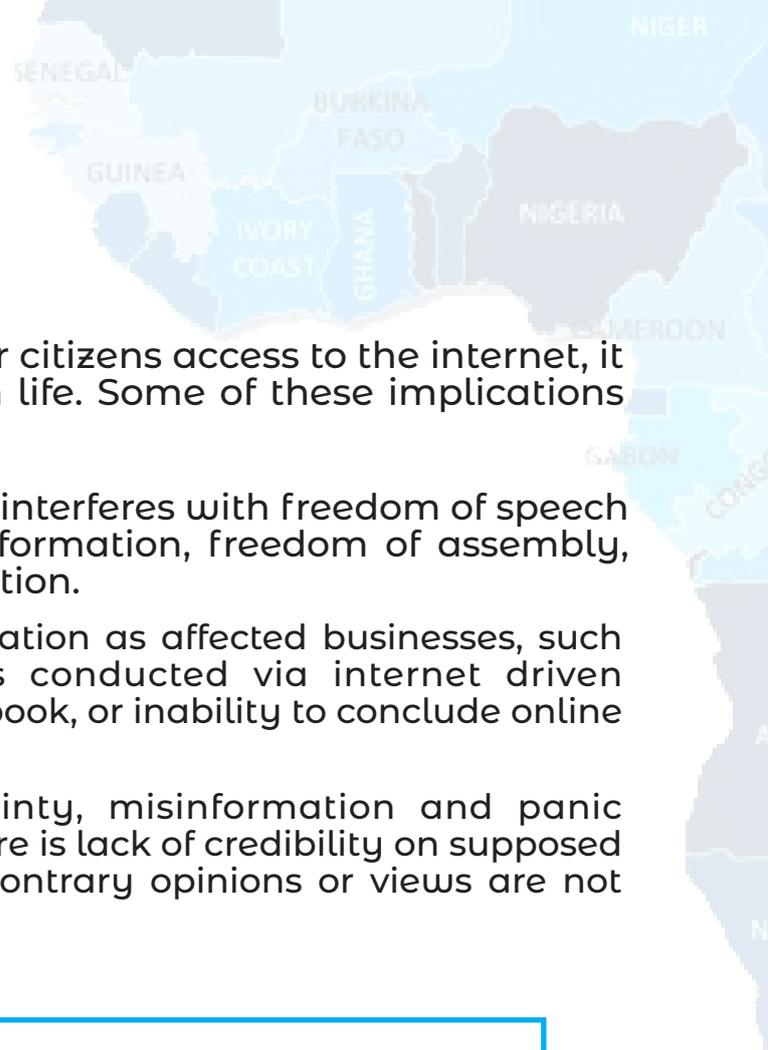


1 INTERNET BLACKOUTS AND SOCIAL MEDIA RESTRICTIONS

1.1 What is it and how is it unfolding in Africa?

This entails deliberate censoring and restriction of online media or information, in a bid to exert control. Internet shutdowns occur in different forms including completely cutting off citizens and organisations' access to the entire web within a jurisdiction, or partial shutdown of specific digital platforms. These often come as executive orders, through directives from a nation's telecommunications regulatory agency to internet service providers / telecommunications companies, mandating them to limit network connectivity or restrict users' access to specific websites or web based applications. Governments are able to exert such control since they are often responsible for granting licensing rights to these companies, and as such, can threaten licensees with hefty fines or revoke their licence. For some other countries, the entire or part of the internet infrastructure is routed through state owned operators, so shutdowns are even easier in this instance.

The justification often given for this trend of internet shutdowns, is to protect national security or check the spread of misinformation. It is mostly deployed during electioneering periods and when there is civil unrest.



1.2: Negative impact

When governments deny their citizens access to the internet, it disrupts all aspects of human life. Some of these implications include:

- Human rights violations as it interferes with freedom of speech and expression, access to information, freedom of assembly, freedom of political participation.
- Loss of livelihoods and deprivation as affected businesses, such as micro business activities conducted via internet driven platforms, WhatsApp or Facebook, or inability to conclude online transactions among others.
- Increased levels of uncertainty, misinformation and panic among the populace. Also there is lack of credibility on supposed democratic elections where contrary opinions or views are not permitted.

The estimated economic loss is significant at around \$3.3billion loss in the past three years.

