adapt

Data Practices & Protections in Nigeria

Seyram Avle

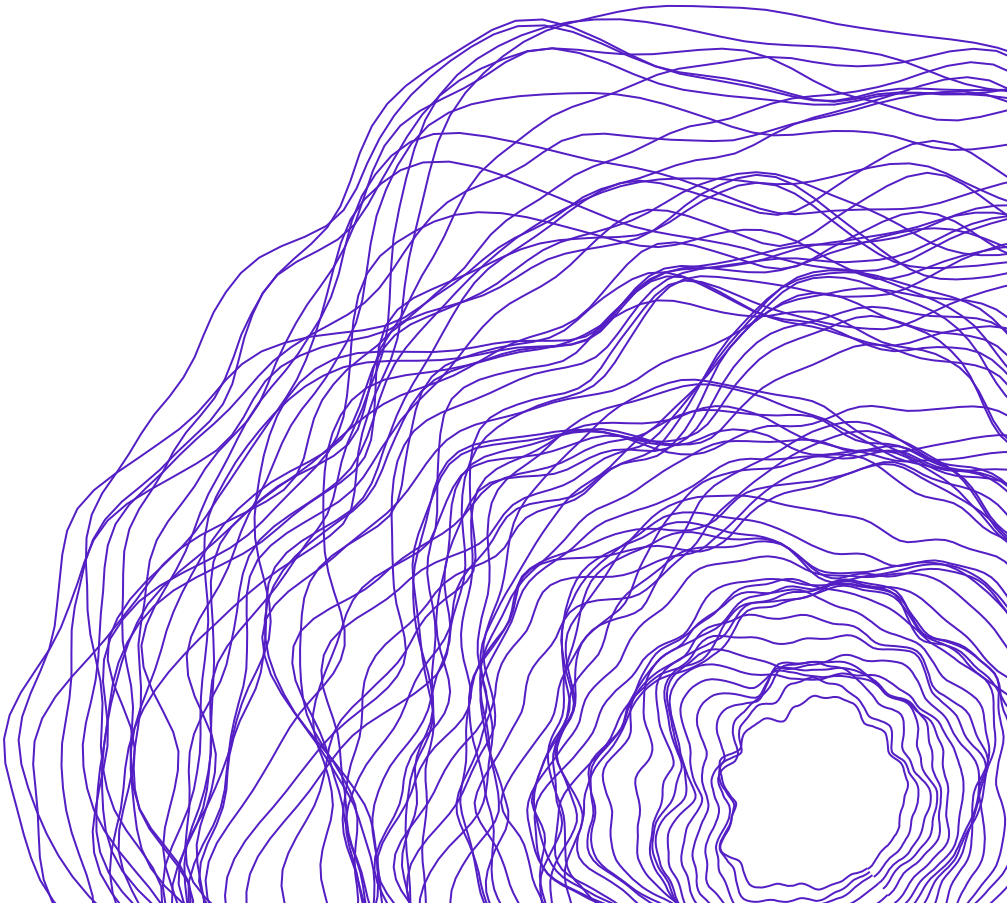

Table of Contents

List of Abbreviations

BVN – Biometric Verification Number

CBN – Central Bank of Nigeria

GDP – Gross Domestic Product

GDPR – General Data Protection Regulation

GPS – Global Positioning System

GSMA – Global System for Mobile Communications (GSM) Association

IMEI – international Mobile Equipment Identity

ITU – International Telecommunications Union

KYP – Know Your Customer

MCDE – Ministry of Communications and Digital Economy

MMO - Mobile Money Operators

MoMo – Mobile Money

NCC - Nigerian Communication Commission

NDPR – Nigeria Data Protection Regulation

NIBSS - Nigerian Inter-Bank System

NIMC -- National Identification Management Commission

NITDA – National Information Technology Development Agency

PIPL – Personal Information Protection Law

PSB – Payment Service Bank

USSD – Unstructured Supplementary Service Data

VAS – Value Added Services

List of Figures and Tables

adapt

Executive Summary

Digital access has been on the rise in Africa over the last decade, enabled by low-cost smartphones and lowering costs of data. With this access comes 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.

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 notion that is enshrined in the constitutes of over 160 states around the world including Nigeria. The report maps and analyzes the range of products, devices, and activities that generate and extract data from users in Nigeria on behalf of non-state (commercial) actors. This is put in conversation with an analysis of the data protections available to Nigerian consumers, allowing for some reflections on the gaps between legal protections and existing data infrastructures and practices. The findings presented are drawn from artifact analyses of some of the most popular smartphones used in Nigeria, alongside a desk study of smartphone uses, as documented by media and news reports from Nigeria, as well as a review of regulatory documents, supplemented by expert interviews.

The report shows that the fundamental business model of harvesting troves of consumer data appears to have taken new turns in places like Nigeria, 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, it shows that 1) the constellations of hardware and software in consumer hands fragments consumer data transnationally across several geographies; 2) hardware are important vessels for the experimentation of artificial intelligence, facial recognition, and other emerging areas of technology, largely by foreign transnational entities; 3) 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, 4) 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.

Recommendations for data activists, legal practitioners, etc. in Nigeria (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 in Nigeria, the Nigerian government and data protection activists may be able to get ahead of potential abuses of data down the line.

Introduction

Nigeria is Africa's largest nation, in terms of both population (~200 million) and GDP (USD 448 billion)[1] ~62% of the population have internet access and 98% of the adult population have a cell phone.[2] The GSM Association (GSMA) anticipates that by 2025, Nigeria will add 32 million new mobile subscribers (see figure 1 below) and estimates smartphone adoption to be at 38%.[3] These factors make the country a desirable market in a global digital economy in which scale (or number of users) matters. As the world becomes increasingly data intensive, a user's every move is a data point that could be monetized, making surveillance and data extraction the norm in the digital economy. Described as surveillance capitalism, data colonialism, etc.[4],[5],[6],[7] this model of harvesting consumer data across territories has encountered regulatory attempts at limiting rampant data extraction and giving individuals the power to control what data is collected about them, when it is being collected, and to what ends.[8] This report explores the data norms and practices in 'everyday' digital uses in Nigeria., as well as the regulatory environment around safeguarding different uses of data. It attempts to map and analyze the range of products, devices, and activities that generate and extract data from users in the country on behalf of non-state (commercial) actors. This is put in conversation with an analysis of the data protections available to Nigerian consumers, allowing for some reflections on the gaps between legal protections and existing data infrastructures and practices.

[1] Prahalad, C. K. (2006). *The Fortune at the Bottom of the Pyramid*. Pearson Education India.

[2] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

[3] GSM Association (2019). The mobile economy: West Africa 2019. https://www.gsma.com/mobileeconomy/west-africa/ Accessed June 10, 2022.

[4] Birch, K. (2020). Technoscience rent: Toward a theory of rentiership for technoscientific capitalism. Science, Technology, & Human Values, 45(1), 3-33.

[5] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency.

[6] Ogunmokun, T. (2022). Assessing data protection in Nigeria: A look at biometric identity, surveillance, encryption and anonymity, and cybercrimes. Tech Hive/Omidyar Network/Paradigm Initiative, Nigeria.

[7] Suarez-Villa, L. (2001). The rise of technocapitalism. *Science & Technology Studies, 14*(2), 4-20.

[8] Two regulatory attempts that have received academic and media attention are the European Union (EU's) General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL). The former is seen as a model for the latter, although they operate under different political and regulatory environments. The GDPR also shares a framework with some African data protection regulations, including Ghana and Kenya's.

