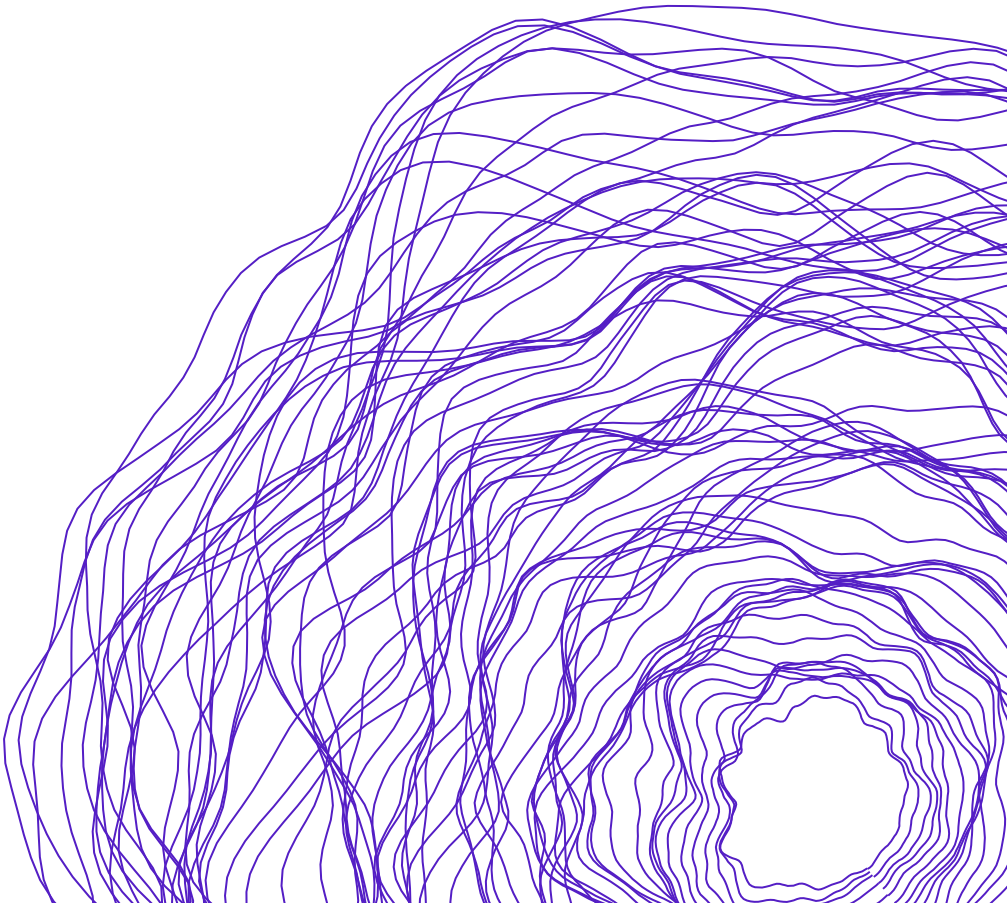
adapt

Data Practices and Protections in the Smartphone Era: Emerging Issues in Nigeria and Kenya

Seyram Avle



adapt

Internews

About

This report synthesizes research on data practices in Nigeria and Kenya to provide an overview of emerging issues in the increased datafication in Africa, primarily through increased access to digital technologies.