Figure 1: Infringement of internet freedoms and accompanying costs

Country	Total Cost (\$Million)	Shutdown Duration (Hrs)
Sudan	1,935.10	1,599
Nigeria	646.2	2,928
Algeria	209.4	76
Ethiopia	208.8	8,562
Chad	149.9	9,366
DRC	61.2	456
Uganda	51.4	692
Zimbabwe	34.5	144
Tanzania	27.5	432
Eswatini	16.4	216
Mauritania	13.8	264
Guinea	6.1	238
Egypt	3.8	24
Zambia	1.7	48
Republic of Congo	1.6	72
Bénin	1.1	21
Gabon	1.1	29
Eritrea	0.4	240
South Sudan	0.3	24
Burundi	0.2	24
Senegal	0.2	7
Somalia	0.2	31
Liberia	0.1	12
Togo	0.1	24
	3,371.1	25,529

Sources: [Cost of internet Shutdowns tracker](#)

* Note that associated costs vary depending on the nature of shut down. Also, the list excludes sub-national shut downs in certain instances which are also commonplace.

2 GOVERNMENT LED PRIVACY INVASION AND INCREASING USE OF SPYWARE

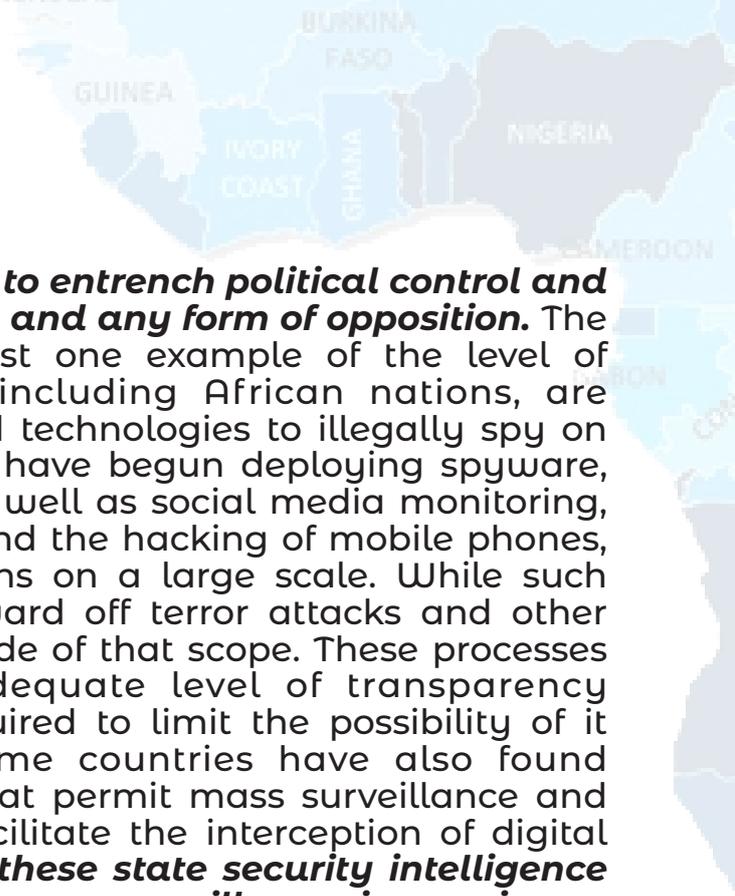
2.1 What does this entail?

The appetite for African governments to engage in mass instigated digital surveillance of citizens in the guise of intelligence gathering for national security purposes is gradually growing and becoming worrisome - refer to Figure 2.

Figure 2: Sightings of state abuse of digital surveillance



Sources: CIPES / African Arguments



Surveillance tools are being used to entrench political control and to spy on civil activists, dissidents and any form of opposition. The [Pegasus Project](#) revelations is just one example of the level of investments various countries, including African nations, are committing to enhanced tools and technologies to illegally spy on citizens. Some countries in Africa have begun deploying spyware, drones, and video surveillance, as well as social media monitoring, mobile phone location tracking, and the hacking of mobile phones, messaging, and email applications on a large scale. While such actions might be necessary to ward off terror attacks and other ills, it is also being deployed outside of that scope. These processes are sanctioned without the adequate level of transparency accountability and oversight required to limit the possibility of it being abused or corrupted. Some countries have also found loopholes in the legal systems that permit mass surveillance and mandate telecom providers to facilitate the interception of digital communication. ***The activities of these state security intelligence agencies that are involved in mass surveillance is worrisome because of the level of secrecy and lack of transparency, which begs to question if there any avenues for the citizens they serve to hold them accountable for actions taken, or an unbiased mechanism whereby those who have been victimised by surveillance may seek redress.***

The activities of these state security intelligence agencies that are involved in mass surveillance is worrisome because of the level of secrecy and lack of transparency, which begs to question if there any avenues for the citizens they serve to hold them accountable for actions taken

2.2: Why is it a problem?