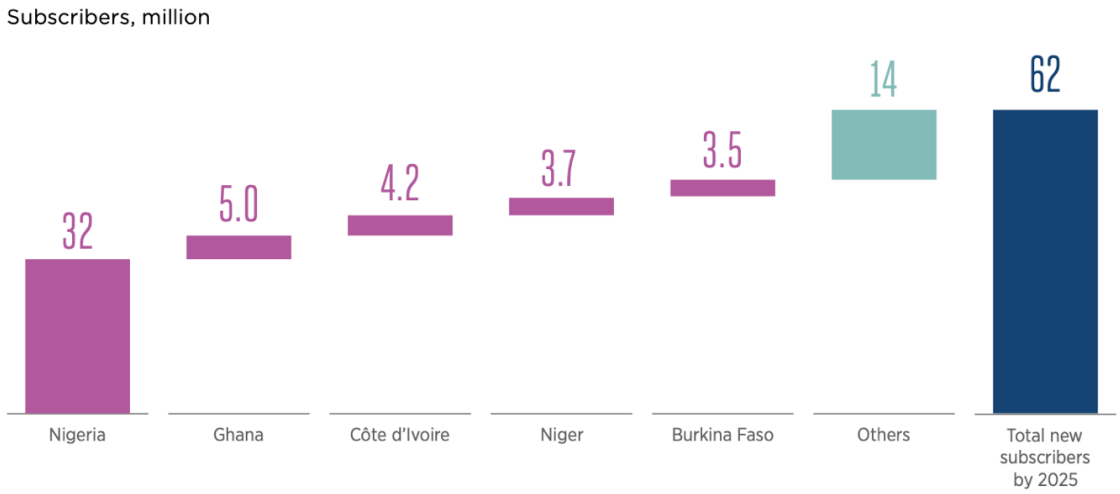

Figure 1: Anticipated new mobile subscribers in West Africa[9]

Both domestic and foreign entities provide products and services to Nigerians across finance, health, agriculture, etc. Many of these, as we will show, treat Nigeria as a lawless frontier in which various experiments are enacted to see what sticks, while borrowing established tactics from elsewhere. Borders and boundaries appear irrelevant to tech companies, and "it is becoming increasingly difficult to hold them to account within nation-states."[10] Nigeria issued a data protection regulation (NDPR) in 2019. It, however, operates alongside a long-standing array of laws with overlapping aims, leading to a somewhat confusing and fragmented implementation environment. Many of the existing and overlapping regulations around data practices stem from what might be characterized as a 'whack-a-mole' approach in which ad hoc guidelines and frameworks materialize to quell bad behaviors that rear their head in different sectors.

This report takes the view that a more networked view of data protections, i.e., seeing regulatory action as linked to real lived data practices, is of paramount importance if the digital economy is to be made safe, inclusive, and beneficial for all Nigerians. By understanding where and how citizen data is generated, regulators can get a better understanding of and be better positioned to anticipate areas of data extraction and proactively prevent the harms that come from abuse of user data. At the very least, this networked understanding highlights which actors are worth keeping an eye on and help provide comprehensive scopes of challenges before any remedies are put in place. Thus, this report aims to make visible interconnections between different sectors by mapping the software, hardware, and user practices of some of the most popular smartphones in Nigeria, along with an analysis of the various 'data protection adjacent' regulations to find the key gaps between practices and protections.

[9] GSMA Intelligence 2019 [GSM Association (2019). The mobile economy: West Africa 2019. https://www.gsma.com/mobileeconomy/west-africa/ Accessed June 10, 2022. p.7]
[10] Avle, S., & Fox, S. (2021). Tech labor: A new interactions forum. interactions, XXIX (July/Aug 2021).

To do this, we combined a desk study of dominant data practices and regulatory frameworks in Nigeria with artifact analysis of some commonly used smartphones in Nigeria, supplemented by expert interviews. As part of the desk study, we examined both academic text and media articles both on key practices observed by the author and some of the experts interviewed, covering both industry and government activity. This includes reviewing the ways that industry actors market and communicate with users, what consumers have posted online about particular practices, and what regulatory documents exist for the public. The artifacts analyzed include some of the best-selling Transsion smartphones (Tecno, Infinix, itel) given their dominance in the Nigerian market, as well as others by Samsung and Xiaomi. This analysis includes making sense of the affordances of the devices, user experiences, as well as careful reviews of terms of use, privacy notifications, etc. Understanding what the user is presented with gives a good sense of what is obfuscated in marketing, and how those impact user expectations and whether their consent to data extraction might be considered meaningful. Below, we present first, the data practices engendered by the increased access to mobile phones, particularly smart phones, with a special section on fintech, and then provide some overview of data protections that currently exist in Nigeria. We then present the key gaps between the two and offer some recommendations based on these findings.

Data Practices

Whether it is health data, education, online browsing habits, smartphone location or the myriad data points that are now routinely collected across industries and practices, personal data can reveal intimate details about a users' body, thoughts and attitudes, their loved ones, their daily routines, etc. Digital data creates 'data doubles' and leaves traces of lives in ways that are highly personal and can be used in various ways, and impact life both positively and negatively.[11],[12] Access to such information, authorized or not by the user, poses several risks that can be especially dangerous for children, marginalized identities, activists, and other vulnerable populations. It is therefore important to understand how data is collected and used, by whom, *and* what consumers understand of that process for any kind of data protection to be meaningful applied.

In this section, we present some of the ways that various data are collected from Nigerian citizens and consumers through mobile phones. We map out the range of commercial actors and consumer technologies that are present in the everyday of Nigerians, focusing on the hardware and software on smartphones largely because of the significant role they play in the increased access that Nigerians have to the internet, functioning, as it were as a gateway to the constant data surveillance that underlies the

[11] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency.

[12] GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022.

digital economy today. We contextualize that with what consumers know before they give consent, where consent is sought or even implied. State actors also sometimes unintentionally create opportunities for the exploitation of citizens and users, through (in)action in other sectors. We show how this combination of state in(action) combines with common user needs and digital issues in the finance sector, can produce a series of egregious practices that puts consumers in a vulnerable position.

Mapping Commercial Actors and Consumer Technologies

An increasing number of users around the global south access the web primarily via their phones and through that, are open to a staggering range of applications and services that almost universally operate on surveillance logics, with or without informed or meaningful consent. The uptick in global south users is in part due to 1) access to low-cost smartphones almost primarily Chinese smartphone makers, specifically from the Shenzhen hardware ecosystem that drives the global production of smart hardware[13],[14],[15] and 2) increased connectivity of 3G and 4G across regions. Sub-Saharan Africa has the widest coverage and usage gaps in mobile connectivity globally although these gaps are reducing steadily.[16] This region also has the highest percentage of basic or feature phone connections (about 45%) and a significant share of smartphones support 3G only, according to the same GSMA report. This is in part due to the significant cost/affordability barrier -- the poorest 20% of individuals expect to spend more than 100% of their monthly income on an entry-level internet enabled handset and 15% of their monthly income on a data plan. Similarly, the ITU finds that the cost of connectivity is highest in Africa.[17]

This cost barrier is not negligible. Research on Transsion, the company behind the best-selling phones on the continent shows that such constraints inform design decisions; for instance, designing the size and capacity of a batteries based on limited electricity as well as memory and space constraints to keep the lowest-cost phones (branded as itel on the market) at an affordable rate for the poorest segment of the market.[18] 'Smart-feature' phones do not have all the capabilities of smart phones, but they still allow for

[13] Lindtner, S., Greenspan, A., & Li, D. (2015). Designed in Shenzhen: Shanzhai manufacturing and maker entrepreneurs. Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives, Aarhus, Denmark.
[14] Lu, M. (2020). Designed for the bottom of the pyramid: a case study of a Chinese phone brand in Africa. *Chinese Journal of Communication*, 1-16.
[15] National Assembly of the Federal Republic of Nigeria (2020). Data Protection Bill. https://www.ncc.gov.ng/accessible/documents/911-data-protection-bill-draft-2020/file Accessed May 19, 2022.
[16] GSM Association (2021). The mobile economy: Sub-Saharan Africa 2021. https://www.gsma.com/mobileeconomy/sub-saharan-africa/ Accessed June 10, 2022.
[17] International Telecommunications Union (ITU) (2021). Measuring digital development. Facts and figures. ITU Development Sector. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf Accessed June 10, 2022.
[18] Lu, M. (2020). Designed for the bottom of the pyramid: a case study of a Chinese phone brand in Africa. *Chinese Journal of Communication*, 1-16.

a range of applications to be installed and can provide better browsing experiences than basic-feature phones. In 2020, such phones cost about $28 USD bringing digital connectivity within reach of much of Africa's poorer population, even if it comes at relatively significant personal cost to them. Phone makers such as Transsion and other Chinese manufacturers that target the 'bottom of the pyramid'[19] are therefore crucial links in how users access the internet and by extension, the data infrastructures embedded therein. In this section therefore, we review the hardware and software features of the dominant market player, Transsion, to illustrate how smartphones and smart enabled devices act as access points for data surveillance. We separate hardware from software to more clearly articulate where the risks for data extraction and exploitation emerge from.

