StearsData Luminate
Building stronger societies

Data & Digital Rights in Nigeria

Assessing the activities, issues and opportunities

Contents

About this Report

Luminate commissioned this report as part of its Data & Digital Rights initiative. Stears Data was engaged to map Nigeria's data and digital rights landscape. This included providing an analysis of the legislative framework and the activities of the stakeholders in research, advocacy, policymaking, regulation, litigation, and data use. The research focused on the context-specific issues related to data and digital rights in Nigeria, i.e. issues with existing interest or momentum from civil society, private sector and government, and the prominent supporters of this work.

Research Methodology

The methodological approach combined desk research with stakeholder engagement. The data and digital rights ecosystem is made up of different actors who are motivated by different incentives. To capture the main drivers influencing the ecosystem, the following steps was adopted.

1. **Engagement Strategy:** An engagement strategy was prepared to outline the goals of the engagement. This was to understand the stakeholders' point of view, successes, concerns, and broad context.

2. **Stakeholder Mapping:** Defining the criteria for identifying and prioritising stakeholders—primarily based on their influence on the issues and regulatory framework—and the engagement mechanisms to be used. The key groups were identified by conducting preliminary desk research, i.e. advocates, regulators & lawmakers, and data controllers & processors.

3. **Stakeholder Engagement:** Interviews were conducted with stakeholders from each group. Where this was not possible, we offered the ability to provide written responses to consider in the preparation of the report. Breakdown of stakeholder group:
   a. Ten advocates (6 civil society organisations, three academic & research institutions and one independent researcher)
   b. Four funding organisations
   c. Two representatives from the public sector
   d. Two representatives from the private sector
   e. Two representatives in the journalism and media sector

4. **Identifying Opportunities:** Assessing the potential opportunities and gaps using the information collected from independent research and the feedback received from stakeholders. Our approach considered deficits in supporting data and digital rights in Nigeria and how to address these by working with the stakeholders.

Limitations of the Research

While significant attempts were made to hear as many voices as possible, it is essential to note that the evidence collected during this exercise represents only a sample of the data and digital rights stakeholders. Additionally, due to various factors, some stakeholders contacted were unable to provide their input to our research.

We emphasise that this is not representative of the views of all stakeholders in Nigeria's data and digital rights ecosystem. Instead, it is a synthesis of the priority issues identifited from conversations and information provided by our sample of stakeholders.

Executive Summary

Data and digital rights include a range of rights and obligations required to effectively and safely participate in a tech-enabled society. Data rights focus on empowering individuals with rights to determine how data about them is used, while digital rights are the rights required by individuals in the digital age.

This report maps the data and digital rights landscape in Nigeria by identifying key issues within the space; effective responses and approaches to addressing those issues; opportunities for impact; and key stakeholders involved in data and digital rights who are potential beneficiaries, local and international partners or collaborators. The report also analyses Nigeria's existing legislative framework to identify gaps that need to be addressed to strengthen data and digital rights.

Nigeria has no comprehensive legislation that addresses data and digital rights. Instead, various pending and enacted sector-specific laws govern data and digital rights. A summary of significant laws and regulations governing data and digital rights is provided in the table below.

KEY DATA & DIGITAL RIGHTS LAWS AND REGULATIONS IN NIGERIA

Legal provision	Type	Summary	Implication/Example
Constitution of the Federal Republic of Nigeria 1999 (Chapter IV)	Constitution	Grants fundamental right to privacy and freedom of expression. Rights do not invalidate any law reasonably justifiable in a democratic society including laws in the interest of defence, public safety, order, morality and health.	The right to privacy and freedom of speech online is not well defined. "Public safety" can be broadly interpreted.
Nigerian Communications Act 2003	Federal Legislation	Established the body to regulate the communications sector. It allows for authorised interception of communications, suspension of licences, order disclosure or prevention of specified communications, under the justification of national interest and national security.	Limited judicial oversight, broad interpretation of national interest leads to abuses. Can be used by security agencies to access communications of advocates or members of the public.
Cybercrimes (Prohibition, Prevention Etc) Act 2015	Federal Legislation	Provides the framework for punishing cybercrime. It states that any person who knowingly or intentionally spreads information they know to be false to cause annoyance, inconvenience, insult, injury...has committed an offence and shall be eligible for prosecution.	Frequently used to prosecute journalists for criticising the government.
Freedom of Information Act, 2015	Federal Legislation	Enacted to make public records and information more freely available. Contains a number of exemptions that allow delay or refusal of disclosure.	Exceptions are broad and can be used as a catch all to prevent disclosure of information.
National Identity Management Commission Act 2007	Federal Legislation	Creates the commission to establish the National Identity Management System. The Act provides that no person or corporate body has access to data in the database concerning a registered individual without authorisation from the Commission. However, the Commission can provide a third party with information in the database without consent, if in the interest of national security.	"National security interests" can be broadly interpreted. There have been concerns around the data protection frameworks that protect the information collected by NIMC.
Nigeria Data Protection Regulation	Federal Legislation	Regulates and controls the use of data in Nigeria. Confers the rights to information, access, rectification, withdraw consent, object, portability and to be forgotten concerning personal data. Governing body is NITDA, sitting within the Ministry of Communications and Digital Economy, so there is no independent oversight.	Conflicts of interest can easily arise regarding the use of data by NCC or other government ministries.

Developing Issues

In preparing this report, stakeholders were engaged to provide insights into the key issues they faced. Issues that were identified from discussions with stakeholders were as follows.

Data Rights - Data Protection

There is insufficient judicial and regulatory oversight available to sufficiently protect personal data, especially when the government perpetrates breaches for administrative functions or national security purposes. Provisions in telecommunication and cybercrime legislation can be exploited by government departments to collect personal information from telecommunications providers without a court order. In the private sector, there are reports of telecoms service providers repurposing customer data without appropriate consent. Some financial service providers also offer products that are not built with sufficient security features to protect their customers against hacks and data breaches.

Data Rights - Open Data

Open Data supports the transparency of government activities, allowing citizens to hold them accountable and encourage greater efficiency in the public sector. The Nigerian government has a long history of secrecy, entrenched in law through the Official Secrets Act and perpetuated through three decades of military rule. Although the Freedom of Information Act, 2011 supersedes this, it only imposes a duty to react to requests, and a deeper cultural shift is needed towards proactive disclosure.

Digital Rights - Freedom of Expression

Freedom of expression in Nigeria is being threatened through the assent of repressive bills. The Protection from Internet Falsehood and Manipulation Bill, 2019 ("Social Media Bill") and the Prohibition of Hate Speech Bill ("Hate Speech Bill") both restrict freedom of speech online, with unclear provisions against sharing statements likely to be prejudicial to national security. These can be interpreted to prosecute anyone who criticises the government. Although the Nigerian Constitution provides for freedom of expression, repressive techniques can be used to effectively censor advocates and members of the public.

Digital Rights - Online Privacy & Surveillance

The Nigerian government has been building its surveillance capacity, with allocated budgets exceeding NGN15 billion since 2017. Although the government claims that these capabilities are being built to fight domestic terrorism,[1] there is the potential they are also being used to spy on citizens. Journalists have reported they fear monitoring and surveillance by the government, and many have had to go into hiding after receiving threats. During the 2020 EndSARS protests, prominent online activists spoke of receiving threats, having their bank accounts and phone numbers blocked, and passports seized.

Opportunities for Impact

Based on the core activities of stakeholders in data and digital rights, the following strategies have been effective at enacting change.

Advocacy

This includes activities by an individual or group aimed at influencing decisions within political, economic, legal and social institutions e.g. media campaigns, lobbying, public townhalls/speeches and the commissioning of research.

Lobbying, a form of advocacy targeted at legislators on specific issues or legislation, has been a high impact activity for advocating change as critical concerns voiced by stakeholders often require lawmakers' support to change or enact legislation. Lobbying efforts by civil society groups[2] have helped push back against laws such as the Social Media Bill and motivated the Data Protection Bill, which is going through its second reading in the National Assembly.

Similarly, public campaigns have been effective at raising awareness and sensitising the public to data and digital rights issues. For example, Amnesty International's campaign for protecting freedom of expression for journalists has brought attention to the harassment and detainment of journalists.

Further funding support is required to keep up lobbying efforts, and stakeholders have highlighted the opportunity to improve the effectiveness and reach of public campaigns through local media and other communication channels.

Ligitation

Data and digital rights litigation is a nascent area, with many regions around the world still developing or updating their legislation to reflect changing technologies. Strategic litigation provides an opportunity to clarify the interpretation of existing laws and how they may be applied to data and digital rights issues. By doing so, gaps in the existing legal framework are identified, promoting progressive jurisprudence and the reform of repressive laws.

There are opportunities to increase the effectiveness of strategic litigation. The first requires an increase in the pool of knowledgeable professionals in the system; the second requires litigants to collaborate and pool resources; and the third requires funding organisations offer flexible litigation funding to allow operators to prioritise emerging issues.

Public Education

Many Nigerians do not know their rights or how they can enforce them.[3] Public education and sensitisation to the issues will help increase participation in advocacy. There's an opportunity to improve funding to grassroots organisations, to enable access to those in rural communities or without access to the internet. Citizens aside, there is much learning that needs to be done in public institutions. Some advocates are already engaging in capacity building for public servants and members of the legal community. This is important to build skills, knowledge and relationships for future collaborations.

Building a Community

Many segments of society are trying to progress data and digital rights in Nigeria in various ways. There have been some attempts at collaboration at a regional level, but few specifically focus on Nigeria as coordination efforts have not been country specific. Building a community will provide visibility over other stakeholder activities, where support is needed, and better coordination to exert additional pressure on government stakeholders required to enact change. There's an opportunity to bring together the different groups working to address data and digital rights in Nigeria, helping to upskill smaller grassroots organisations, accelerate research through ease of access to materials or other meaningful activities. Joining forces will help to enhance the impact of all actors.

1. Introduction

1.1. Understanding Data and Digital Rights

Data rights can be understood as a framework that empowers individuals with rights to determine how data about them is used. This includes rights such as being protected from unreasonable surveillance, from having one's behaviour unknowingly manipulated or being unfairly discriminated against based on data.[4] There are ongoing debates around the implementation[5] and exercise of data rights, primarily related to ownership over personal data and the right to use, possess, and dispose of it.[6] This report looks at how data rights may manifest in the areas of open data and data protection.

Overlapping with data rights are digital rights, which can be understood as human rights required in the digital age.[7] This report looks at the right to online privacy and freedom of expression—extensions of the equal and inalienable rights laid out in the United Nations Universal Declaration of Human Rights.[8] It is important to note that the scope of data and digital rights extends beyond[9] what is covered in this report as the focus areas merely reflect the activities in Nigeria. Other areas of concern include the use of artificial intelligence and automated decision making in the public sector, which is the subject of future work for Luminate.