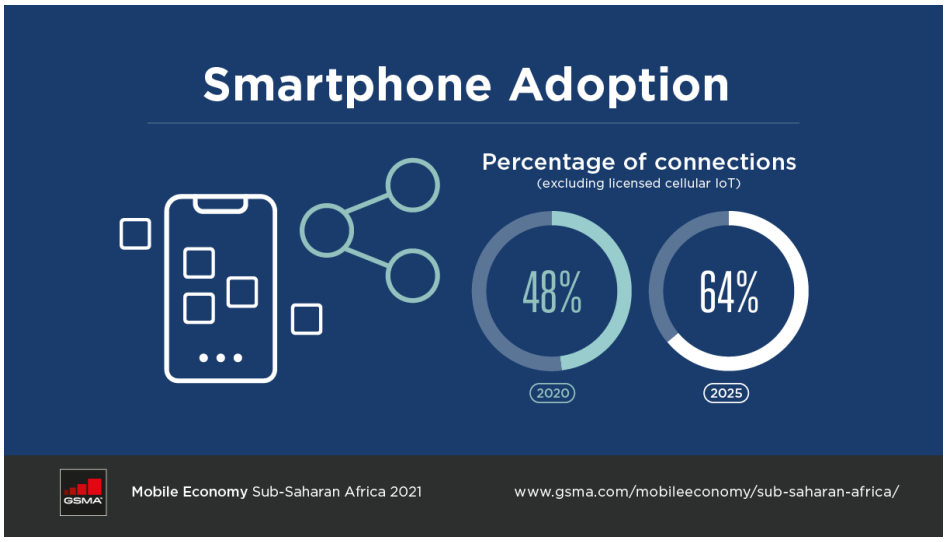
Acknowledgements

Thank you to Neo Nyoni (Northeastern University) for her work as a research assistant, Khadijah El-Usman (Paradigm Initiative, Nigeria), Grace Githaiga (KICTANet, Kenya), Meshak Masibo (KICTANet, Kenya) for legal research and expertise, Internews staffers Laura Schwartz-Henderson, Benjamin Whitehead, Skyler Sallick, and the experts and users interviewed in Nigeria and Kenya.

Overview

Digital access has been on the rise in Africa over the last decade, enabled by low-cost smartphones and lowering costs of data. According to ITU estimates, about 33% of Africa's population used the internet in 2021. Between 2019 and 2021 alone, internet use on the continent jumped by 23 percent. 40% of African youth use the internet compared with 27% of the rest of the population.[1] Moreover, one half of urban dwellers are online compared with 15 percent of those in rural areas. [2] In terms of mobile coverage, about 49% of Africa is covered by 4G, 33% by 3G and 7% by 2G. The increased use of smartphones, owing largely to their increased affordability, is often seen through the prism of increasing access to the internet for the majority world. While access is important for many reasons, it also comes with practices of technological surveillance and data extraction endemic to the global digital economy.

Whether it is health data, education, online browsing habits, smartphone location, or any of the myriad data points that are now routinely collected across industries and practices, personal data can reveal intimate details about a users' body, their thoughts, and attitudes, who their loved ones are, etc. Access to such information poses a risk for all users, given how they can be used for targeting different populations. This is especially true for vulnerable populations, who might include marginalized groups, activists, journalists, etc. African governments and regulatory bodies' focus on access only may have created a blind spot in which African citizens and consumers are left vulnerable to egregious extractive practices that arguably pose higher risks.



This report, commissioned by Internews Network, stems from the premise that understanding the kinds of data collected about users, how they are collected, used, and to what effect, is a necessary precursor to safeguarding people's right to privacy, a

[1] Youth are 15-24 year olds, rest means below 15 and above 24 according to the ITU (2021).
[2] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

notion that is enshrined in the constitutions of over 160 states around the world including Nigeria and Kenya.

The questions underlying this project are:

1) What are the established and emerging norms around datafication in everyday digital and electronic devices in low- and middle-income countries in Africa?
2) What data protections are being enacted through law and how do they stack up against the norms and practices in question 1?
3) What actions need to be taken to improve citizen and consumer protections where there are mismatches between law and market practices?

Methods

The research maps and analyzes a range of products, devices, and activities that generate and extract data from users on behalf of both state and non-state (commercial) actors. Specifically, findings are drawn from artifact analyses of some of the most popular smartphones used in Nigeria and Kenya, alongside a desk study of smartphone uses, as documented by media and news reports, as well as a literature review of regulatory documents and civil society reports, supplemented by expert and user interviews. These were put in conversation with an analysis of the data protections available to consumers, allowing for some reflections on the gaps between legal protections and existing data infrastructures and practices. Such a multi-faceted qualitative approach aims to provide nuance and specificity to how stakeholders might understand the gaps between data practices and protections in Africa. This summary report is accompanied by a Methods Guide that details how this was done with pointers on how others might replicate the research in other geopolitical contexts.