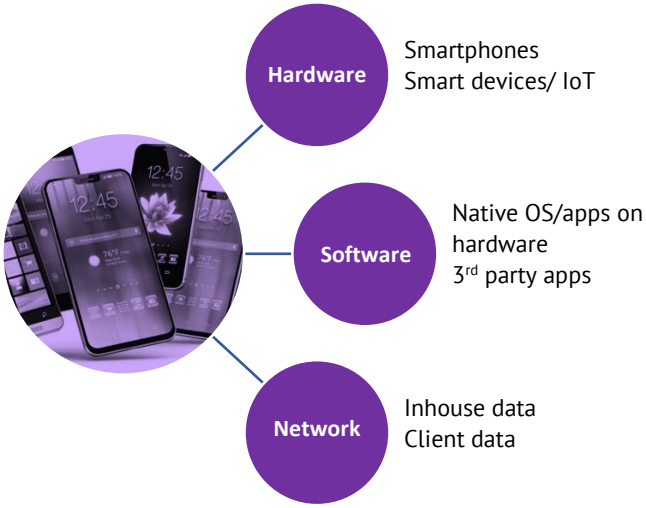

Figure 2: Key actors in consumer technology

Smartphone hardware, artificial intelligence, and facial recognition

Smartphone hardware is predominantly foreign made in the Nigerian market, a fact that is also true for most countries the world over. Global electronics supply chains are complex, but they frequently lead to the south of China, particularly the Shenzhen area in Guangdong province. The Chinese firm, Transsion, which originated from Shenzhen, is the market leader for smartphones in Nigeria (and the rest of Africa) primarily because of the mix of affordability and value for money. Transsion's phone brands Tecno, Infinix, and itel[20] run the gamut in cost and thus cater to a wide range of consumers, competing with other Chinese makers such as Huawei, Oppo, Xiaomi, Vivo, and Gionee, as well as Samsung (Korea), Apple (USA), Nokia (Finland), and HTC (Taiwan). There are a handful of domestic Nigerian brands that our research revealed primarily focus on providing

[19] O'Donnell, M. A., Wong, W., & Bach, J. (2017). *Learning from Shenzhen: China's Post-Mao Experiment from Special Zone to Model City*. University of Chicago Press.
[20] The itel brand is mainly basic and smart feature phones (enhanced feature phones that are not quite as sophisticated as other smartphones).

affordable tablets (e.g., Bryet Gadgets, Imose, and Pliris1) although some make phones as well (e.g., RLG and Obi).

Smartphone cameras in the last three years have been labeled 'AI triple' or 'AI quad' with some evidence of a patent war between the various Chinese makers brewing.[21] AI cameras are used to identify objects, are built into 'auto modes', and continually blur the lines between image capture, enhancement, and manipulation.[22] Most AI applications have been available commercially for years now and are used daily in everyday communication such as Facebook's photo tagging. Transsion cameras are optimized for dark skin tones, making them desirable in Africa and giving Tecno, Infinix, and itel an edge on a continent with a predominantly youthful population that is also active on social media. The promotion of their cameras as 'being able to capture the beauty of Blackness' is rightfully appealing to a population that is notoriously left of out tech design imaginaries. On the one hand, this narrative falls within the argument for further inclusion of Black people into facial recognition and other next generation technologies, as examples from primarily western countries show that the lack of training data that includes diverse faces creates downstream problems in which people are wrongfully identified in law enforcement scenarios.[23],[24],[25] Counter arguments against greater inclusion argue that the cost of the 'exclusion overhead' of not having representative training datasets in facial recognition does not outweigh the surveillant and carceral uses of Black peoples' data.[26],[27],[28]

More broadly, the argument that the Chinese government might be exporting its surveillance style to Africa through large scale state projects (for instance in Zimbabwe) cannot be understood separately from the development of AI enabled cameras.[29] While it is difficult to prove that a company such as Transsion might be sharing its data and

[21] Lu, M., & Qiu, J. L. (2022). Empowerment or warfare? dark skin, AI camera, and Transsion's patent narratives. *Information, Communication & Society*, 1-17.
[22] Buolamwini, J. (2017, May 29, 2017). Algorithms aren't racist. Your skin is just too dark. *Hackernoon*. Carter, J., & Lawton, R. (2021). What is an AI camera? How AI is changing photography and photo editing. *Digital Camera World*. https://www.digitalcameraworld.com/features/what-is-an-ai-powered-camera. Accessed August 11, 2021.
[23] Buolamwini, J. (2017, May 29, 2017). Algorithms aren't racist. Your skin is just too dark. *Hackernoon.*
[24] Buolamwini, J. (2017, May 29, 2017). Algorithms aren't racist. Your skin is just too dark. *Hackernoon*. Carter, J., & Lawton, R. (2021). What is an AI camera? How AI is changing photography and photo editing. *Digital Camera World*. https://www.digitalcameraworld.com/features/what-is-an-ai-powered-camera. Accessed August 11, 2021.
[25] Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency.
[26] Browne, S. (2012). Race and Surveillance. In K. S. Ball, K. Haggerty, & D. Lyon (Eds.), Routledge Handbook of Surveillance Studies (pp. 72–79). Routledge.
[27] Browne, S. (2015). *Dark Matters: On the Surveillance of Blackness*. Duke University Press.
[28] Haggerty, K. D., & Ericson, R. V. (2017). The surveillant assemblage. *Surveillance, Crime and Social Control*, 61-78.
[29] Chutel, L. (2018). *China is exporting facial recognition software to Africa, expanding its vast database*. Quart. Retrieved 20 October 2020 from https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to- africa-ensuring-ai-dominance-through-diversity/

technology with the Chinese state, there is already evidence of others like Cloudwalk (which reportedly made the above referenced deal with the Zimbabwean government) that have been already been key instruments in the surveillance of populations in places like Xinjiang in China. This unknown aspect of what happens to the data outside of corporate servers is a point of concern, just as the amassing of private identity data more generally in the hands of transnational corporate entities ('big tech') should be of concern in African jurisdictions. The 'everyday' AI and facial recognition tools embedded on low-cost smartphones are becoming central to platformization, altogether yielding vast amounts of data flow between wide varieties of people, corporations, governments, and across borders.[30]

Operating Systems and Native Software

Most of the smartphone brands sold in Nigeria, except Apple, run on the Android operating system (OS). Android was built on Linux for touch screen phones and was acquired by Google in 2005. All brands tailor features to this underlying system, and the associated data policies operate both in tandem and separately from Google's. For instance, Transsion phones bundle their own digital products (e.g., Boomplay Music) along with Google and Facebook products on all their phones (particularly Facebook and WhatsApp), creating a user experience that requires, at a minimum, three different data policies, and most often, more if additional third-party apps are downloaded in the Google store (see figure 3 below). While the Android basis of most of the phones produced here forces Google products into the mobile phone marketplace, its openness means it makes for a flexible base from which companies can build on in multiple ways. Transsion phones, for instance, increasingly include privacy features, a distinct departure from previous years, yet the underlying practice of collecting volumes of consumer data continues despite this promise of privacy.

Together, these differing data policies fragment consumer data across multiple geographies outside Nigeria and these data are largely held by western and Asian 'big (and medium) tech'. Many products on these smartphones cannot be used without giving consent to access consumer files that may not be immediately related to the product or app being used. This opt-out default for digital devices continues, enabling transnational corporations like Apple to now carve a whole new marketing value on privacy options and opting-into sharing as a value add for using their devices. Some commentators argue that Apple's privacy practices harm advertising models in the app economy, locking out a whole industry that then cedes power to a global duopoly of Apple and Google.[31]

[30] Avle, S. [forthcoming] Chinese smartphones in Africa: Hardware and data in the platform era. Media, Culture, and Society.