1.2. A Need for Regulation

The technology/ICT sector in Africa has seen continuous growth driven by mobile technologies and services that have supported 3.8 million jobs (directly and indirectly), contributed $155 billion of economic value (8.5% of the GDP of sub-Saharan Africa), and $17 billion to the public sector through taxation.[10]

Furthermore, the recent pandemic has made digital transformation a top priority again for African governments. As the African Union Commissioner Amani Abou-Zeid highlighted: the "COVID-19 crisis has become the single biggest catalyst for digital transformation and has moved digitalisation from a niche market into mass adoption".[11]

A natural consequence of digitisation is the increase in day-to-day activities conducted online. As more users continue to go online, their data and digital rights, particularly the rights to privacy and freedom of expression, are increasingly essential and need adequate protection. In its 2019 report on the State of Internet Freedom in Africa, the Collaboration on International ICT Policy in East and Southern Africa ("CIPESA") highlighted a worrying trend toward greater digital surveillance by African states, lacking comprehensive privacy laws and low levels of public awareness around data protection.[12]

> **"Data governance and data ethics are emerging issues that have not had a lot of traction but social media regulation is a pertinent issue."** - Academic Researcher

Moreover, as governments worldwide implemented pandemic-related emergency measures and fought misinformation and disinformation related to Covid-19, data and digital rights were neglected or undermined in some cases. Several African governments have enacted vague and broad legislation that curtailed freedom of expression and restricted access to information through censorship, filtering of content, arbitrary arrests, and harassment of journalists, online activists and bloggers. These laws required the collection of personal data, contact tracing and surveillance activity in countries such as Kenya, Nigeria, South Africa, and Tunisia, undermining individuals' data rights in the absence of robust data

protection safeguards.[13]

1.3. Nigeria in Focus

Nigeria is Africa's most populated country and largest economy, with a population of around 211 million and a GDP of $467 billion.[14] As of 2020, the number of Nigerians using the internet was estimated at 100 million (with a 46.6% penetration of the population).[15] This figure is projected to grow to 131.7 million internet users by 2023, and internet penetration is set to reach 65.2% in 2025. With almost three-quarters of Nigerian web traffic being generated via smartphones, Nigeria ranks at the top of the list of African countries based on the share of traffic via mobile.[16]

Given the advancements in the use of technology by the private sector, increased civic engagement online and ongoing government attempts to regulate internet use, this report considers the various concerns that arise in Nigeria's data and digital rights ecosystem.

> **"Online harassment is an area of concern as the Nigerian government is quite sophisticated in surveillance." -** CSO

According to Freedom House, Nigeria's online environment has seen a continuous decline following the February 2019 elections, with increasing misinformation being spread online, attempted legislation to limit free speech online, and journalists prosecution for online activities.[17] The government has also continued its consideration of legislation such as the Social Media Bill that would restrict online speech even with fervent opposition from internet users and civil society.[18] There have also been reports by numerous advocates, journalists and internet users of arrests for their online activities, with charges that included spreading false information about COVID-19[19] and insulting government officials.[20]

The Nigerian government has officially acknowledged the connection between digital rights and human rights through a 2012 United Nations resolution that affirmed that the civil, political, economic, and social rights that people enjoy offline must also be protected online (which was reaffirmed by Nigeria in July 2016).[21] However, there are ongoing tensions between the government on the one hand and civil society and Nigerian citizens on the other due to the use of online surveillance and attempts to regulate internet activity.[22]

2. The Legal & Regulatory Landscape

2.1. Nigeria's Legal System

Understanding Nigeria's legal framework is essential for assessing the issues faced in data and digital rights and the opportunities for impact. Due to its history, Nigeria has four distinct sources of law that form a hybrid legal system:[23]

- statute law;
- common law;
- customary law; and
- Sharia (Islamic) law.

Federal laws are made up of statutory and common law, while state laws are derived from all four sources. Customary laws are administered by native or customary courts and are usually presided over by traditional rulers, who generally hear cases relating to family issues such as divorce. Sharia law is based on the Maliki Islamic code and is administered by *Qadis* (judges).[24]

State legislatures are prevented from passing laws on matters that are part of the Exclusive Legislative List,[25] which includes defence, foreign policy, and mining—all of which are the province of the federal government.[26] In addition, federal law prevails whenever federal legislation conflicts with state legislation.[27]

Spectators have noted conflicts between state Islamic laws and federal laws—particularly in the area of human rights. For example, Human Rights Watch highlighted some concern around the implementation of *hisbah*[28] and Sharia laws in Northern Nigerian states arguing that they conflict with certain fundamental human rights—including the right to privacy.[29] Hisbah refers to community morals, and by extension, to the maintenance of public law and order and supervising market transactions.[30]

According to observers, hisbah can serve as a collective community watch to report individuals suspected of breaking the law or violating Islamic practices.

In some instances, this could ultimately mean the violation of a person's right to unlawful interference with their private life, family, home or correspondence.[31] In researching this report, few cases of abuse of data and digital rights resulting from the enforcement of Sharia law were identified. However, some recent cases include: musician Yahaya Sharif-Aminu's death sentence for sending a voice note sent over Whatsapp "blaspheming against the prophet Mohammed";[32] and the actress Rahama Sadau's charge for inciting blasphemy over an image posted on Instagram in an outfit revealing her back.[33]

2.2. Human Rights Laws

Chapter IV of the Nigerian Constitution outlines fundamental human rights and protects these rights. Other international treaties on human rights are recognised and enforced in Nigeria if they are ratified and enacted by the legislature.

Some of the human rights entrenched in the Constitution include:

- The right to life.
- The right to respect and dignity.
- The right to personal liberty.
- The right to privacy.
- The freedom of thought, conscience and religion.
- The freedom of expression.
- The freedom of assembly and association.
- The freedom to move freely throughout Nigeria and to reside in any part.

2.2.1. Data & Digital Rights as Constitutional Rights

The right to privacy and freedom of expression are derived from Chapter IV of the 1999 Constitution of the Federal Republic of Nigeria. Section 37 provides that the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications are guaranteed and protected.

In contrast, Section 39 provides that every person is entitled to freedom of expression, including the freedom to hold opinions and to receive and impart ideas and information without interference.[34]

Although the constitutional right to privacy and freedom of expression are established as fundamental rights, data and digital rights are not well developed or established under the Nigerian legal and regulatory frameworks. Instead, a combination of legislation and regulation incidental to data and digital rights are relied upon as no legislation explicitly addresses the subject of data and digital rights. Naturally, this creates legal gaps and loopholes that need to be addressed to strengthen individuals' rights.

2.2.2. Data & Digital Rights as Human Rights

It is crucial to highlight the significance of privacy in the development and enjoyment of other human rights. The introduction of legislation and regulation often presents an opportunity to enhance privacy in a region. However, lawmakers also attempt to balance competing rights, such as the free flow of data, transparency, national security and overriding economic interests. As a result, how regulatory and supervisory authorities evaluate the importance of privacy determines the data protection standards and sets the benchmark for their interpretation. It is common to approach this from an assumption that all competing interests are equal. However, human rights law scholars argue that not all human rights should be treated as equal, and privacy should occupy an elevated position.

First, privacy is a critical element to personal fulfilment and self-development, which has intrinsic value in fostering a democratic society cultivating diverse views. Second, a liberal development of personality is a necessary precondition for the free exercise of certain human rights, e.g. freedom of expression; freedom of thought, conscience and religion; free elections; and freedom of assembly and association. Finally, some level of privacy should be guaranteed in order to exercise these human rights freely.[35]

2.3. Regulation of Data & Digital Rights

As previously noted, Nigeria has no comprehensive data privacy and protection legislation. However, various pending and enacted sector-specific laws contain privacy and data protection provisions. These form the framework under which data and digital rights are protected. The key laws and regulations governing data and digital rights are outlined below.

2.3.1. The Nigerian Constiution

The Constitution of the Federal Republic of Nigeria 1999 (as amended) provides Nigerian citizens with a fundamental right to privacy and freedom of expression.

However, the Constitution also provides that none of the rights granted to citizens will invalidate any law that is "reasonably justifiable in a democratic society".[36] This includes laws that are in the interest of defence, public safety, public order, public morality or public health, or to protect the rights and freedoms of other persons. Effectively, acts of the National Assembly that are deemed to fall within the exceptions provided in the Constitution can override the constitutional rights to privacy and freedom of expression.

2.3.2. Cybercrimes Act

The Cybercrimes (Prohibition, Prevention etc.) Act 2015 ("Cybercrimes Act") provides a legal and regulatory framework that prohibits, prevents, detects, prosecutes and punishes cybercrimes in Nigeria. Cybercrimes are crimes in which a computer is the object of the crime or is used as a tool to commit an offence. Offenders may use computer technology to access personal or commercial information or use the internet for exploitative or malicious practices. The Cybercrimes Act requires financial institutions to retain and protect data and criminalises the interception of electronic communications.

HIGH AND LOW RELEVANCE* LEGISLATION AND REGULATION

CONSTITUTION

HIGH RELEVANCE

Constitution of the Federal Republic of Nigeria 1999 (Chapter IV)

FEDERAL LEGISLATION

HIGH RELEVANCE

Nigerian Communications Act 2003

Cybercrimes (Prohibition, Prevention Etc) Act 2015

Freedom of Information Act, 2011

LOW RELEVANCE

National Identity Management Commission Act 2007

Child Rights Act 2003

Credit Reporting Act 2017

National Health Act 2014

FEDERAL REGULATIONS

HIGH RELEVANCE

Nigeria Data Protection Regulation

Consumer General Code of Practice 2007

Nigerian Communications (Enforcement Process, etc.) Regulations 2019

Registration of Telephone Subscribers Regulations 2011

Lawful Interception of Communication Regulations 2019

LOW RELEVANCE

Consumer Protection Framework 2016

***High or low relevance** is determined by the provisions included in the legislation or regulation relevant to data and digital rights. For instance, while the National Identity Management Commission Act, 2007 presents key challenges on data protection for citizen's identity, the legislation primarily focuses on the establishment and management of identity systems and less on the protection of personal data. Thus, from a legal and regulatory perspective, we class it as "low relevace".

> **"Nigeria has been stigmatised as the hub of cybercrime over the last 10 years. This creates incentives to have stronger regulation and legal frameworks to fight cybercrime and cyberterrorism."** - Funder

Section 24 in part III of the Cybercrimes Act, in particular, is said to be aimed at regulating exploitative and malicious practices. Section 24(1a) of the Cybercrimes Act states that any person who knowingly or intentionally sends a message or other matter using a computer system or network that "is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be sent" has committed an offence under the Act and shall be eligible for prosecution.

Also, Subsection (1b) provides that any person who knowingly or intentionally spreads messages or other matters using a computer network system that "he knows to be false, to cause annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent" faces the same possibility of punishment. The broad nature of the wording in the provision has had immense implications for online press freedom in Nigeria and freedom of expression.