- Indiscriminate monitoring of citizens, mass interception, hacking and interference with citizens' digital communication is at tangent with democratic values.
- It is a clear breach of citizens' human rights to privacy and expression. Also, it threatens digital rights in Africa, and weakens civilsociety's engagement in democratic processes. Diminishes appetite for participation in democratic processes. Activists, government critics and journalists become fearful and less expressive of their opinions on political affairs.
- Such actions create major power imbalances. It obstructs the separation of powers, as the executive branch is able to carry on without sufficient oversight from the legislature and judiciary.



3 DATA PROTECTIONISM

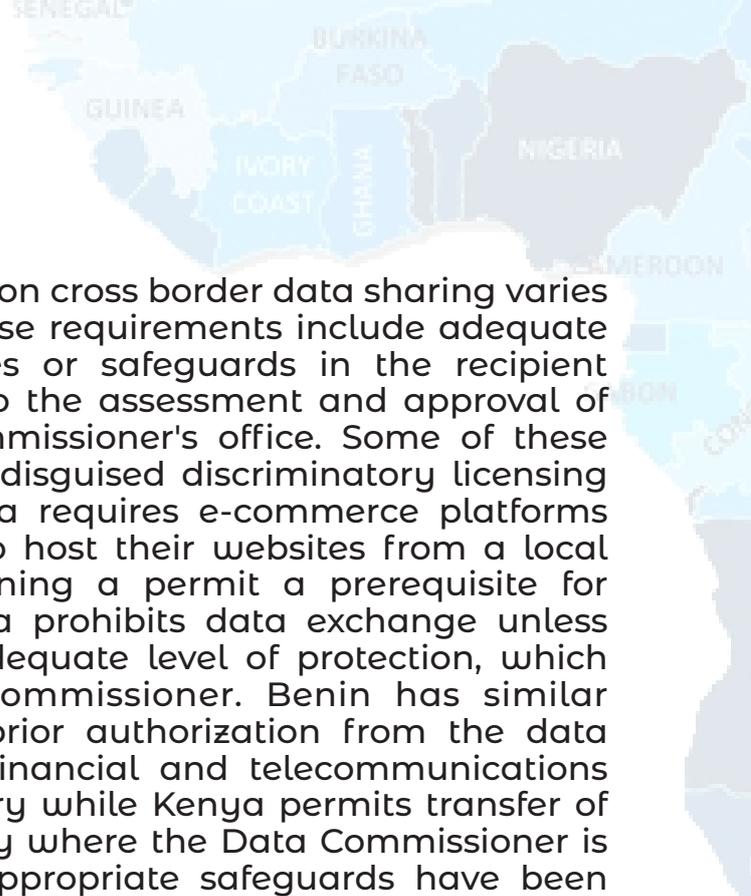
3.1 What does this entail?

Data protectionism is subject to varied interpretations, with no universal consensus of what it entails. However, we align our thoughts with UNCTAD which describes data protectionism as the regulation of data flows by governments, with the intention of creating competitive benefits for the domestic sector and adversely affecting the level playing field for foreign players. African governments have sought to enact regulations that force foreign technology companies to store and process locally generated data on domestic servers or data centres physically located within the borders of national jurisdictions, as well as limit their ability to transfer such data overseas.

Figure 3: Examples of African countries that have adopted direct and indirect stringent conditions on cross border data flows



Source: 'CSEAS DATA PLATFORM / DLA PIPER



The degree of restrictions or conditions on cross border data sharing varies by country. But broadly speaking, these requirements include adequate assurance of equivalent data policies or safeguards in the recipient country which is oftentimes subject to the assessment and approval of the data protection authority or commissioner's office. Some of these provisions also introduce stringent or disguised discriminatory licensing and certification. For instance, Algeria requires e-commerce platforms conducting business in the country to host their websites from a local data centre. Egypt has made obtaining a permit a prerequisite for cross-border data transfers. Botswana prohibits data exchange unless that recipient country provides an adequate level of protection, which will be determined by the Data Commissioner. Benin has similar provisions, in addition to obtaining prior authorization from the data protection authority. In Nigeria, all financial and telecommunications data must be hosted inside the country while Kenya permits transfer of personal data outside the country only where the Data Commissioner is provided with sufficient proof that appropriate safeguards have been implemented.