[31] See, for instance, the opinions expressed in this Twitter thread by an industry insider: https://twitter.com/TheHolyKau/status/1533776598331101184?s=20&t=yNerEtncRM0smlqiYFSxWA

Transsion's apps come as default options on their devices, with some built by the parent company's many subsidiaries. For example, a rather intrusive news app called Scooper News is produced by Transbyte App, which also makes several apps called PostNow, X Player, PAB-Album Secure, Joga (Funny trends) and Meow – Sweety girl. Scooper News is described as "more than just news" and brings the "latest viral contents [sic] from Kenya, Nigeria, Egypt, Ghana, Africa and the World". On the Google Play store, the app promotes "news, funny videos and more with data-saving and offline reading feature … picks trending and breaking news for you, elaborately *[sic]*. It customizes your favorites according to your choices and interests." Across the top tier Tecno and Infinix phones that examined, this app's algorithms continually fetched news from questionable sources, apparently using virality as the core variable and ultimately serving up news and videos that contain verifiably false news and mis/dis information, with only the option to share.[32]

What is equally interesting is that this app is like the Google news widget embedded on recent android versions (most recently checked on android 11). Transsion, a smaller actor, but large within Africa, here can be viewed as mimicking the global industry giant, Google, although with some important differences. Some of Transsion's apps give users information on what sorts of data are being collected whereas Google's preinstalled ones do not. All of Google's products came pre-checked to allow access, forcing users to opt out, while some of Transsion's followed the 'opt-in' model. Lengthy terms and multiple steps mean that even users who wish to change pre-sets are discouraged. Most are forced to accept both Google and Transsion's data options out of convenience thereby not giving meaningful consent.

Finally, our research showed that some older smart and smart feature phones on the market were sold with outdated software. According to Privacy International which examined a Tecno Y2 phone in Uganda in 2021, older phones no longer produced by manufacturers but still in circulation pose serious security and privacy risks.[33] These risks include "lack of meaningful consent with pre-installed apps" where many apps "use the phone as a trojan horse" for data harvesting, crypto mining, etc., similar to those described by BuzzFeed for the tecno w2 in 2020.[34] Other issues uncovered were "irremovable bloatware", "outdated and insecure apps", all of which means compromised privacy. Outdated phones are cheaper on the market, therefore people on the lowest end of the economic ladder, already more vulnerable, have a higher risk of being unwillingly enrolled into data infrastructures and likely incur more cost struggling to keep the phones functioning.

[32] Avle, S. [forthcoming] Chinese smartphones in Africa: Hardware and data in the platform era. Media, Culture, and Society.

[33] See https://privacyinternational.org/long-read/4605/how-one-tecno-phone-putting-users-privacy-and-security-risk

[34] See https://www.buzzfeednews.com/article/craigsilverman/cheap-chinese-smartphones-malware

Third Party Applications

At time of writing, the top 10 free android apps in Nigeria were split between foreign (primarily American and Chinese) social media (TikTok, WhatsApp Messenger and Whatsapp Business, Facebook Lite, Snapchat) and both foreign and domestic mobile banking/microfinance apps: Umba Mobile (fully digital Irish owned bank), OKash (by BlueRidge microfinance), FairMoney (digital bank by a microfinance organization operating in Nigeria and India) and the Swedish owned Spotify music and podcast app (see figure 4 below).[35] These apps have varying degrees of protections and data requested, opt out defaults, etc. TikTok's popularity for instance is tied to its algorithms that curate content for users based on 'next generation' uses of facial recognition and artificial intelligence.

A common practice found across apps is to request access to users' address books, with varying explanations given based on what the app is for. For instance, True Caller which positions itself as a 'leading global call ID & call blocking app' collects the address book contents of all users to build what it euphemistically calls "a community-based spam list from over 300 miliion users". Through this database, users "identify and block spam calls or SMS, search for unknown numbers, call and chat with friends".[36] Essentially, without the express permission of people in any user's address book, personal phone numbers are matched to names in this 'global database' by this Swedish company and shared with worldwide users. Putting focus on spam calling touches a nerve, certainly in Nigeria where interviewees mentioned rampant 'caller fraud'. When one user saves a number as 'fraud, do not pick' or, 'evil person' (in reference to say a former romantic partner as one interviewee detailed), this is what other users see through this app. In other words, people's personal relationships as they are encoded in their addresses become public information, along with their mobile numbers, on a transnational scale across borders. Marketing and advertising emphasize the legal uses of 'robocalls' taps into user dissatisfaction on 'fraudulent calls, therefore allowing privacy to be exploited as a fix.

In general, we found that apps did not obtain meaningful consent in part because they promise a path to solving a real need, for instance access to loans, thus exploiting users' vulnerable positions, and did not provide clear language on how the apps collected and used data to provide the service for which they were being downloaded. In section2.2, we use loaning apps and other fintech to showcase how the relations between sectors incentivizes business models that violate privacy and elaborate on how personal data obtained through abuse of consent can and has been weaponized in Nigeria.

[35] See Similar Web's list of top apps by rank based on https://www.similarweb.com/apps/top/google/store-rank/ng/all/top-free/ and https://www.similarweb.com/apps/top/google/store-rank/ng/all/top-free/

[36] See https://www.truecaller.com, https://apps.apple.com/us/app/truecaller-block-spam-calls/id448142450, and https://play.google.com/store/apps/details?id=com.truecaller&gl=US

Mobile Network/Data Providers

Beside the importance of low-cost devices and the role that hardware design plays, it's important to understand that the practices of mobile and data network providers also represent a vulnerability in terms of data protection. There are four mobile network service providers (telcos) in Nigeria, three of which are foreign owned: the South African MTN (Africa's largest provider), India's Bharti Airtel (Airtel Nigeria), Globacom (owned by Nigerian Mike Adenuga), and 9mobile (formerly Etisalat, from the UAE). In 2019, Globacom announced that it had extended 4G network to all 36 of Nigeria's states, and Airtel extended 4G services to 100 towns and cities in 2019.[37] While, by and large, telcos follow the laws of the land, ownership determines corporate behavior and most transnational companies operate on profit principles that are not always in the interest of consumers. Unless there are explicit rules on how data should be managed, commercial actors will set and follow practices aimed at the bottom line, often determined by global industry practice.

Telcos connect hardware and software consumers through data and mobile services. Data collection is intrinsic here, but what becomes of that data is a separate matter. In Nigeria, as elsewhere in Africa, mobile service is prepaid via various modalities. In the early days of mobile service provision, voucher scratch cards, in which a customer purchases a fixed value or credit of service and 'loads' it by entering the number on the card into their phone.[38] These practices have changed over time, but the fundamental prepaid model remains. Telcos hold a significant amount of user data as they serve as the connection between the users and other actors described above, i.e., the hardware maker (say Tecno phones' native apps), the intellectual property owner of the underlying operating system (android or Google) or third parties (e.g., games) that run on these operating systems.

Smart Devices, IoT, and AIoT

Using Transsion again as emblematic of dominant practices, we unpack here how surveillance works its way into homes and on bodies through smart devices other than smartphones.

Smart devices incorporate Internet of Things (IoT) into daily affordable goods that in previous decades may have been out of reach of the majority of the world's population. In 2021, Tecno added Artificial Intelligence of Things (AIoT) to what the brand does, claiming this shift as a commitment to providing "the best contemporary technologies for progressive individuals across global emerging markets, giving them elegantly

[37] GSM Association (2019). The mobile economy: West Africa 2019. https://www.gsma.com/mobileeconomy/west-africa/ Accessed June 10, 2022.

[38] Avle, S., Quartey, E., and Hutchful, D., 2018. Research on mobile phone data in the Global South: Opportunities and challenges. The Oxford Handbook of Networked Communication. Oxford University Press.

designed intelligent products that inspires *[sic]* consumers to uncover a world of possibilities…".[39] Here, class mobility in terms of affordable home goods is equated with progressive values and connectivity to transnational peers with similar taste.

As far as marketing goes, Transsion presents its (A)IoT products as cutting edge but affordable. The product lines have since expanded to include two tablets and a wide array of accessories including ear buds, portable Wi-Fi routers (essential in the African market), cables, and smart watches. This sort of expansion into other personal electronics mimics the Chinese giant company Xiaomi which has recently entered various African countries with its wide array of smart devices, as well as western firms like Bosch and GE who all have also turned to AIoT in their home appliances, all aimed at the middle class. Smart devices continuously collect data that is then mined for other uses, again with little meaningful consent.