The provisions in Section 24 prescribe the punishment of a fine ranging between NGN7 million and NGN25 million and imprisonment ranging between one and ten years—depending on the severity of the offence. There have been high profile cases of online journalists and commentators charged and prosecuted for content published or comments made online.[37] This has affected stories and comments published online that have been deemed "offensive", "obstructive", "insulting", or "annoying" with actionable consequences under Section 24 of the Cybercrimes Act even when the stories are factual and accurate. Restrictions on content published or comments, even if they are false, risk censorship of the public and stifles free speech.

2.3.3. FOI Act

The Freedom of Information Act, 2011 ("FOI Act") was enacted[38] to:

- make public records and information more freely available;
- provide for public access to public records and information;
- protect public records and information in line with the public interest and the protection of personal privacy;
- protect serving public officers from adverse consequences for disclosing information without authorisation; and
- establish procedures for the achievement of these objectives.

This is important legislation for the promotion of open data initiatives in the public sector.

The FOI Act supersedes the Official Secrets Act, originally enacted in 1911, which forbade the unauthorised transmission, obtaining, reproduction, or retention of any classified matter. The FOI Act applies not only to public institutions but also to private organisations providing public services, performing public functions or utilising public funds.

The Act still has its challenges due to the number of exemptions provided that allow the delay or refusal of disclosing public information. Some of these exemptions are justified, e.g. protecting privacy or the right to a fair trial and for criminal investigations. However, the exemptions for "international affairs and defence", "law enforcement and investigation", or "third party information" can be used as a catch-all to prevent disclosure by public officials.

A more practical challenge with the FOI Act highlighted by a stakeholder was the difficulty of complying with FOI requests. The poor culture of record-keeping, maintenance and capacity challenges in many public institutions, frustrating and time-consuming bureaucracy, the politicisation of information and ignorance around the provisions of the FOI Act prevent effective implementation of the legislation.

> **"The Official Secrets Act is what you are given when you join the public service. You are told that you are bound by the Act."** - Public Sector Stakeholder

2.3.4. Communications Act

The Nigerian Communications Act 2003 ("Communications Act") established[39] the Nigerian

Communications Commission ("NCC") as the body responsible for regulating the communications sector in Nigeria. As part of its regulatory oversight, the NCC requires providers of a range of services to obtain a licence that grants them the authority to engage in a telecom business or provide telecom services. These services, among others, include; sales and installation of terminal equipment (mobile cellular phones, satellite communication etc.); internet services; prepaid calling card services; paging services; fixed telephony services (employing cable and radio); satellite network services; repairs & maintenance of telecommunications facilities; cabling services; telecentres/cybercafes and non-commercial/user-operated radio networks.

The Communications Act also expressly provides for matters that are in the national interest (Sections 146–149). These require licensees to prevent the use of their facilities or services to commit any offence under any law in operation in Nigeria and allow the NCC or any other authority to assist as far as reasonably necessary to prevent an offence, including for the preservation of "national security". Licensees are protected by the Communications Act from any liability while carrying out this duty.

> **"A Data Protection Act will provide very clear rules because the rules in Government can be very inconsistent."** - Public Sector Stakeholder

It further allows the NCC to require a licensee to implement the capability to allow authorised interception of communications (under Section 147) and for the NCC to suspend licenses; take temporary control of services or networks; order the disclosure, interception or prevention of specified communications; or take possession of network facilities, service, or customer equipment. These are justified by national interest and national security, which can be open to interpretation and thereby abused.

Since its establishment, the NCC has issued the following regulations:

- **Consumer General Code of Practice, 2007** governs how licensees collect information on individual consumers and the policies to ensure proper collection, use and protection of the information they collect.
- **Registration of Telephone Subscribers Regulations, 2011** requires licensees to capture subscriber information and transmit this information to a central database maintained by the NCC. Security agencies can access this database by written request.
- **Nigerian Communications (Enforcement Process, etc.) Regulations, 2019** require a licensee to keep records of call data per the Cybercrimes Act and the Consumer Code Regulations. Any authority may access basic information with a written request signed by a police officer (at or above the rank of an assistant commissioner or equivalent). In contrast, non-basic information requires a court order.
- **Lawful Interception of Communication Regulations, 2019** governs the conditions in which communications in Nigeria may be intercepted, collected and disclosed. The regulations make it an offence to intercept any communication in Nigeria except by an authorised agency.

These regulations are essential as most online communications and activity are conducted via mobile phones and networks, so they rely on telecommunication networks and their providers. However, their effectiveness in protecting data and digital rights may be limited by the provisions of the Communications Act that allow the government either through the NCC or an authorised agency to intercept, surveil or take control of network services for national security or matters that are in the national interest.

2.3.5. NDPR

The National Information Technology Development Agency (NITDA) was established under the NITDA Act, 2007[40] as the national authority for planning, developing, and promoting information technology in Nigeria. NITDA issued the Nigeria Data Protection Regulation ("NDPR") in January 2019 to regulate and control the use of data in Nigeria.

The NDPR applies to all transactions intended to process personal data of natural persons residing in Nigeria or Nigerian citizens residing in foreign jurisdictions. Based on the NDPR, data processing includes collecting, recording, storage, retrieval, use, disclosure, transmission, erasure and destruction of personal data. The NDPR also confers explicitly

certain rights on persons that data relates to, i.e. Data Subjects. These include the right to information about their data, the right to access data about them, the right to rectify data about them, the right to withdraw consent, the right to object, the right to data portability, and the right to be forgotten.

> **"There needs to be better enforcement of the rules like the NDPR, and this enforcement should be visible, not just to pay lip-service."** - Academic Researcher

In terms of compliance requirements, the NDPR requires Data Controllers (organisations and institutions that hold the personal data of Data Subjects) to develop adequate security systems to protect data within their custody. In line with this requirement, Data Controllers must maintain and publish a data protection policy that conforms with the NDPR and continually train and build the capacity of staff members on data protection and privacy procedures. The NDPR also requires Data Controllers to appoint Data Protection Officers to comply with the regulations.

Data Controllers require lawful consent of Data Subjects before processing their data. They are required to display a simple and obvious privacy policy on any medium through which they collect or process personal data. This policy should contain a description of the kind of personal data to be collected and the purpose of collecting the data, amongst other information. Such privacy policy must also govern any contractual engagements between a third party and the Data Controller.

Other provisions cover Data Controllers conducting an audit on the data privacy policies of their organisation. Only Data Controllers that process data on more than 1,000 Data Subjects within six months are mandated to file a soft copy of the summary of their audit with the NITDA. Data Controllers that process data on more than 2,000 Data Subjects within 12 months are mandated to file a summary of their audit with NITDA no later than March 15 in the following year.

NITDA also requires a verification statement by a licensed Data Protection Compliance Organisation (DPCO) that should accompany all filings made. A DPCO is any entity licensed by NITDA to train, audit and render consulting services and other services and products for compliance with the data protection laws applicable in Nigeria. A list of licensed DPCOs can be found on NITDA's website,[41] which predominantly includes professional services firms such as accounting and law firms with data protection practices.

The consequences for failure to comply with the regulation are: (i) a fine of 2% of a Data Controller's Annual Gross Revenue or NGN10 million, whichever is greater (if the Data Controller processes data on more than 10,000 Data Subjects); or (ii) a fine of 1% of a Data Controller's Annual Gross Revenue or NGN2 million, whichever is greater (if the Data Controller processes data on less than 10,000 Data Subjects).

Since the implementation of the NDPR, observers believe it has had little effect on data protection in Nigeria.[42] The regulation is still seen as a partial instrument because NITDA's core mandate is to expand a "regulated" digital market and the agency sits under the Ministry of Communications and Digital Economy.[43] Therefore, NITDA is not an independent regulator. This is particularly critical when dealing with data protection violations by the government or government institutions. Furthermore, as secondary legislation, the regulation still ranks below primary legislation.

2.5.6. Other Laws and Regulations

Further relevant laws and regulations that influence the data and digital rights framework in Nigeria are outlined below.

NIMC Act

The National Identity Management Commission ("NIMC") Act, 2007 created NIMC to establish and manage a National Identity Management System ("NIMS"). NIMC is responsible for enrolling citizens and legal residents, creating and operating a National Identity Database and issuing Unique National Identification Numbers ("NIN") to qualified citizens and legal residents. Section 26 of the NIMC Act provides that no person or corporate body shall have access to data or information in the database concerning a registered individual without authorisation from the Commission. The Commission is empowered to provide a third party with information recorded in an individual's database entry without the individual's

consent, provided it is in the interest of national security.

> **"Mandatory SIM card registration has been an issue in data and digital rights. The process for encouraging enrollment should not be by disconnecting people."**
> - CSO

NIMC has faced several legal challenges in its rollout. In 2019, Paradigm Initiative brought a court case against the Commission for attempting to roll out the programme without a sufficient data protection framework to manage it. The mandatory enrollment and use of a NIN without a comprehensive data protection framework leaves citizens open to a breach of highly sensitive information and no room for recourse. Citizens who did not comply with the registration can be denied access to essential services (most recently in 2020—this threat included cutting off the phone lines of registered phone users without a NIN).[44]
According to the World Bank, the enforcement of digital identity programs must be "rooted in an upgraded legal framework", with "clear definitions for the interconnectivity and interoperability with other registries".[45] It should also safeguard against the risk of increased rent-seeking—manipulating public policy for profits—behaviour during registration. Data and digital rights stakeholders believe that NIMC has not upheld these principles.

Credit Reporting Act

The Credit Reporting Act, 2017 establishes a legal and regulatory framework for credit reporting by Credit Bureaus. To ensure confidentiality and protect the subject's information, Credit Bureaus are compelled to keep their data safe, secure and confidential. It prevents the disclosure of credit information received from a Credit Bureau to any person, or use of such information for any purpose other than a permissible purpose, except with the written consent of the Data Subject and unless such disclosure is required by applicable law, court order or by the CBN; and where the Data Subject is involved in financial or credit-related malpractice, e.g. the issuance of dishonoured cheques.
The Act also gives data subjects the right to request the correction of credit reports, which may be false or inaccurate, by providing additional information to rebut disputed information or support additional claims. Furthermore, a credit bureau that gathers information from providers that appear to be untrue must take the necessary steps to verify such information.

Child Rights Act

This Child Rights Act, 2003 reiterates the constitutional right to privacy as it relates to children. Section 8 of the Act guarantees a child's right to privacy subject to a parent or guardian's right to exercise supervision and control their child's conduct. Some Nigerian states have also enacted Child Rights Laws. Like many jurisdictions, these rights have not been tested online, so it is unclear how they are applied to control and manage data collected on children by technology companies through mobile and web applications.

Consumer Protection Framework

The Consumer Protection Framework, 2016 was enacted under the Central Bank of Nigeria Act 2007. The Framework contains provisions that prohibit financial institutions from disclosing customers' personal information. The Framework further requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data. Financial services providers must obtain written consent from consumers before personal data is shared with a third party or used for promotional offers. The Consumer Protection Framework has been implemented, but there has not been much activity around data protection as it has primarily been used to dispute charges by Financial Service Providers.