Nigeria

For Nigeria, the research found that the fundamental business model of harvesting troves of consumer data appears to have taken new turns, with highly motivated actors taking advantage of the size of the population, increasing internet access, lower smartphone costs, as well as a lax and somewhat confusing regulatory environment. More specifically, we found that:

a) the constellations of hardware and software in consumer hands fragments consumer data transnationally across several geographies;
b) hardware are important vessels for the experimentation of artificial intelligence, facial recognition, and other emerging areas of technology, largely by foreign transnational entities;

c) fintech presents a particularly potent point of vulnerability in part due to high demand for financial access and lack of regulatory attention to digital applications; and,

d) the federal government of Nigeria employs what could be best described as a 'whack-a-mole' mode of regulation -- generating ad hoc guidelines and frameworks to quell bad behavior that rear their head in different sectors – rather than a unified data protection focused approach.

In general, findings show that the regulatory environment is as fragmented as the data practices engendered by the increased uptake of smartphones and devices. Read the full report here.

Kenya

Since 2019, the Government of Kenya (GoK) has initiated several digitization projects that aim, among other things, to improve governance and boost the economy. As the Covid-19 pandemic wore on, new forms of data collection took hold and more surveillant practices were implemented, according to Kenyan civil society groups who have been vigilant about these changes. We examined key aspects of the prior work done by such civil society groups, vis-à-vis the workings of the Data Protection Act (DPA) and put them in conversation with an analysis of data practices by the state and the commercial sector. Together, these provided a landscape of how data is generated from Kenyans in their everyday encounters with the state and uses of digital technologies, and crucially, what protections are available to them. Key findings include:

a) the state is a crucial data processor, sometimes in breach of its own law on data protection, a reality that fosters a lack of trust.

b) institutions set up to implement the data protection law are underfunded, understaffed, and vulnerable to political intrusions.

c) foreign actors have an outsized role in the extraction of Kenyan data, leading some to characterize the situation as data colonialism.

d) the technical knowledge base underpinning the implementation of data privacy, e.g., developers, have been left out of the discussion, creating a significant implementation gap.

e) there is a strong lack of awareness among the Kenyan population about the data protection law and the institutions charged with enforcing it.

Read the full report here.

Recommendations

Recommendations for data activists, legal practitioners, etc. in Nigeria and Kenya (and elsewhere in Africa) in their fight for data protections and a safe digital environment for all include advocating for a more networked view of data protection; specifically, incorporating technological changes into data protection regulation that may help anticipate problematic data practices.

- By bringing the lessons of data protection learned elsewhere into conversation with everyday uses and practices, African government and data protection activists may be able to get ahead of potential abuses of data down the line.
- We also recommend a more open and transparent data protection environment in these African countries. Specifically, we recommend governments work to foster public trust in how they handle citizen data by being more transparent, less data hungry, and more security conscious in safeguarding any data collected, particularly in terms of encryption, domestic storage, etc.
- We support recommendations by civil society groups to strengthen the independence of the Office of the Data Protection Commissioner by separating staff appointments from political office and providing a robust funding mechanism that will be sustainable long term. In addition, we suggest that such commissions employ a mix of "sticks and carrots" in nudging commercial actors towards greater accountability and compliance. For instance, it might include positively reinforcing and rewarding good data behavior in addition to punishing bad behavior through random data audits and higher fines/penalties.

Finally, the broader challenge of global big tech and foreign extraction of African data needs to be taken seriously and urgently, with a first move being adding a more forceful (and implementable) amendment to data protection laws on how foreign entities access and use Africans' data. This might include ensuring that data is stored locally and providing a mechanism through which this can be enforced. However, given the tendency towards abuse of state power, there needs to be equally forceful rule making on upholding citizen rights to privacy even beyond the reach of the state. This might come through several avenues, including the judiciary and activism/advocacy by civil society and consumer rights groups. Governance of data privacy and data protections more broadly will most benefit from multistakeholder engagement.