Crucially, Transsion's gradual shift towards AI, IoT, facial recognition and AIoT, and its efforts to increase intellectual property (IP) in those areas in anticipation of 'warfare,'[40] underscore how significant hardware are as entry points for new forms of data collection from ever expanding populations. More specifically, under the rubric of innovation, design, and continual upgrade, increasingly affordable smart devices enroll populations that hitherto were left out of the logics of surveillance/techno capitalism through the placement of devices on bodies and both private and public spaces, continually abstracting facets of life into calculable data for profit.[41],[42],[43],[44]

Fintech Case Study

Nigeria's financial industry is an essential supporting pillar for the domestic economy with increased electronic payment transactions hitting 34.67 trillion Naira (~ 82 billion USD) in March 2022.[45] In 2017, about 44% of the Nigerian adult population had a bank account, up from 30% in 2014 but only about 1% of the population had any form of insurance or other complex financial product, according to the GSMA, which sees such figures as indicative of a "huge financial inclusion gap."[46] In part due to this gap, the youthful population, and increasing connectivity, fintech activity has been on the rise in Nigeria, attracting an increasing number of commercial actors and marking it as a highly

[39] https://www.tecno-mobile.com/about-us#/

[40] Lu, M., & Qiu, J. L. (2022). Empowerment or warfare? dark skin, AI camera, and Transsion's patent narratives. *Information, Communication & Society*, 1-17.

[41] Avle, S. [forthcoming] Chinese smartphones in Africa: Hardware and data in the platform era. Media, Culture, and Society.

[42] Birch, K. (2020). Technoscience rent: Toward a theory of rentiership for technoscientific capitalism. Science, Technology, & Human Values, 45(1), 3-33.

[43] Ogunmokun, T. (2022). Assessing data protection in Nigeria: A look at biometric identity, surveillance, encryption and anonymity, and cybercrimes. Tech Hive/Omidyar Network/Paradigm Initiative, Nigeria.

[44] Suarez-Villa, L. (2001). The rise of technocapitalism. *Science & Technology Studies, 14*(2), 4-20.

[45] Financial Derivatives Limited (FDC) 2022 https://nibss-plc.com.ng/news/413z20c586qev6grpbv42yd144

[46] Buolamwini, J. (2017, May 29, 2017). Algorithms aren't racist. Your skin is just too dark. *Hackernoon.*

active sector that sees considerable government scrutiny. It is also the sector in which we observe some of the most bewildering uses of consumer data, largely from an explosion of microfinance apps. Most purport to provide small amounts of money quickly and without hustle but ultimately exact not only high interest rates but also, high privacy costs.

Microfinance and Digital Banks

By early 2022, Nigeria had a fair number of 'digital banks', with estimates of between 60-80 loan apps in Nigeria, and suggestions that they belong to about 20 firms replicating the same practice. For instance, Sokoloan, which was fined 10 million Naira by the National Information Technology Development Agency (NITDA) in August 2021 for invasion of privacy, has about seven different apps,[47] a practice that might be tied to the fact that customers sometimes borrow different amounts from different apps to cover their financial needs. It is unclear if consumers know when they are borrowing from the same bank under different apps. SokoLoan describes itself as an "entirely online lending platform that provides short-term loans in Nigeria to help cover unexpected expenses or urgent cash needs" and offers consumers "instant arrival within five minutes", "recommended rewards up to 100N", "short period, high amount", etc.

As mentioned above in section 2.1.3, some of the top downloaded apps in Nigeria include financial ones, for e.g., Umba Mobile (fully digital Irish owned bank), OKash (by BlueRidge microfinance), and FairMoney (digital bank by a microfinance bank operating in Nigeria and India). There were reports that some Tecno phones now come bundled with EasyBuy, an app that offers "flexible mobile phone installment loans",[48] implicating Chinese phone makers along with Irish and Indian 'digital banks' in the Nigerian finance sector. All claim 'quick and easy' ways to access money, often stating that all a customer needs are "an Android phone and a BVN" (Fairmoney) or "an android device, a data connection, a means of identification, as well as valid bank account and card" (Okash).[49] Many advertise aggressively, including sending unsolicited SMS messages through telcos who are also complicit by providing access without consent. One interviewee shared a screenshot of the ads received (see figure 4) to illustrate how these ads show up on mobile phones. The specification of an android phone and a data connection underscores the ease with which consumers can now access these services and showcases how key operating systems are for user data. Third party apps in the Google Play store on android phones are notoriously not robustly vetted for security and many come with malware. While on the one hand, this relatively lax process allows anyone to

[47] See https://techcabal.com/2021/08/24/nitda-fines-soko-loan/ and https://techcabal.com/2022/03/12/nigerian-government-shuts-down-6-illegal-digital-loan-companies/?utm_source=dlvr.it&utm_medium=facebook

[48] https://quickloanarena.com/easybuy-app-digital-loan-purchase-phones/

[49] See https://fairmoney.ng

build and include an app in the store at a relatively low cost, the downside is that unscrupulous actors get to prey freely on vulnerable populations.

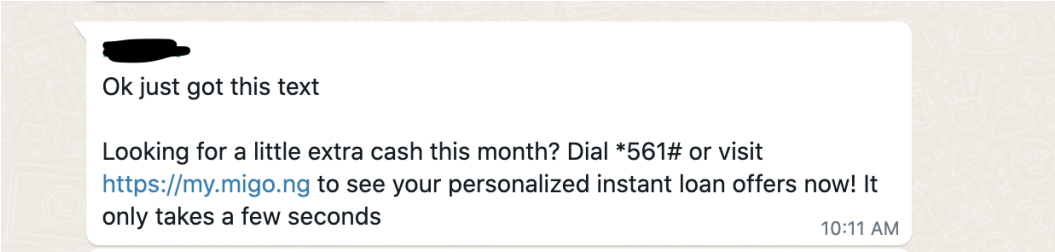

Figure 3. WhatsApp Image showing text of an SMS received on a Nigerian user's phone.

The identification parameters given by these digital banks are basic requirements instituted by the Central Bank of Nigeria (CBN) and give these apps an air of legitimacy. Bank Verification Numbers (BVNs) are unique identifying numbers tied to the biometric data of bank customers that is verifiable across banks. Initiated by the CBN in 2014 through a collaboration with NIBSS and a German biometric firm, Dermalog,[50] BVNs have also been advertised as both a way to curb fraud (through the industry logic of 'Know Your Customer (KYP)), increasing confidence in the Nigerian banking sector, and increasing financial inclusion. The rollout process included the Nigerian Communication Commission (NCC) and Mobile Money Operators (MMO) in 2019 to increase rural participation. As of April 2022, the Nigerian Inter-Bank System (NIBSS) reported that 54 million registrations had been recorded across the country. [51] Combining BVNs with mobile money operation, on the one hand formalizes mobile money within banking infrastructures and on the other hand, works to digitize formal banking in the hands of users. This arguably makes it easier for consumers to trust digital banks, when there may not have good reason to do so given the prevalence of fraud mentioned by Nigerians online and in interviews. Digital banks certainly use their licensure with the CBN to entice and appease users despite their problematic practices.[52]

Unauthorized Uses of Personal Data

Sokoloan's 2021 fine was reportedly for "unauthorised disclosure, failure to protect customers' personal data and defamation of character, and to carry out due diligence as prescribed by the Nigeria Data Protection Regulation (NDP)".[53] NITDA, in the role of a data protection enforcer, found that Sokoloan embedded trackers in their apps and shared customer data with third parties without the knowledge and consent of users.

[50] https://www.dermalog.com Dermalog has been actively providing biometric services in the global south, including ID services, temperature sensors, etc. It's unknown what the agreement is for where the data collected is held and how it might be used downstream by the company. One key issue here is to examine how EU companies operate outside their region, given the dictates of GDPR.

[51] NIBSS 2022 https://nibss-plc.com.ng/news/40t2t6rx62zbfx67xa7qmydxma

[52] See for instance https://www.vanguardngr.com/2022/03/blueridge-microfinance-bank-reassures-its-customers-of-its-continued-business-operations/

[53] https://techcabal.com/2021/08/24/nitda-fines-soko-loan/

This issue of unauthorized sharing of data with third parties includes the release of the personal data of applicants as an instrument to enforce repayment of default loans. Practices included spamming contacts in loan applicants' phone address books with embarrassing messages about their payment defaults, using insulting language, and including threats of harm.