Health Act

The National Health Act, 2014 ("Health Act") provides rights and obligations for health users and healthcare personnel. Under the Health Act, health establishments are required to maintain health records for patients of health services and maintain the confidentiality of such records. The Health Act further imposes restrictions on the disclosure of patient information. It requires persons in charge of health establishments to set up control measures for preventing unauthorised access to information. The Health Act applies to all information relating to patient health status, treatment, admittance into a health establishment and further applies to DNA samples collected by a health establishment.

2.4. Designing Data & Digital Rights Legislation

The laws and regulations outlined in this section refer to free speech and data protection but are not primarily designed to address data and digital rights directly. For this reason, many of the laws and regulations have not had a significant impact on protecting data and digital rights.

Issues with the implementation of specific laws and regulations partly explain the limited impact they have had. A UN report notes that there is "weak institutional capacity for effective implementation and monitoring of child rights issues and programmes" regarding the Child Rights Act.[46] Similarly, stakeholders interviewed noted that NIMC had no funding source, limiting its ability to perform effectively. This means that these laws and regulations are not used to effectively redress data protection breaches.

A critical advocacy effort to improve the data and digital rights legal framework in Nigeria has centred around implementing the Data Protection Bill.[47]

> **"If I was a member of the National Assembly, I would question why we need a huge organisational infrastructure to run the data protection agency."** - Public Sector Stakeholder

The Data Protection Bill is a proposed Act to establish a Data Protection Commission responsible for protecting personal data, rights of data subjects, regulation of the processing of personal data and other related issues. It attempts to design a law specifically focused on data and digital rights and create institutional capacity for effective implementation.

To understand the process for its enactment, the legislative process for enacting laws—as set out in the Nigerian Constitution—is outlined below.

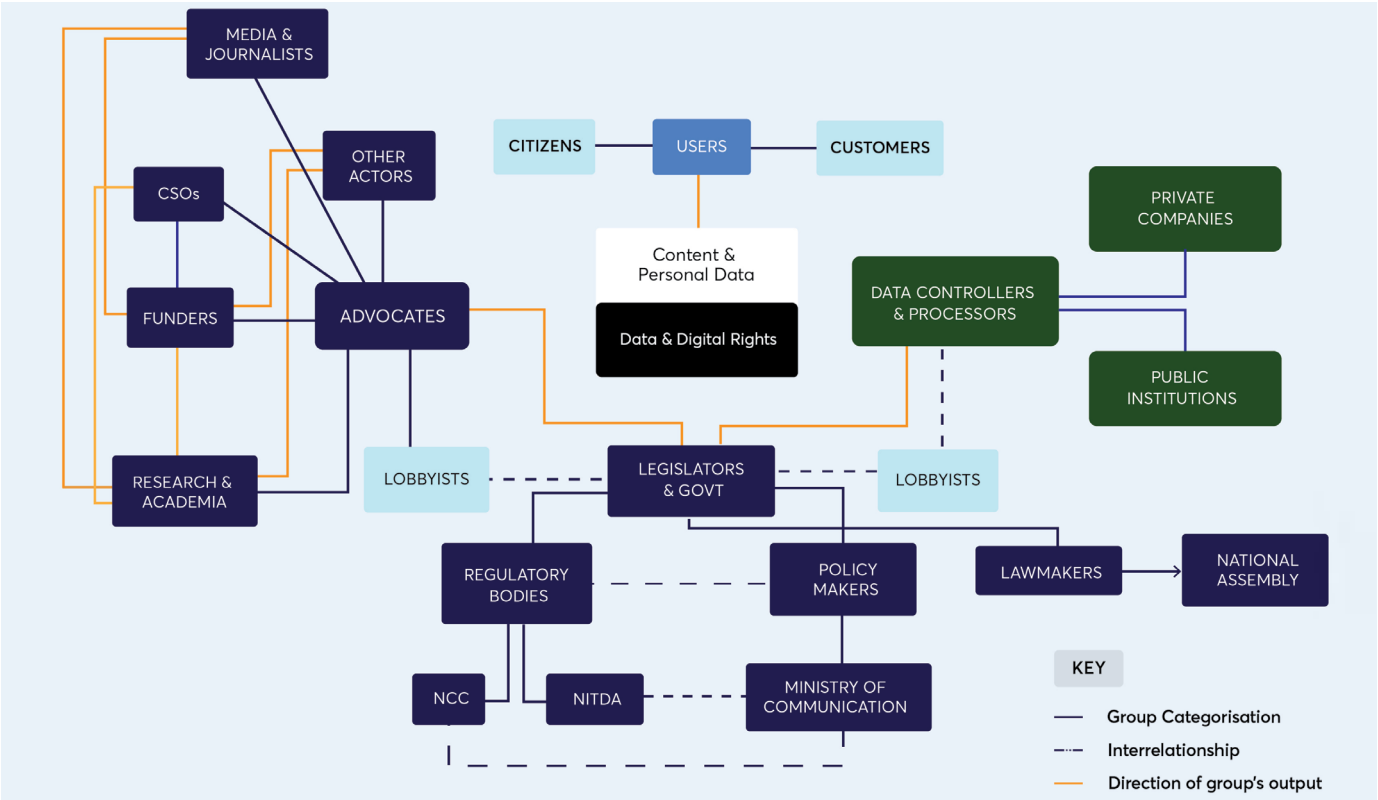
PROCESS FOR ENACTING LEGISLATION IN NIGERIA

First & Second Reading → Standing Committee Stage → Report & Committee Stage → Third Reading → Engrossment

1. **First Reading:** The Clerk of the House or Senate reads the short title of the Bill and tables it before the Speaker or the Senate President (whichever is applicable).
2. **Second Reading:** The second reading gives the members sufficient time to deliberate on the general principles of the Bill (for example, its merits and demerits). At this stage, legislators can decide to approve or reject the Bill.
3. After the second reading, and provided that the Bill was not rejected at that stage, the Bill will be passed to a Standing Committee for thorough scrutiny.
4. The Standing Committee will conclude extensive deliberations on the Bill, which can include arranging for a public hearing and requesting contributions from experts on the subject matter of the proposed law.
5. **Report stage:** After the Standing Committee has concluded its work, it will set a date on which to present its findings to the House or Senate. The Chairman of the Standing Committee will conduct the report on the Bill.
6. **Whole Committee Stage:** At this stage, the Presiding Officer will call out the number of every clause in succession or the first and last number of a group of clauses. If there are proposed amendments, they will put them forward.
7. Corrections and amendments can be made at this stage if there are errors or oversights that have occurred during the Bill's journey.
8. If a legislator wishes to suggest an amendment, they must make a motion that the Bill be "re-committed" to the committee stage for the amendment to be included. After all necessary amendments have been made, the House or Senate proceeds on the third reading and passes the Bill.
9. Engrossment involves the production of a final clean copy of the Bill by the legal department after all of the amendments agreed to by the legislators have been made.
10. The Bill will be drawn up in the proper legal draft format and sealed with an authenticated certificate endorsed by the Clerk of the House or Senate. The Bill is then presented to the Chief Executive (President or governor of a state) for their assent or otherwise.

3. Stakeholder Map

DATA & DIGITAL RIGHTS STAKEHOLDER MAP



3.1. Advocates

The advocates category of data and digital rights includes civil society organisations ("CSOs"), researchers and research institutions. CSOs considered for this report identify and support advocacy in the data and digital rights space. Their work predominantly focuses on freedom of expression, data protection and privacy. Organisations include the Paradigm Initiative, BudgIT, Digital Rights Lawyers Initiative and Amnesty International (Nigeria).

Researchers and research institutions include academic researchers and lawyers identifying emerging issues on data and digital rights, e.g. through regulatory reviews or field research. The stakeholders engaged for this report included individual researchers and representatives from Tope Adebayo LLP, OAL Law/Human Rights Law Service, Research ICT Africa, African Academic Network On Internet Policy ("AANOIP") and the Digital Rights Lawyers Initiative ("DRLI").

While the involvement of local organisations in advocacy has been growing, it is essential to note the prevalence of international organisations in the CSO group. The stakeholders interviewed highlighted resource constraints as a primary limitation for the involvement of local organisations. One specific challenge faced by local organisations was setting the priorities or focus for data and digital rights issues. This stems from the fact that funding organisations, predominantly international organisations, have set agendas and priorities for disbursing funds. As a result, local organisations seeking funding define projects that fall within a funder's priorities, which may not align

with local priorities.

Another concern expressed by smaller CSOs and advocacy groups was the inability to access more considerable funds compared to established organisations. Due to the established track record of organisations such as Paradigm Initiative or BudgIT, they are more likely to attract more significant disbursements from funding organisations. As a solution, some stakeholders expressed an interest in collaborations between smaller or niche groups and larger CSOs on projects with larger grants. An example of this was the recent collaboration between the Paradigm Initiative and Digital Rights Lawyers Initiative on providing legal support to EndSARS cases.

STAKEHOLDER SPOTLIGHT

Paradigm Initiative

Paradigm Initiative is a social enterprise that builds ICT-enabled support systems and advocates for digital rights to improve livelihoods for under-served youth. Its programs include digital inclusion programs for life skills, ICT and financial readiness. In 2013, it established an ICT Policy Office in Abuja to focus on internet freedom. Paradigm Initiative has been involved in litigation against public sector actors. For instance, in 2016, along with the Media Rights Agenda and Enough-is-Enough, it instituted a matter at the Federal High Court, Lagos, against the National House of Assembly due to the harsh punitive measures of the bill dubbed the Social Media Bill against freedom of expression online.

They also publish policy briefs on internet freedom, cybersecurity, internet access and data privacy. The briefs aim to raise awareness, identify structural policy issues and recommend possible actions to policymakers and legislators. Beyond internet freedom, other digital rights work includes training non-profit organisations and educational institutions to use ICT for digital security, online and social media advocacy.

BudgIT

BudgIT is a civic-tech organisation that improves access to public data in Nigeria by simplifying the government budget and publicly available data. This is done by providing line-item breakdowns of budgets and spending to aid probing and analysis with the ultimate goal of increasing the standards of transparency and accountability in government.

Tracka is a tool developed by the organisation to allow citizens to self-report the status of ongoing public sector projects and extractive transparency, a unit BudgIT runs, works closely with extractive sectors of the economy, i.e. gas, minerals, mining industries, to understand the output of these sectors. BudgIT also operates an open government unit where it supports government institutions with openness in their service delivery. The organisation's overall goal is to improve the accessibility of data, enabling citizens to use the data at their disposal to make demands of the government and take action.

Amnesty International

Amnesty International (Nigeria) is a CSO that conducts investigations on human rights abuses. They acknowledge the additional challenges the digital frontier presents to the protection of human rights. In 2014, Amnesty International and a coalition of human rights and technology organisations launched 'Detekt'—a simple tool that allows activists to scan their devices for surveillance spyware.