While the common reason given for having these provisions is to guarantee data privacy and national security, there is often an economic undertone/motivation. Due to the enormous economic value of data, access and control over data can influence competitive advantage, especially as the intersections between digital trade and data exchange deepens. Considering that Africa as a continent is a late entrant into the data driven global digital economy, some of these data localisation laws are targeted at boosting the local economy by pushing foreign companies to invest in or patronise local data centres and cloud solutions providers, in order to help the domestic ICT sector and create job opportunities. However, Africa could be the biggest loser if every country similarly introduced stringent data exchange policies, with lower innovation, higher trade and communication barriers and more transaction costs in the digital space. ***Irrespective of the justification for data protectionism, it is important to fit within the multilateral framework to prevent tits-for-tats and other deleterious effects.***

Irrespective of the justification for data protectionism, it is important to fit within the multilateral framework to prevent tits-for-tats and other deleterious effects.



3.2 Counterproductive implications

There are legitimate reasons for advocating that developing nations should be given leeway to enact protectionist-based digital strategies. However:

- There is a risk that these policies can have an adverse effect since multinational companies might find it increasingly difficult and costly to operate in jurisdictions with restrictive data sharing laws, thus making it unattractive to do business in such markets altogether.
- Complying with restrictive data obligations can also raise the costs of entry and operation for regional firms, especially smaller firms, which can be a hindrance to the African Union's regional integration initiatives.
- In addition, it could unintentionally restrict the creative abilities and competitiveness of local firms because of the “temporary and artificial” support systems available to them.
- Local firms might also be restricted from accessing online data not available domestically, as other countries might adopt retaliatory restrictions. Thus, adversely impacting the productivity of local firms.
- Customers are only able to access limited choices and in some cases more expensive products/services.
- Data protectionism undermines the potential for addressing data threats through international collaboration on data governance issues.

It is difficult to estimate the resultant annual costs or losses from data protectionist laws in the African region, however, ***studies suggest significant negative outcomes and economic losses where data protectionism exists.***

studies suggest significant negative outcomes and economic losses where data protectionism exists.



Ways to Cut Down Extremes in Data Governance

Data governance is much needed, but needs to be done right. Seeing that different government agencies are culpable, **addressing the problem of extreme or restrictive data policies should involve a holistic and systems thinking approach.** Policy makers need to aim for more-nuanced solutions in finding a balance. These include:

- 1 Built in check and balances for transparency and accountability:** No singular arm of government or stakeholder group should have absolute power on how the data ecosystem is run. Multi-stakeholder involvement of the private sector, civil society and different government agencies should jointly be in charge. Judicial review and legislative input can be useful in checking arbitrariness and excesses of the executive. There is also a need to close the legal loopholes that governments exploit in abusing surveillance systems. Also, in the rare event that extreme state interventions are genuinely required, there should be independent oversight mechanisms to review the practises adopted, to ensure that there is strict adherence to human rights provisions. Those involved in such oversight roles or judicial systems need to also have requisite competence and understanding of the issues
- 2 Raise public awareness and participation:** An effective data governance strategy must ensure that citizens and all stakeholders are fully aware and involved in data privacy and digital rights policies. There also needs to be deliberate avenues for the public to be empowered with necessary knowledge and capacity to challenge incidents of unconstitutional use of state surveillance on citizens.
- 3 Review the design of data governance strategies:** Costs that are ultimately imposed by data governance policies should be weighed against any corresponding benefits that such requirements are used to support. The assessment of whether it is proportionate to the risks presented, ought to take into account several factors, such as the extent to which it is demonstrated that data localisation measures effectively achieves the goals for which it was introduced, and whether there are any less restrictive alternative measures that could be enacted. Also, focus needs to shift from where data resides to a focus on real accountability.

addressing the problem of extreme or restrictive data policies should involve a holistic and systems thinking approach.

- 
- 4 **Integrate data governance as part of the broader good governance campaign:** Good governance practises need to be created in the region, to stem the trend in overall bad governance. Here we hope for reversed Greham's Law in that good practises would drive out bad practises. This will only work if the data governance framework delivers economic and social benefits and freedom for citizens.
 - 5 **Greater collaboration at regional and global level:** Establish a threshold or standard for data rights and state communications surveillance which member countries cannot go below. For instance, such rules can include provisions that ensure that surveillance is only used on potential perpetrators based on verifiable evidence, as opposed to political opposition. Further, since decisions taken by antitrust authorities in one jurisdiction have spillover effects in many others there is scope for closer cooperation among these authorities. Certain policy issues, particularly international rules governing cross-border data flows need to be tackled through multilateral cooperation.