Online/digital banks advertise no collateral but release the personal data of applicants to their address book contacts publicly shame them in cases of default either through the defaulter's own shame at being outed, or, as one interviewee suggested, 'secondhand shame' felt by their contacts on their behalf. If the shaming is to get customers to repay their loans with interest plus high default fees, some repeat offenders might be deterred, but many are simply able to reapply on different apps, sometimes to the same digital bank. Often users do not know that they are applying to the same banks, and it is unclear if the banks sync their data across their different apps. In our research, we also saw some suggestions that some app glitches, whether intentionally created or otherwise, were triggering higher rates of default, which in turn were generating high default fees and punitive interest rates. Several public commentaries on social media and news websites reporting on these practices alluded to this practice as well.[54]

The practices of digital banks have recently seen a response from the Nigerian federal government following public outcry. In March 2022, the Federal Competition and Consumer Protection Commission (FCCPC), NITDA, and the Independent Corrupt Practices and Related Offences Commission (ICPC), in conjunction with the police, raided six digital banks/lending platforms: GoCash, OKash, EasyCredit, Easi Moni, KashKash, and Speedy Choice, reportedly after a 2-year investigation. Some of them were shut down for illegally operating in Nigeria, yet public comments (linked via Facebook) on websites that reported news of these events include dozens of companies such as Easy credit, getcash, 9ja cash, Thumbmoni, Starloan, Aje loan, Lcredit, 9credit, etc. some of which were still visible on the Google Play store. In fact, after Sokoloan was fined and removed from the Google play store in late 2021, reports a mere 48 hours showed the app back online.[55]

Fintech vulnerabilities

The crackdown on these banks was specific to their banking operations (with raids at their offices) but without concomitant attendance to their digital presence and operation. Digital banks can operate from anywhere and shutting down a physical office has considerable limits when they can still directly prey on consumers either by changing their apps or simply staying accessible in an app store. The Google Play store is a

[54] https://techcabal.com/2022/03/12/nigerian-government-shuts-down-6-illegal-digital-loan-companies/?utm_source=dlvr.it&utm_medium=facebook

[55] See https://quickloanarena.com/rogue-app-sokoloan-returns-google-play-store/

transnational marketplace and while sovereign states have routinely asked for the removal of apps, there appears to be little consistency in the rulemaking around removal and reinstatement of apps in particular countries. The entry point in this software application market is just as important as the entry point on the hardware (via AI enabled cameras) discussed in the previous section. Both require specific attention if any meaningful form of data protections is to be enacted.

Moreover, rather than see the practices of micro loaning apps as a purely banking and finance issue in which a few bad actors need to be made an example of, we advocate a much more networked view in which regulation meant to safeguard the integrity of the banking sector also means safeguarding any data and digital technology that might be enrolled into banking and other types of activities. If BVNs, bank cards, etc. are being asked of consumers alongside access to their contact information and that access is redeployed as a tool for repayment, that access becomes a core aspect of the banking process itself, similar in some ways to how traditional collateral might work. Thus, app permissions, consent processes, and disclosures about information uses are integral to the banking sector itself. Given that many of the lenders simply recreate different versions of apps to reach consumers and leave these online access points for consumers to find even if offline operations are disrupted, it is essential that consumer technologies are included in financial regulation.

Summary of Issues

Section 2 has shown how private commercial actors, at various touchpoints, collect, hold, and share user data. We highlight two main points. First, user data is fragmented across not just multiple applications and hardware but also across the geographies that they originate from. Second, hardware are essential vessels for apps, platforms, and other data logics. Specifically, low-cost hardware are critical to the datafication of the everyday and act as entry points for new forms of data collection through facial recognition and AI. Together they raise concerns around transnational processing of data and consumer electronics, marking them as areas in need of regulation in the interest of Nigerian consumers.

Data Protections

Article 37 of the Nigerian Constitution includes a provision that guarantees “the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communication…”. [56] While constitutional provisions for privacy are common the world over, ensuring that privacy is respected has been difficult and regulation has been slow to catch up with the pace of technological change that makes surveillance capitalism the norm. Self-regulation by those that collect personal data is insufficient and ineffective

[56] 1999 Constitution, amended in 2011

when the underlying incentive is to profit from such data. Without a law in place and its effective enforcement, collecting, mining, keeping, sharing user data without meaningful consent will continue.

Legal experts read Nigeria's article 37 as providing a constitutional basis for data protection, yet the Nigeria Data Protection Regulation (NDPR) instated in 2019 to regulate the domestic and cross border protection of Nigerian data does not mention this.[57] Regardless, the NDPR has since its inception attempted to establish "the governing principles of data processing in Nigeria, the lawful basis for processing the rights of data subjects, cross border transfer rules, contents of a privacy policy and implementation mechanisms."[58] Its main objectives are "to safeguard the rights of natural persons to data privacy; to foster safe conduct for transactions involving the exchange of Personal Data; to prevent manipulation of Personal Data; and to ensure that Nigerian businesses remain competitive in international trade through the safe-guards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice."[59] Some experts view NDPR as a 'subsidiary regulation' because many elements resemble the EU's GDPR, and the underlying framework for both are similar.[60]

The NDPR functions under by the National Information Technology Development Agency (NITDA), itself under the Ministry of Communications and Digital Economy (MCDE). NITDA has been playing the role of the Data Protection Authority (see fintech case in previous section) although in February 2022, a new Data Protection Bureau was given the same mandate as the NDPR. At time of writing, it remains unclear how this new bureau will function separately or in complement with NITDA. Its institution is another example of the overlapping mandates that we find in Nigeria's regulatory environment. The 2020 Data Protection Bill making its way through the legislative process has the express goal of establishing "the Data Protection Commission charged with the responsibility for the protection of personal data, rights of data subjects, regulation of the processing of personal data and for related matters."[61] It is unclear

[57] Ogunmokun, T. (2022). Assessing data protection in Nigeria: A look at biometric identity, surveillance, encryption and anonymity, and cybercrimes. Tech Hive/Omidyar Network/Paradigm Initiative, Nigeria.

[58] National Assembly of the Federal Republic of Nigeria (2020). Data Protection Bill. https://www.ncc.gov.ng/accessible/documents/911-data-protection-bill-draft-2020/file Accessed May 19, 2022, p. 7.

[59] National Assembly of the Federal Republic of Nigeria (2020). Data Protection Bill. https://www.ncc.gov.ng/accessible/documents/911-data-protection-bill-draft-2020/file Accessed May 19, 2022, p. 7.

[60] Ogunmokun, T. (2022). Assessing data protection in Nigeria: A look at biometric identity, surveillance, encryption and anonymity, and cybercrimes. Tech Hive/Omidyar Network/Paradigm Initiative, Nigeria.

[61] National Assembly of the Federal Republic of Nigeria (2020). Data Protection Bill. https://www.ncc.gov.ng/accessible/documents/911-data-protection-bill-draft-2020/file Accessed May 19, 2022.

how that will interface with this new bureau and how either of those two will in turn connect with NITDA.

Furthermore, over the years, the Nigerian government has created several mandates and signed on to various multilateral agreements that we call 'data-protection adjacent'. Many approximate key values of data protection but require coordination across agencies to be effectively implemented. Some federal institutions such as the CBN have been central to many of these regulations, further underscoring how important the government views the banking and finances sector. Below, we give a brief overview of some of these data protection adjacent regulations, all of which were prior to NDPR and then review NDPR and the 2020 data protection bill together, highlighting key areas that speak to the issues raised in section 2.

'Data Protection Adjacent' Frameworks Prior to NDPR

Since 2015, several guidelines and frameworks largely related to the financial sector have been in circulation. Figure 5 traces the timeline of some of the key policies, guidelines, and frameworks that address data protection in one form or the other. Most of these were focused on cybercrime between 2015-2017. Between2018 and 2019, several frameworks around financial services were introduced and additional guidelines were introduced in 2020. Given Nigeria's size and its unrelenting infamy as a source of online fraud, the federal government's instinct to protect financial services and increase confidence in the sector is understandable. However, we find that the net effect of the kinds of regulation in place work to protect financial institutions rather than consumers.

In 2020, Nigeria signed on to the ECOWAS Supplementary Act on Data Protection which is considered binding but has yet to be domesticated by legislature.[62],[63] This took place alongside the 2020 Data Protection Bill. In 2021, the CBN again published guidelines on mobile money among other subsectors and an amendment to the NITDA Act, the original law under which the NDPR was introduced in 2019.[64] In general the NDPR is considered a positive move towards more comprehensive data protection, and much of the language in the proposed 2020 Bill reflects some of the principles of the NDPR. Below, we focus on key aspects of both the NDPR and the 2020 Bill.