Amnesty International has led campaigns on data and digital rights in Nigeria, specifically on freedom of expression online. Recently, it has been at the forefront of campaigns against the Social Media and Hate Speech Bills, highlighting them as attempts to cripple freedom of speech. They release written and video reports and recommendations to educate and draw attention to these issues. The organisation does not directly engage with the Nigerian government. However, there have been attempts to discredit them by the military, online trolls and sponsored protestors who act as a nuisance outside of their office spaces.

Digital Rights Lawyers Initiative

Digital Rights Lawyers Initiative (DRLI) is an organisation focused on supporting strategic litigation in Nigeria that will have a lasting impact on the rights of Nigerian citizens. They are a network of over 200 lawyers that advocate for digital rights and are involved in upskilling lawyers in digital rights which remains an emerging sector globally.

Their litigation efforts focus on data protection, freedom of expression online and digital rights, with almost 40 cases currently filed in courts across the country. The organisation also has an interest in cases around internet shutdowns, cryptocurrency and consumer rights online. DRLI also works with other advocate groups on litigation. For instance, in the aftermath of the EndSARS protests, the organisation worked with the Paradigm Initiative on filing court cases and providing legal defence to protesters.

CcHub

Co-creation Hub (CcHub) is an innovation centre dedicated to accelerating social capital and technology for economic prosperity. For data and digital rights, it operates a unit, GovLab, which focuses on digital security.

CcHub engages public and private institutions that handle data to incorporate safety features into their data products—encouraging a privacy by design approach to developing consumer technology software and products. For example, the organisation has worked with financial services companies to educate customers on safely using digital products to protect them from online fraud, cybercrime and state or non-state surveillance.

3.2. Funders

Funding organisations support advocacy by providing grant funding and other forms of indirect support to stakeholders in the data and digital rights space. This includes supporting advocacy, litigation and policy-making efforts by stakeholders. The organisations engaged for this report include the Ford Foundation, Omidyar Network, MacArthur Foundation and Access Now.

Funding for data and digital rights has shown signs of growth, with organisations such as the Ford Foundation expressing intentions to fund more partners in Nigeria. However, some of these plans had been delayed due to the coronavirus pandemic in 2020. The CSOs interviewed expressed a desire to have access to more funds for their work, but most believed they could access the essential funding needed to operate.

As previously noted, most of the funding for the data and digital rights work in Nigeria originates from international organisations. This, in turn, dictates the issues that get prioritised. There is a need for funders to diversify the scope of their funding or provide more flexibility in their grants. In the past, grants have typically been on a per-project basis, but many CSOs believe that this structure gives little room for testing ideas and core support. Some organisations, such as the Ford Foundation and the Omidyar Network, have responded by granting discretionary funding for grantees to use as they see fit.

Another concern raised by funding organisations was supporting smaller advocacy groups and CSOs due to their legal structures and financial capacity to manage grants. A stakeholder interviewed believed attempts by funding organisations to manage grantee funds was not an appropriate solution to this problem as it increased administrative bureaucracy and dependence.

Instead, a few stakeholders believed a shift in the mindset of funders was needed. They argued that smaller grant opportunities should be seen as investments with high risk and high reward—allowing for more mistakes and creative approaches. From this view, the kinds of support required by smaller CSOs and advocacy groups should focus on providing training and resources that reduce bureaucracy and encourage independence.

STAKEHOLDER SPOTLIGHT

MacArthur Foundation

MacArthur Foundation is a funding organisation that supports creative people, effective institutions and influential networks to build a more just and peaceful world. It makes a few big bets on areas where the foundation believes that truly significant progress is possible. This includes social challenges such as advancing global climate solutions, decreasing nuclear risk, promoting local justice reform in the U.S. and reducing corruption in Nigeria.

The foundation supports Nigerian-led efforts to improve transparency, accountability and participation. In data and digital rights, they primarily focus on the upskilling and protection of journalists, freedom of speech online, surveillance and protecting the space for civic discourse.

Journalists in Nigeria are vulnerable to digital attacks and laws aimed at gagging the free press. The MacArthur Foundation has received feedback from grantees to cover specific issues such as threats to control social media to gag alternative opinions. This feedback, along with considerations for an alternative funding model, will be considered in its next phase of grant-making.

Ford Foundation

Ford Foundation is a private funding organisation that focuses on social justice. Globally the foundation works on a broad range of issues from civic engagement and government; the future of work(ers); gender, racial, and ethnic justice; technology and society; to natural resources and climate change. For data and digital rights in Nigeria, the foundation primarily supports three partners—Paradigm Initiative, CcHub and BudgIT—on various initiatives. The foundation works with Paradigm Initiative to support public interest policy, advocacy and opportunities for social justice. It also works with CcHub to provide technical assistance on digital security projects for consumers and BudgIT to support its open data and open government work. The Ford Foundation also works with African Internet Rights Alliance to support regional collaboration in the region. This provides opportunities to engage with influential partners at the Economic Community of West African States (ECOWAS) and the African Union.

As part of its technology and society programme, which centres around the rules for fair use of technology, the foundation will work on digital resilience for social justice organisations. It also plans to increase its financial commitment to CcHub by launching other technology and society initiatives, but this depends on its current human resource and capacity constraints.

Omidyar Network

Omidyar Network is a funding organisation that works to bring about structural changes that will fundamentally shift the systems that govern people's daily lives. Concerning data and digital rights, the organisation's work on Responsible Technology focuses on making strategic investments. It promotes ideas, technologies, and policies that help ensure a digital world that is safe, fair, and compassionate.

In Nigeria, Omidyar Network directly funds the Paradigm Initiative and Digital Rights Lawyers Initiative. The support for Paradigm Initiative centres on their advocacy work on implementing a digital identity system by NIMC. They also receive support for litigation efforts to suspend the progress of bills that do not align with human rights agendas, such as the Social Media Bill and the Hate Speech Bill. The Digital Rights Lawyers Initiative is a recent grantee of the Omidyar Network that has received core funding support.

Outside of these two direct grantees, the Omidyar Network indirectly supports grassroots advocacy groups through sub-grants. One example is its grantee CIPESA, which offers flexible and rapid response grants through the Africa Digital Rights Fund to select initiatives to implement digital rights activities.

Access Now

Access Now works to defend and extend the digital rights of users at risk around the world. This is done through evidence-based policy analysis, advocacy and global partnerships with civil society and journalists; educating, petitioning and appealing to decision-makers; and flexible grantee-driven

funding to grassroots organisations. The majority of Access Now's funding comes from foundations and development agencies, which includes the Swedish International Development Agency ("SIDA"). These are granted to others through Access Now Grants.

Access Now also organises RightsCon, a yearly event that brings together business leaders, policymakers, lawyers, advocates, technologists, academics, government representatives, and journalists from around the world to tackle the most pressing issues at the intersection of human rights and technology.

In Nigeria, Access Now collaborates with local partners to support them with running campaigns and events. Recently, Access Now wrote an open letter to appeal to the Nigerian government in the wake of EndSARS and the threats of internet shutdowns. The organisation has expressed an interest in supporting strategic litigation through amici curiae briefs, but this is currently not permitted in Nigerian courts—but can be submitted in the ECOWAS Community Court. An amicus curiae brief is a legal document supplied to a court of law containing advice or information relating to a case from a person or organisation that is not directly involved in the case.

3.3. Regulators

Regulators and policymakers are responsible for the regulation and enforcement of data and digital rights laws. In Nigeria, the primary regulators of data and digital rights—the NCC and NITDA—are agencies under the Federal Ministry of Communications & Digital Economy. The Ministry was established to facilitate ICT as a critical tool in the transformation agenda for Nigeria in job creation, economic growth and transparency of governance.

Stakeholders noted several successes and challenges in the regulation of data and digital rights. Specifically, the regulators believe they can and have ensured compliance by other government agencies/ bodies with relevant regulations through strategic collaboration and partnership. Where necessary, they apply sanctions to ensure compliance.

One challenge expressed was the skill and knowledge gap the agencies under the Ministry of Communications & Digital Economy possessed to effectively regulate the digital economy. Given the pace of innovation and adoption of new technologies, regulators require frequent training and upskilling to keep up with trends. Specific needs expressed by regulators include capacity building in data security, cybersecurity, cybercrime and related laws and regulations.

Regulators in Nigeria are also critically underfunded and cannot enforce any of the regulations and standards that they set. Even when a new bill has been passed into law, implementation and enforcement is an important aspect. Where the public bodies charged with doing so cannot enforce the rules, their effectiveness is weakened. This is a significant constraint for proper data protection implementation—and it continues to be a problem given the government's development priorities. A stakeholder noted that some efficiency improvements in regulatory bodies and agencies might be a better bet for relieving the constraints to implementing legislation as government agencies—like other parts of the world—tend to be underfunded.

In addtion to requiring additional funding from the government, regulators note that they are unable to secure donor support and multilateral funding, which would otherwise increase resources for reaching a broader segment of the population.

STAKEHOLDER SPOTLIGHT

Nigerian Communications Commission

As noted in the legal and regulatory landscape, the Nigerian Communications Commission is responsible for the regulation of the telecommunications industry in Nigeria. The independence of the NCC is enshrined in the Communications Act, and it is a revenue-generating agency. It does not outrightly depend on government's funding for the implementation of its regulations.

Currently, the NCC is participating in the drafting of the Data Protection Bill to be forwarded to the National Assembly for consideration and subsequent passage into law. The NCC is a member of the technical committee, which is finalising the draft Bill. The NCC has also recently commenced drafting a data protection regulation for the country's telecoms industry.

According to the Commission, the primary risks that hinder its growth include the vandalism of telecommunications infrastructure, fibre cuts and infrastructure theft due to heightened insecurity, and financing telecommunications projects due to the industry's capital-intensive nature.