[62] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

[63] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

[64] For a more detailed overview of these guidelines and frameworks, see reports by Paradigm Initiative 2021 and Ogunmokun n.d. in the reference list.

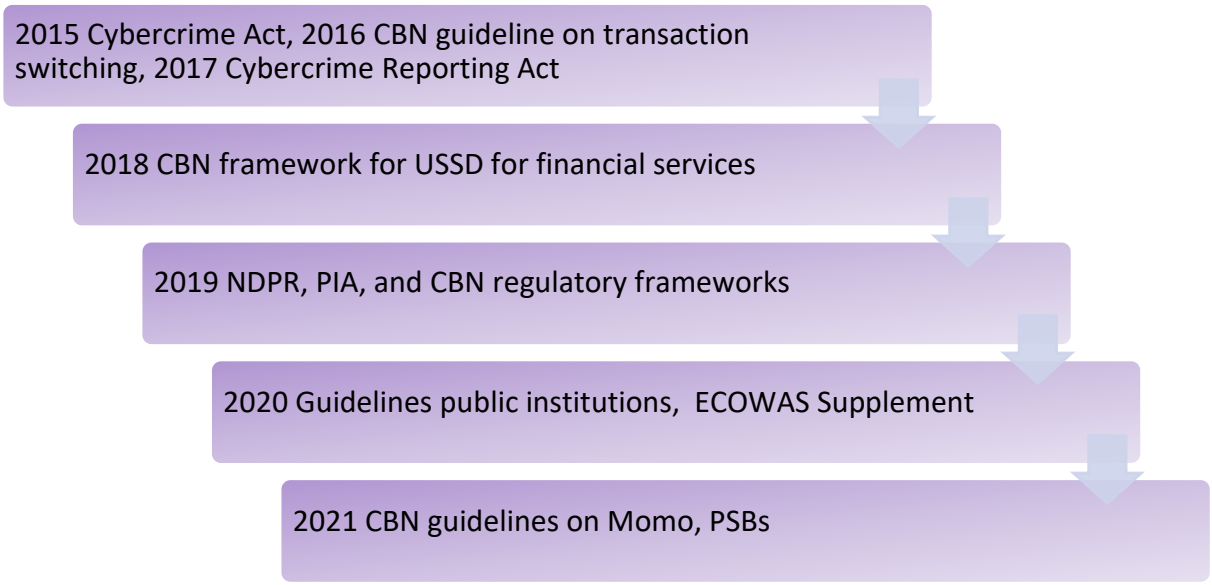

Figure 4: Timeline of Data Protection Adjacent Frameworks and Guidelines

NDPR and The Data Protection Bill

The Data Protection Bill introduced in 2020 retains much of the language of the NDPR, with some additional specifications around categories of people, institutions, and practices. Both emphasize Nigerian nationality, regardless of residence, as the key characteristic of a 'data subject'. At their core, both regulatory frameworks emphasize the dignity of persons through respect for their privacy and aim to provide a framework for the protection of personal data, regulate information processing related to data subjects, and safeguard constitutional rights to privacy. The Bill aims to "promote a code of practice that ensures the privacy and protection of data subjects' data *without unduly undermining the legitimate interests of commercial organizations and government security agencies for such personal data* " [emphasis added]. This aim appears before the language of minimizing harms or abuse to data subjects, fairness, etc. This echoes the NDPR's statement (although listed fourth instead of first as in the Bill), that its objectives include ensuring that "*Nigerian businesses remain competitive in international trade* through the safe-guards afforded by a just and equitable legal regulatory framework of data protection…" [emphasis added]. Based on the previously noted observation that the CBN's data protection adjacent regulations appear to favor institutions rather than individuals, we perceive a shift towards elevating techno-capitalist needs above citizens and consumer safety, even if the latter remains of interest to regulators.

With respect to the importance of digital technologies, and the unique issues they bring for privacy, both the NDPR and the 2020 Data Protection Bill pinpoint technical identifiers such as device IMEI, mac addresses, GPS location, etc. as vulnerabilities that can compromise privacy. In this way, both frameworks are somewhat attuned to the hardware of smart devices in ways that are consistent with the general concerns of this report. Below, we address core categories of issues that intersect with our findings about

the fragmentation of consumer data across hardware, software, and geographies. If the Data Protection Bill passes into law, it would signal a move towards the kind of consolidation that might make implementing data protections more effective, particularly if some prior regulations are amended or grandfathered into the new law. However, some language would have to shift to better prioritize Nigerian *people* over institutions and businesses.

Collecting and Processing Data

The NDPR emphasizes that the collecting, processing, and storing of data should not be beyond what is "reasonably needed". This falls within the principles that collecting, and processing of data should be "adequate, accurate and without prejudice to the dignity of a human person." While this is echoed in the Bill, the latter adds specific language that personal data should "be kept in a form that permits identification of data subjects for no longer than necessary for the purpose for which the personal data is processed, and data shall be deleted once the purpose for which it has been processed has been achieved or kept in a form that prevents any direct or indirect identification of the data subject." We find the specification of deletion necessary because it specifies action data processors must take. Below, we highlight key terminology that we fund essential to safeguarding privacy and protecting data based on the practices we described earlier.

Consent

The NDPR specifies consent as 'freely given, specific, informed, and unambiguous indication of the data subject's wishes by which … through a statement of clear affirmative action, signifies agreement to the processing of personal data…". The Bill takes this further by specifying in section 5 that this consent can be given in writing or orally and that "silence or inactivity does not constitute consent by the data subject." The Bill does away with the language from the NDPR that says consent must be obtained "without fraud, coercion or undue influence" (section 2.3). Moreover, per the NDPR, the request for consent should be "clearly distinguishable from the other matters" and both it and the Bill state this should be presented in a concise, transparent, in an intelligible and easily accessible form" using clear and plain language. Both specify that consent can be revoked and that consent to processes not necessary to the performance of the service should not preclude uses of that service.

These consent parameters are essential in the everyday uses of smartphones and smart devices. First, the global trend is for apps to present long and unreadable privacy policies that request consent for all kinds of activities that force non-use when the user declines. This forceful non-use is named as unacceptable in the NDPR. The choice to opt out of data practices has only become visible, for instance, in the use of cookies on websites, and widely so because regional law such as the GDPR require websites to disclose their cookies and give consumers the option to opt out of all but 'strictly necessary' cookies. Recent research, however, suggests that these are having at best modest effects, and at

worst represent 'a useless exercise' because of the ways that this information is displayed to users, among other things.[65] The complex and bundled languages present in requests for consent in app stores violate the parameters of informed consent outlined by the NDPR and the 2020 Nigerian Bill.

One key difference between some of the phones we examined was that Google products required consent for use, and some bundled software made by the Chinese phone makers allowed use even without consent. Google's consent forms were longer in language that was not understandable, increasing the burden of the user and raising the likelihood that they would not attend to language carefully. Transsion and Xiaomi's native apps on the other hand, used simplified language and informed the user to some extent what to expect when consent is given.

Moreover, some, such as Xiaomi on the top-level phone 11T, go as far as revoking consent for apps that have not been used in a while, thereby respecting the rule to not keep data indefinitely. Here, the western giant perpetuates a surveillant logic that the Chinese producer rejects. This flies in the face of narratives that Chinese techs are unilaterally surveillant because the state surveils its own people. While we note that Chinese hardware are entry points for surveillant practices, the core challenge comes from the western software that these phones come bundled with and the differing data policies they hold compared to the hardware makers'. Such bundled software also includes Meta products like Facebook and WhatsApp, which also come with yet a different set of data policies that a consumer must attend to separately. The different data policies and consent process can and do overwhelm users and thus policies aimed at obtaining informed consent must address how consent is fragmented and require consolidation in a way that is consistent with protecting users.

In the case of the fintech raids described in section 2, NDPR in collaboration with other government agencies named the improper uses of personal data and subsequent defamation of users' character. We found that the advertisements used by the apps constitute coercive means and their requests for consent are generally obfuscated in ways that violate NDPR. However, while the raids were justified, and named the general offenses, we did not see an accompanying requirement to change either the consent practices and information given to consumers or ensuring that those apps do not become accessible through the Google Play store after the digital banks and loan sharks have ostensibly been shut down. The NDPR's penalties for default only specify the payment of fines, which was the case with Sokoloan, which clearly did not take away the problem. Thus, in as much as the Bill specifies deletion of data, we find that including specific breaches of informed consent as a legally enforceable breach of law and

[65] See https://www.nytimes.com/2022/01/29/business/dealbook/how-cookie-banners-backfired.html?searchResultPosition=1

requiring removal of access point essential for changing common problematic data practices in the digital market.

Foreign Processing

Given the preponderance of foreign made hardware and software on the Nigerian market, the section of the NDPR and Bill that address this are crucial to enforcing data protections. In section 6 of the Bill, a data controller (in our cases, the apps, hardware makers, etc.) should inform the data subject (user) of "any intended transfer of personal data to a third party or foreign nation or international organization and a description of the safeguards provided to ensure the adequate protection of personal data". The relatively sparse language on this is in sharp contrast to the depth of section 2.11 of the NDPR that focuses on transfer to a foreign country. We sense the impending loss of opportunity to regulate a substantial aspect of data practices and recommend legal interoperability be added to the Bill before it is passed into law. We do not suggest enforcement will be easy, but Nigeria is a large desirable market that has the leverage it needs to exact accountability from foreign technology firms.

The current governing framework in the NDPR's section 2.11 charges that foreign transfers of data be supervised by the federal attorney general, and those transfers can only happen when the destination ensures adequate level of protections. This is evidently not being enforced as there is no indication of the attorney general being involved with the data policies of the top 10 apps described in the data practices section of this report. That section of the NDPR also specifies that the attorney general must take into consideration "the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation.... And the access of public authorities to personal data". Moreover, the attorney general must also consider the implementation of "data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another foreign country..." and, "the existence and effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organization is subject, with responsibility for ensuring and enforcing powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the relevant authorities in Nigeria". Until February 2022, when a Data Protection Bureau was instituted, such an organization didn't exist in Nigeria itself even though the NDPR was crafted in 2019. This bureau takes away the need for the attorney general to do this work that is more suitable for an independent data protection agency, and somehow it has been brought into existence outside of the Data Protection Bill whose express aim was to give regulatory powers to it. We find this confusing phenomenon another example of a fragmented regulatory environment.

The NDPR suggests that should the attorney general or the data protection agency/bureau be unable to make these necessary determinations, a transfer can only

happen if one of any of the following is true: that "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers," the transfer is deemed necessary for a number of reasons including for the "performance of a contract between the Data Subject and the Controller or the implementation of pre- contractual measures taken at the Data Subject's request", or "for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person" (section 2.12). In all circumstances, the data subject is supposed to be "manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country."

Needless to say, all of these are missing from the actual practices and interactions between smart device users and the product makers. Without clear penalties and enforcement, digital platforms and tech providers have shown they will follow the path of least resistance and continue to harvest droves of consumer data, move them across borders, and share with third parties if they can profit from doing so. Across the board, Nigerian data goes to Irish and Indian digital banks, American and European social media apps, as well as Chinese hardware manufacturers and social media. We did not notice clear warnings in the user agreements about foreign transfer of data or any acknowledgment of domestic laws in that regard. While the NDPR appears well crafted towards protections, its lack of clear implementation across spaces in which data is processed (i.e., real practices) remains the biggest obstacle to data protections. The lack of detail on all this in the 2020 Bill is concerning as well. Below, we suggest some recommendations on how to reconcile the current protections with practices observed in the uses of smartphones and other smart devices.

Discussion and Recommendations

Based on our findings that user data is fragmented across not just multiple applications and hardware but also across the geographies that they originate from, we agree with prior assessments that a comprehensive law that is cognizant of data realities within Nigeria and also attends to international standards needs to be passed for data protections to be effectively implemented.[66] This implementation needs to pay attention to technological shifts in consumer electronics and be bolder in regulating the transnational logics of data extraction. Boldness here includes being unafraid to enforce foreign processing and transfers in ways that are consistent with standards elsewhere (for instance the EU's GDPR) and raising the penalty for default, while being responsive to changes in practice and technology.

[66] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

While the responsiveness to crises is laudable, as seen in the fintech case study, they always come after the fact, and in Nigeria, they join an already formidable compendium of regulations. Indeed, after the joint raid of microlending platforms and 'loan sharks' as some Nigerian news outlets described them, the FCCPC was quoted that yet another regulatory framework for loan platforms would be introduced, again, responding to a sector specific issue. This game of 'whack-a-mole' -- generating new regulatory language to quell bad behavior that rears its head -- makes keeping track of regulations, let alone their enforcement, difficult for both regulators and those they are supposed to serve. Rather than such action resulting in robust and clear data protections for consumers, this creates "fragmentation of the Nigerian data protection regulatory landscape."[67] Below, we highlight what this looks like and discuss two key regulations, the NDPR and the 2020 National Data Protection Bill in terms of the vulnerabilities described above.

Provisions for Hardware and Emerging Techs through Periodic Review

Based on our findings that hardware acts as experimental sites for new forms of datafication, we recommend amendments that allow for flexible enrollment of emergent tech into data protection regulation. Specifically, including a provision for continual assessments of emergent technology such as artificial intelligence and facial recognition, like the requirement in section 2.1(5) of the Bill for annual reports by a specific date, would give regulators a chance to be more quickly caught up to industry practices and user concerns. This must be within the purview of the regulatory body with sufficient expertise and independence to make these determinations. Governance of such tech are a global challenge but by making provisions for annual reviews of key practices, the Nigerian data protection agency/bureau can effectively respond with the right kinds of processes to protect personal data and enact an overall data protection environment that is responsive and accountable to Nigerians people rather than business entities. We believe it is possible to enact a data regime that allows profit making as well as societal protections. Even though cookie policies have been critiqued, their implementation shows that they may not be as damaging to business interests as industry suggests and therefore the Nigerian government can still protect its economy as well as its people from rampant and unchecked technocapitalism.

Legal Interoperability

Data move with little regard to borders, but this need not be the case. A key challenge remains in the language around foreign transfers (or lack thereof in the case of the 2020

[67] Paradigm Initiative. July 2021. Data protection authorities in Africa: A report on the establishment, independence, impartiality and efficiency of data protection supervisory authorities in the two decades of their existence on the continent.

Data Protection Bill). First, rather than task a third party outside the data protection bureau – in this case the federal attorney general – to oversee this practice, it might be better to more clearly add this to the data bureau's mandate and give it legal powers to enforce penalties (backed by courts) when data processors default. Secondly, rather than require granular knowledge of foreign destinations for data transfers, current law making through the Bill can aim to be interoperable through use of strategic language. This is already visible in the overlap between the language of the Nigerian data protection regulations and the EU' GDPR. Some broadness in definition might be beneficial here when in other places we have advocated for specificity. If amendments suggested in section 4.1 are rooted in practices, this would make legal interoperability easier across sovereign jurisdictions.

Conclusion

Access to digital technologies is on the rise and the industry keeps finding inventive ways to enroll daily life into the digital environment through new affordable devices. In this report, we have sought to highlight the role that smartphones play within a landscape of increased digital access and the processes of digitization of the everyday. Specifically, we have shown how hardware are a key entry point for new forms of data collection and how consumer data is geographically fragmented. Regulation needs to be attuned to these realities, not in an ad hoc whack-a-mole way but rather in a comprehensive way that comes from taking a networked view of data practices and protections. Our recommendations are for a more responsive regulatory environment attuned to changes in practices of technology production and uses, but one that is consolidated in a data protection agency rather than spread across multiple government agencies. We emphasize the importance of privileging individual data rights above or alongside institutional protections.

adapt

About the Author

Seyram Avle studies how digital technologies are made and used in the Global South, particularly as they relate to labor, identity, and futures. She currently works as Assistant Professor of Global Digital Media at the University of Massachusetts, Amherst.

Acknowledgements

Neo Nyoni (Northeastern University), Khadijah El-Usman (Paradigm Initiative, Nigeria), Grace Githaiga (KICTANet, Kenya), Meshak Masibo (KICTANet, Kenya), Internews staffers Laura Schwartz-Henderson, Benjamin Whitehead, Skylar Sallick, and the experts and users interviewed in Nigerian and Kenya.