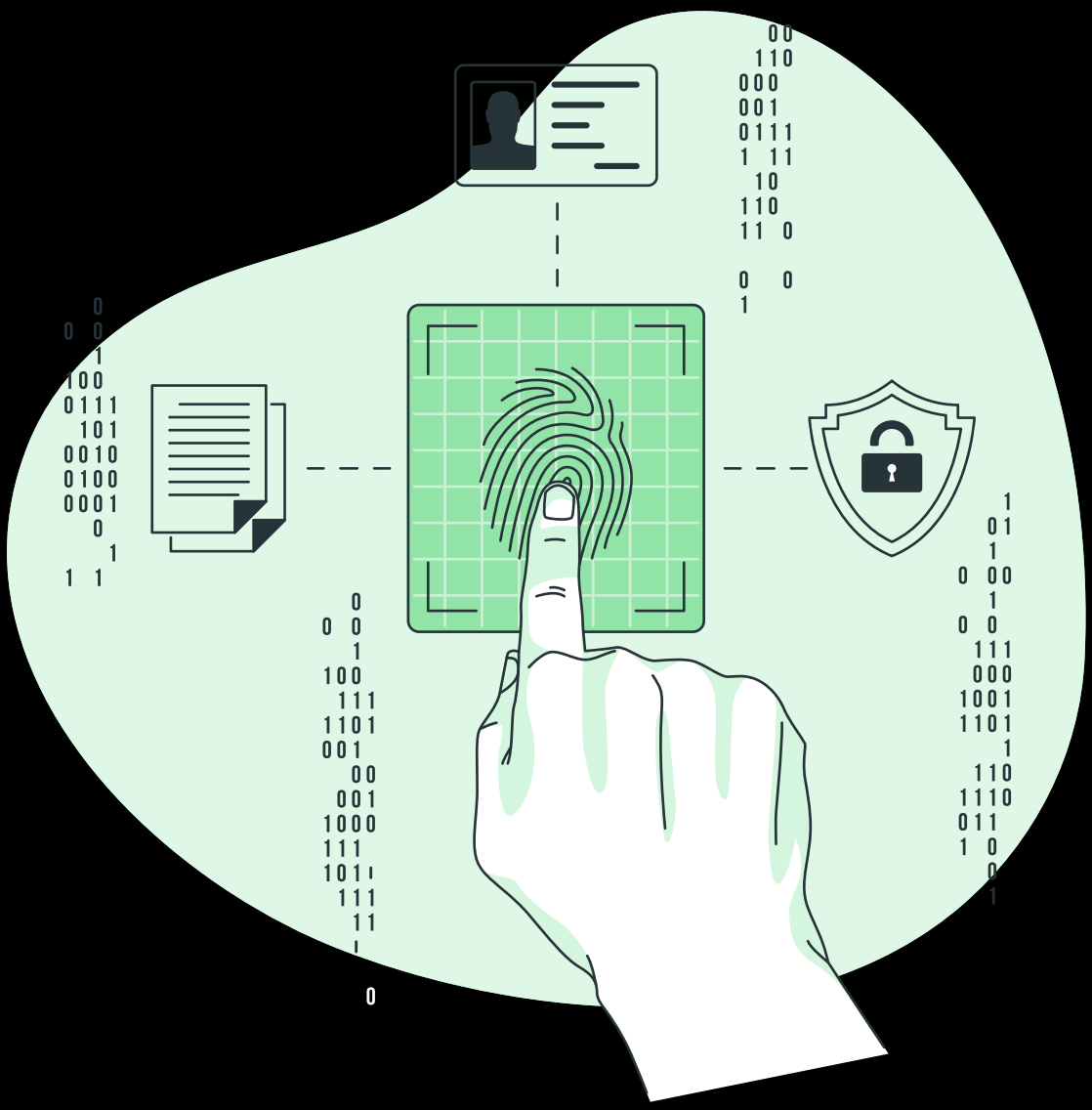
3.4. Data Controllers & Processors

Government institutions, public bodies, and private companies are responsible for controlling and processing data about users in the country. Relevant government institutions include the identity management body, tax collection agencies, immigration services, the central bank and other financial services regulators. In the private sector, the most significant data controllers and processors are telecommunication companies, financial services firms, banks and technology companies that collect data regularly from their customers and users for various purposes.

Recently, NITDA has imposed fines on government agencies and private companies for data breaches. In 2020, the agency fined the Lagos State Internal Revenue Service (LIRS) NGN1 million for a breach of taxpayers' data. This was allegedly the result of a glitch on the tax collection websites where taxpayers' personal information was exposed to the public. More recently, in March 2021, NITDA announced that it had imposed a fine of NGN5 million on Electronic Settlement Limited for personal data breach following a 16-month investigative process.

CSOs and advocacy groups have expressed reservations over NITDA's ability to set appropriate fines for violations of victims' data protection regulation and compensation. DRLI, for example, filed suit against both LIRS and NITDA on the 2019 data breach seeking orders mandating NITDA to fine LIRS as provided under the NDPR to the tune of 2% of their annual gross revenue. This, however, did not affect the eventual fine imposed on the LIRS.

Other data and digital rights violations highlighted were by private companies in the telecommunication sector, with ongoing issues such as selling customer data for commercial use. There are also interactions between telecommunications companies and government agencies that raise concerns as provisions in specific laws stipulate that telecommunications companies can hand over customer information extrajudicially, leaving room for abuse of power.



4. Developing Issues for Data & Digital Rights

4.1. Data Rights

4.1.1. Data Protection

Data protection is a contentious issue in Nigeria. This is largely because there is no comprehensive data protection law in Nigeria, and better regulatory oversight is needed. Many of the stakeholders interviewed identified data protection as one area that cannot be ignored.

Government databases are high risk

According to some stakeholders, the Nigerian government has not been proactive in addressing data protection concerns.[48] The government has often asked citizens to provide increasing amounts of personal data, with no comprehensive legal framework for managing it. NIMC has come under fire for attempting to establish a digital identity system using biometric data. Without appropriate legal protections in place, this leaves citizens vulnerable to interference with their digital identity and with limited room for redress.

> **"The primary person of influence for data protection in Nigeria is the Minister of Communications and Digital Economy."** - Academic Researcher

Paradigm Initiative filed a court case against NIMC to address this issue. Although the judgement was not in Paradigm's favour, the judge affirmed that data protection for digital identity needed to be implemented more robustly. This motivated the introduction of the Data Protection Regulation. However, Privacy International notes that it is only a partial instrument. The enforcing agency—NITDA, sits under the Ministry of Communications and lacks the independence to sufficiently monitor and penalise breaches.[49] Given a fair amount of citizen data breaches are perpetrated by the government agencies and departments, there is an apparent conflict of interest.

Many stakeholders pointed to instances where government departments have gone further in mismanagement, crossing over to breach of citizen's private data by publishing sensitive information on public forums. For example, one stakeholder recalled an instance in 2016 when voters' data was publicly displayed on the Independent National Electoral Commission (INEC) website.

Another recent incident under investigation by NITDA was the publication of a Nigerian citizen's details by the Immigration Service as punishment for allegedly vandalising property in the Nigerian High Commission in London.[50] More recently, in 2021, the Presidential Task Force published the passport details of 100 travellers as a penalty for failing to take a repeat Covid-19 test upon entry into the country.[51]

CSOs such as the Paradigm Initiative and the DRLI strive to hold the government to account through strategic litigation. A large number of their cases have been targeted at government agencies. However, the judgements in these data protection cases are often unfavourable as the jurisprudence around data protection and online privacy in Nigeria is still underdeveloped. More test cases are needed to understand how to balance competing rights and legislation. Currently, many lawsuits filed by CSOs are still pending and can take years for a resolution, so the full impact of strategic litigation is yet to be uncovered.

Judicial oversight for national interest exemptions

Researchers and lawyers in the stakeholder group also identified a gap in judicial oversight for breaches in data protection. Limited judicial oversight provides room for abuse of power. Security agencies are currently able to collect customer information from telecommunication providers without a court order. There are provisions in existing legislation that provide exemptions for accessing data for security purposes—the Communications Act and the National Communications Commission Regulations, 2011 are two examples.

However, even where a court order is required, this requirement is not always adhered to—for example, security agencies search mobile phones and laptops of those in their custody.[52] Consequences for these breaches are even rarer. In cases that have been taken to court, the pace of the Nigerian judicial system means that getting a judgement for a violation of data privacy rights could take years to resolve. Civil society and individual cases against government agencies have involved NITDA, the NCC and even the National Assembly. There are no specific laws in Nigeria that allow or prohibit litigation against government agencies. They are treated as institutions or companies.

Digital security for consumer products

Consumer data protection is an area that is also seen as problematic. The practice of telecom providers and private companies selling or repurposing customer data without consent is increasingly prevalent. Bulk SMS platforms offer databases of phone numbers for sale. Data brokerage is illegal, and there have been calls from the public for law enforcement to intervene.

> **"We are concerned about the private sector companies in predatory lending, e-commerce, ride-hailing because there is no oversight on what they are doing."**
> - CSO

The DRLI has been involved in data brokerage litigation with a recent case filed (outcome pending) against LT Solutions & Media Limited in the Abeokuta High Court.[53]

Consumer data protection is also a concern in the financial services industry. A stakeholder identified that many financial services providers create products without incorporating safety features into the product. This mostly comes as an afterthought. Data Subjects (customers) are also not informed on how to use safety features in products at the initial point of use, e.g. being prompted to create a secure password or ensuring that customers do not share sensitive details about their accounts. The lack of strong safety features and sensitisation of customers has led to security breaches.

In 2020, a Cowrywise customer was the victim of a breach, losing millions of naira from their account. The account was accessed with the correct credentials, which suggests that the perpetrator knew the victim personally.[54] This is arguably avoidable with additional safety features such as multifactor authentication or biometric identifiers.[55]

A better model for obtaining informed consent

Some financial technology companies rely on personal data as part of their business models, using it as collateral without informed consent from consumers. For instance, digital lender Sokoloan has received complaints in Nigerian forums for shaming its customers into repaying their loans by messaging individuals on their contact lists. Many of these customers were not aware that the app accessed their contact lists or what it would be used for.[56] Another lender, Migo (formerly KwikMoney), scans the user's contact lists and SMS for any known debtors, using this as a risk assessment.[57]

Although consumers agree to the terms and conditions, many are not aware of the implications of this consent. From a data rights perspective, collecting personal contact data is unnecessary to achieve the aims of processing loans. As such, it should be considered a breach of data protection regulation and the right to privacy. Some lenders argue that they must resort to more creative measures[58] because the risk of default is high in Nigeria. Regardless, these models for compliance are still problematic and rely on a significant invasion of privacy.

4.1.2. Open Data

Open data is data that can be freely accessed, used and shared by anyone for any purpose. As it pertains to governments, open data is a tool that can be used to develop a more responsive government.

Open government and transparency

Open data supports transparency of government activities, making it easier to monitor government spending and activities. The availability of information allows the public to hold the government accountable and tackle corruption. It also promotes efficiency in the public sector by reducing the friction involved with access to data between ministries. Removing this barrier allows governments to plan more efficiently, create better-informed policies, and monitor the impact on different sectors.

Insufficient access to data slows down the work of researchers and journalists who provide critical perspective, argument and analysis of data rights in Nigeria.[59] The inability to access resources for research narrows debate and discourse, stifling progression in academia. Stakeholders that conduct research on data rights spoke of the difficulty accessing a centralised knowledge base and the restrictive budgets provided to access academic materials for research.

Open data can also refer to the availability of laws and discourse in data rights for citizens to educate themselves on their rights, understand when a breach has occurred and engage in litigation when necessary. Nigeria's open data culture still has room to improve, with Open Data Watch ranking the country 87th out of 187 countries profiled.[60] Stakeholders complained of a culture of secrecy that pervades both public and private institutions resulting in limited information and knowledge sharing. It also encourages the use of privacy as a justification against open data.

Balancing openness and privacy

Although open data offers benefits to many segments of society, it is argued that open data can threaten the privacy of individuals where personal data is concerned. The complexity of balancing utility and privacy in open data means a one-size-fits-all approach cannot be taken. It should be acknowledged that releasing data carries benefits for the public and potential risks to individual privacy. These risks are inevitable, but governments must protect the sensitive information they possess. What should be considered is an approach that incorporates privacy at each stage of the data lifecycle and not just when releasing open data.[61] Privacy risks can emerge throughout the data lifecycle of collection, maintenance, release, and deletion. Some risks are best addressed at the stage they arise.

Another consideration is whether governments can and should become comfortable with a certain level of risk with open data. It is crucial to conduct risk-benefit assessments on the value of open datasets and if it outweighs the potential privacy risks. However, this only promotes an open data culture to the extent that governments are comfortable taking informed risks. Developing operational structures, processes and security controls for privacy management to mitigate some of these risks may offer some comfort to the government when releasing data.[62] Open data and data protection need not contradict each other as there should be processes and legislation to safeguard the use of data.

Freedom of information in practice

Before enacting the Freedom of Information Act of 2011, the Official Secrets Act of 1962 defined the culture of information flow in Nigeria. This legislation provides for the protection of official information to prevent the disclosure to the public of any matter the government considers classified. Thirty years of military rule further cultivated this culture of secrecy and limited access to public data.

> **"Even after implementing a Freedom of Information Act, it takes a while to see a change in culture."** - Public Sector Stakeholder

Whilst this law has not been repealed, the FOI Act 2011 is intended to supersede it. Public servants have to comply with the FOI Act, which aims to make public records and information more freely available. The implementation of the FOI Act increases the openness of publicly available data. However, it's not enough to reactively respond to requests for data. There needs to be a culture of transparency embedded in public institutions and the promotion of proactive disclosure. It's important to note that although the FOI Act provides for access to publicly available data, this does not imply the accessibility of it. While the

government may argue that it makes data available, the information is not provided in a form that's easy for citizens to understand or engage with—and this needs to be addressed. Some advocates have been working to foster an environment of openness in the public sector, conducting training and capacity building work for financial transparency.

There's commentary that the "third wave of open data" is emerging. The first wave corresponded with the enactment of freedom of information laws—where data is made available on request. The second wave was calling on governments to make their data open by default. The third wave goes further than these, with some of its goals being to match the supply of data with public interests and foster partnerships with NGOs, small businesses, local governments and others to translate data into meaningful real-world insights.[63]

With this in mind, it can be argued that the Nigerian government sits between the first and second waves, with some government data made available to the public, e.g. national economic data is often freely available. Simultaneously, CSOs and advocates have had to invoke freedom of information requests to access other data, e.g. to understand how government agencies are using citizen data.

4.2. Digital Rights

4.2.1. Freedom of Expression

In 2019, President Buhari refused the assent of the Digital Rights and Freedom Bill into law.[64] This law would have extended the protection of human rights for Nigerians to the internet. The refusal was followed by attempts to enact restrictive bills such as the Social Media Bill and Hate Speech Bill.[65] Both of these bills have the effect of shrinking civic space and prohibiting freedom of expression online.[66]

The fear of social media

When engaging with stakeholders, the majority expressed concerns over the recent and growing trend towards censorship in Nigeria. CSOs noted concern over the recent EndSARS protests. It was an example of how repressive techniques could be used to limit public discourse and effectively control what happens online, including using influencer and sockpuppet Twitter networks to amplify pro-government content and mount campaigns targeting activists.[67] These protests inspired renewed interest amongst lawmakers to try and pass the Social Media Bill. The provisions of the Bill in its current form are vague and can be exploited by the government.

For instance, there is a provision against sharing statements "likely to be prejudicial to Nigeria's security, public safety, tranquillity, public finances and friendly relations of Nigeria with other countries." This can be interpreted to prosecute critics of the government and/or its policies. The Social Media Bill passed its second reading at the Senate in 2019 and only needs one more reading to become law.

A threat to activism and journalism

Recently, access to the Feminist Coalition website was removed by various Internet Service Providers in Nigeria, without a court order, under the guise of national security—this is just one example of infringement of freedom of expression that could occur unchecked.[68]

> **"Recent reports and articles on the EndSARS protests have put myself and my team under scrutiny from the government and police force. We have been publicly defamed and are privately being monitored."** - Journalist

Human rights academics have looked into how restrictions on the use of social media platforms can infringe on the right to freedom of expression and understanding the connection between social media and free speech.[69] Although it can be inferred, the Constitution does not directly provide for freedom of expression online, and new legislation should be updated to reflect new technologies. In 2016, the African Commission on Human and Peoples' Rights ("ACHPR") passed a resolution on the right to freedom of information and expression on the internet. But, the ACHPR still requires member states to take legislative measures to guarantee, respect and protect this right. The restraints on freedom of expression make journalists vulnerable and directly impacts freedom of the press. As a result, many journalists are intimidated and arrested for doing their jobs. Some funders have turned their attention to protecting journalists threatened by laws aimed at stifling alternative

opinions. During the EndSARS protests, there were many reports of journalists being arrested, having their equipment confiscated and devastatingly culminating in a news reporter being killed.[70]

Institutionally, the National Broadcast Commission (NBC) appeared to have contributed to stifling free press by releasing a statement advising news stations against broadcasting any information that would lead to the government's embarrassment. It went further to issue fines against AIT, Arise News and Channels TV over their coverage of the protests.[71]

4.2.2. Online Privacy & Surveillance

Over the years, the Nigerian government has continued to expand its surveillance capacity by spending on surveillance equipment as documented in Paradigm Initiative reports.[72]

Building government surveillance capacity

In the 2020 executive budget documents, the office of the National Security Adviser ("NSA") and the Department of State Services ("DSS") reported a combined budget of about NGN5 billion ($13.8million) aimed at purchasing surveillance related equipment.[73] The government's intent to enhance its surveillance capabilities is also reflected in previous federal budgets, which in 2018 allocated NGN4.6 billion ($12.8 million) to the Stranvisky Project 2 and an Office of the National Security Adviser ("ONSA") project that was allocated NGN13.9 billion ($45.6 million) in 2017.[74] Observers believe these projects have been for new surveillance technology as several other line items in the 2018 budget for the ONSA and Department of State Security include the "Social Media Mining Suite," with an allocation of NGN2.2 billion, and "Mobile Surveillance Facilities" with NGN240 million allocated, among others. Government officials frequently assert that new technology is acquired to fight the Boko Haram terrorist group, but these capabilities may also be unknowingly used on other citizens.

Overextension of the Cybercrimes Act

Legislative instruments have also been used to justify the invasion of privacy of Nigerians. Similar to the Social Media and Hate Speech bills, vaguely drafted provisions leave room for abuse. The Cybercrimes Act includes a "Cyberstalking" provision that has been used as a justification to detain and harass journalists that criticise the government.[75] The provision in Section 24 (detailed above) has the effect of gagging freedom of expression online. It cultivates a hostile environment for journalism and political commentary.

Another issue raised by stakeholders is that the Cybercrimes Act does not specify what type of crime permits interception, which means that surveillance can be conducted for minor offences. In addition, the Communications Act makes it mandatory for network service providers to assist authorities in preventing crime and protecting national security.[76] It also grants senior police officials the power to obtain call data from telecommunications companies without a court order.[77]

> **"Nigeria isn't particularly great when it comes to press freedom and many journalists have been arrested and intimidated for simply doing their jobs."**
> - Journalist

One of the main targets of surveillance and interception are journalists. Stakeholders reported that they feared surveillance and monitoring by the government, with some going into hiding for publishing certain articles after receiving threats from the government. A prominent illustration is the case of Samuel Ogundipe, a journalist at Premium Times. He was unlawfully detained and charged in 2018 for refusing to reveal his source for an article published on the inspector-general of police. The police had a file with his bank statements and phone records, which had been provided by his bank and telecoms provider. In 2020, the Committee to Protect Journalists ("CPJ") reported that he was forced to go into hiding after receiving threatening phone calls, strangers lurking around his home and then a warning from a source that he may be arrested.[78]

During the EndSARS protests, prominent online activists spoke up about receiving threats directed towards them or their loved ones, their bank accounts and phone lines being blocked, as well as their passports being seized.[79]

5. Opportunities for Impact

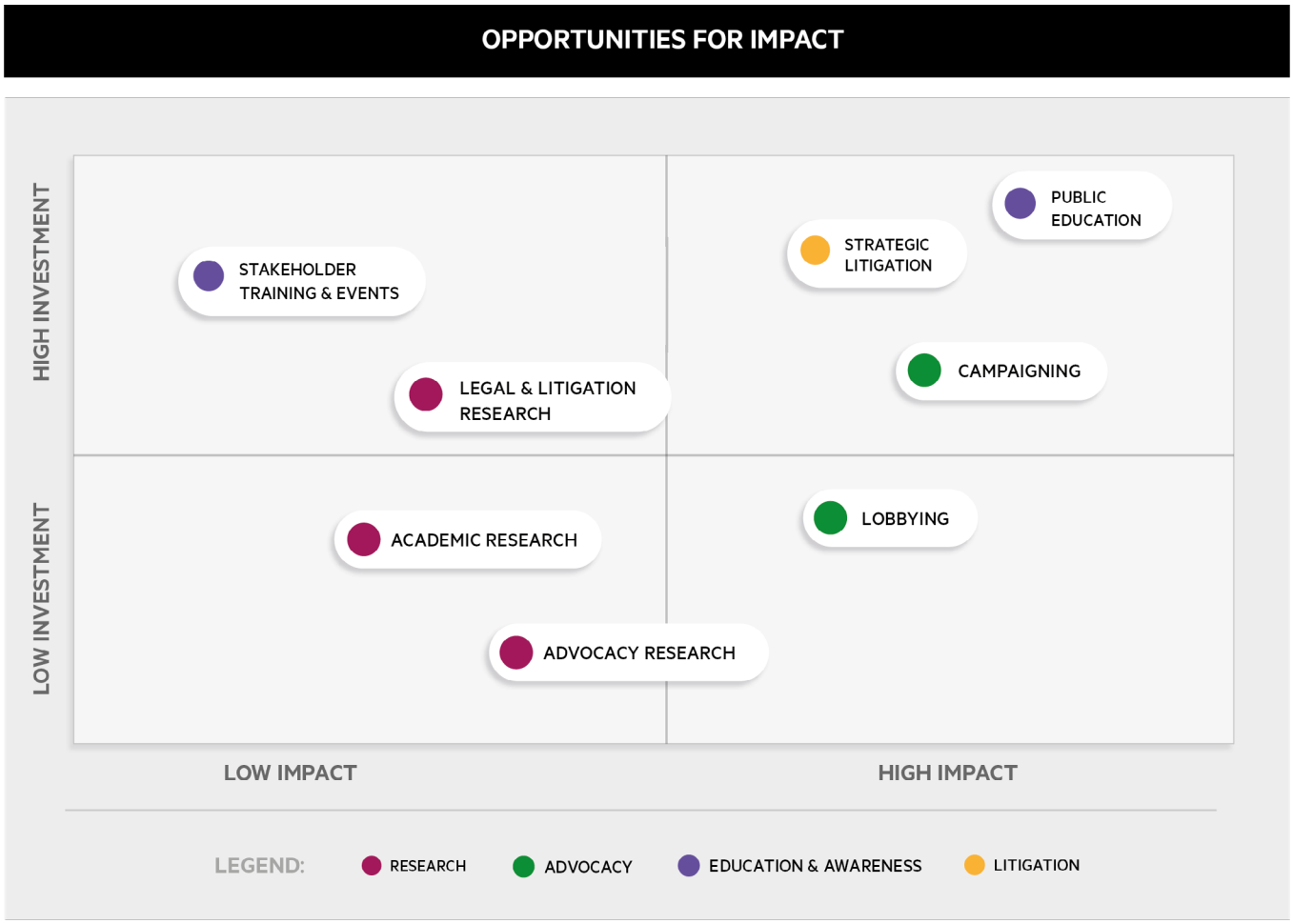
In considering the opportunities for impact, this report explores the roles of research, advocacy, litigation and education in building and strengthening the data and digital rights ecosystem. Specifically, it looks at how stakeholders use these activities to further their cause and effect change.

Using a scale of effectiveness—based on conversations with stakeholders—activities are mapped onto a matrix considering the resources/ investment required and the impact on strengthening the ecosystem. The resource and investment scale includes the time investment required by stakeholders and the costs in running the activities. The impact scale considers the effectiveness and likelihood of having a wide-reaching impact.

It is essential to highlight that these are subjective scales as they are derived from stakeholder engagement. However, they provide an insight into what are considered high impact activities in Nigeria.

5.1. Role of Research

In Nigeria, many sectors are not familiar with the data protection rules stemming from legislation and regulations because of the accessibility and clarity of the laws. In innovative sectors such as financial technology, legislation has not caught up with the developments. Research plays a vital role in explaining



how the rules apply in specific scenarios. Notably, this research is important for understanding whether the laws and regulations are achieving the desired effect, conflict with existing provisions or create an unintended consequence.

Research is also essential for creating the foundational understanding for ordinary citizens to assert their rights better. It enables citizens and advocacy groups to hold their government to account by understanding what constitutes a violation of human rights online. While research generally falls into the low impact category of the matrix above, it is often seen as an enabler of other activities. Academic research, for instance, helps identify nascent and emerging issues that other advocacy groups and campaigners can use as evidence to lobby or campaign for change. Similarly, legal and litigation research is crucial for implementing an effective strategic litigation project.

5.1.1. Academic Research

Academic research in data and digital rights consists of (i) analysis of the existing environment—the uses of data and technology, the legislative frameworks, the key players in the ecosystem; and (ii) understanding where the gaps are and how these gaps can be addressed.

Support is needed for academic researchers to access grants and other resources for their research. Funding mechanisms, especially for independent researchers, can be challenging to access as universities do not receive sufficient academic funding from the government.[80] The researchers engaged noted that they often rely on word-of-mouth to understand where funding is available. The friction in accessing funding impedes their work by limiting resources at their disposal and discouraging participation. Academic scholars in the Nigerian data and digital rights space are rare.

Academic researchers expressed an interest in having larger platforms to engage with other stakeholders to ensure their research is as effective as possible. In some countries, academic researchers are used as a resource to understand developing issues in data and digital rights as well as where and how laws need to adapt to be more fit for purpose.

> **"Having data protection laws is a starting point, but there needs to be greater awareness in the industry. Many sectors aren't conversant in what the data protection rules are"** - Academic Researcher

In Nigeria, the government involves external stakeholders at their discretion. They do engage in public consultations on occasion and are doing so with the Data Protection Bill. A researcher interviewed was consulted by the NCC on developing the Internet Codes of Practice. Their work involved a legal assessment of the existing gaps and drafting parts of the Code, including provisions on net neutrality, privacy and data protection, safeguards against unsolicited communications and obligations pertaining to unlawful content.

This consultation was the result of ongoing stakeholder interactions between the researcher and members of the Commission. However, there should be a systematic process for engaging researchers, rather than on an ad hoc basis. The NCC does conduct public consultations with other stakeholders, but this should become a standard, so each draft bill involves a comprehensive public consultation as standard.

5.1.2. Legal Research

This type of research is conducted as part of legal reviews, audits and litigation. Like academic research, it involves analysing existing legislation, but it is used to help clients or litigants. Law firms use legal research for auditing purposes to ensure their clients comply with existing data protection regulations. Some law firms have government institutions as clients and assist them with developing the legal framework to encourage growth in the digital sector. They also engage with governments to analyse how restrictions on the use of social media infringe on the rights to freedom of expression.

Legal research is also used to hold private or public institutions to account as part of litigation efforts. In Nigeria, individuals and CSOs can file court cases against institutions that violate existing laws. Cases

are often brought against government agencies. In these cases, research is vital to understand the existing rules and the jurisprudence that exists. Unfortunately, jurisprudence related to digital and data rights in Nigeria is still in its infancy, and work needs to be done to develop it.

We cover the specific opportunities for impact in strategic litigation section below but see an opportunity to reduce the costs associated with legal research by streamlining the cases that advocacy groups are filing against the most significant perpetrators of data rights violations—government agencies and telecommunications companies—through class-action lawsuits. Class-action lawsuits are few and far between in Nigeria, but they are actionable contingent on judicial discretion.[81] This action also relies on further support from funders, the collaboration between different civil society groups, as well as public education and awareness.

5.1.3. Advocacy Research

Advocacy Research is necessary for advocates, i.e. private actors, civil society, legal actors, to support their work. Their use of research differs depending on the kind of advocacy work they engage in. Some advocates are involved in disseminating information in reports and highlighting events or occurrences, like Amnesty International.[82] Their research is important in understanding current and developing events, ensuring their reports are accurate before sharing with the public.

An advocate such as BudgIT also disseminates information for data transparency purposes. Their research involves understanding where publicly available data exists and acquiring it to make it accessible for the citizens—an important initiative for supporting open data and government accountability. Research is used to support the aims of the organisation. To gather and use the information to bring about change and improvements in society, whether through litigation, lobbying, reporting or more. CIPESA, has set up a second call for its African Digital Rights Fund to respond to rising digital rights violations such as arrests and intimidation of internet users, network shutdowns, and a proliferation of laws and regulations that hamper internet access and affordability.[83] This is potentially a valuable source for supplementing research. However, few West African initiatives received grants in the 2020 round. Advocacy research can be strengthened by providing additional support to the organisations and individuals that engage in it, precisely where funding is concerned. This is further explained in the role of advocacy.

5.2. Role of Advocacy

Data and digital rights advocacy in Nigeria is critical as the government does not provide strong protection for these rights. Advocacy groups apply pressure on decision-makers to develop, implement and enforce the laws required to ensure these rights are recognised as human rights. Advocacy has helped provide pushback to oppressive laws such as the Social Media Bill. Although the Bill is still going through the National Assembly, fierce lobbying against it when introduced resulted in removing the death penalty provision in the Bill.[84]

> **"Drafting a Data Protection Bill is one thing but getting it through the National Assembly is another challenge."** - Public Sector Stakeholder

Some organisations leverage a combination of innovative campaign tactics, visual advocacy and partnerships with other CSOs, journalists and technologists. This provides an opportunity to educate, petition and make appeals to decision-makers, deliver technical resources and support to at-risk users, and mobilise online support to pressure powerful organisations.

5.2.1. Lobbying

This type of advocacy involves collaborating with pivotal stakeholders in the ecosystem to bring about change—ranging from public consultations,[85] steering committees[86] to community town halls. It also includes attempts to engage the government through press releases[87] and open letters.[88]

Paradigm Initiative has been at the forefront of this work. They led the push for Nigeria to enact a Digital

Rights and Freedom Bill in 2016 and have also engaged and educated policymakers on the need to pass the Nigerian Data Protection Bill (initially introduced in 2011) into law—particularly as the new draft Data Protection Bill, 2020 only addresses a fraction of the concerns raised.[89] Paradigm Initiative also facilitated engagements between NIMC and civil society groups, grassroots advocates, and social media activists.[90] Last year, it hosted top officials in two engagement sessions with stakeholders from the Niger Delta region and Uyo. This included a virtual conversation between the Director-General of NIMC and civil society representatives, where they received feedback and concerns on the implementation of the National Identification Number.

The Data Protection Bill previously went through the legislative process in 2019 and was passed by the 8th National Assembly, but President Buhari refused assent due to "some reservations and time constraints".[91] A new Bill is being revised with an ongoing public consultation process involving civil society groups such as the NetRights Coalition. The NetRights Coalition is a network of over 100 global civil society groups led by Paradigm Initiative. They have submitted comments on the draft Data Protection Bill raising numerous concerns around its provisions.

Lobbying is categorised as a high impact activity because key concerns voiced by CSOs around data and digital rights require policy and lawmakers to support the enactment of legislation or change government policies. For the draft Data Protection Bill, these include: (i) a proposed independent data protection commission/regulator that is funded; (ii) reducing the number of government actors currently proposed for the data protection commission's advisory board as it impacts its independence; and (iii) including independent members—from civil society, media, and academia—on the advisory board to balance government and private sector representatives equally. It is worth noting that while lobbying helps enact changes to laws and regulation, additional work is still required for effective implementation.

There's also an opportunity for the local private sector to increase lobbying participation. The lack of clarity in legislation is a hindrance for any institution that handles data. New laws need to provide clarity on data protection for various sectors to benefit from the rapid development of technologies that rely on data. More robust enforcement is also necessary to increase consumer protection and trust. Local businesses that depend on technology do not actively participate in this field. There is a general sentiment among tech-enabled businesses that regulators have a draconian approach to technology regulation, making it challenging to engage effectively. Nevertheless, if laws such as the Social Media Bill were to be passed, it would be detrimental to many businesses. This should be an incentive for local companies to be involved in the conversations around developing strong legal frameworks for data and digital rights.

> **"The tech community is in a position to act—but they do not recognise the dangers they may face by not participating or adding their voice to the conversations around the government's attempt to regulate social media...It would be good to get more their support."** - CSO

5.2.2. Campaigning

Many CSOs are involved in campaigns for freedom of expression online, online privacy, digital security and more. The campaigns include educating the public about the issues, addressing current events, publishing reports, or coordinating events. There are ongoing attempts to build momentum and bring attention to the issues. Amnesty International, for example, has campaigned for the protection of freedom of expression, particularly for journalists, and consistently brings attention to harassment and detainment of journalists.[92]

Campaigns are a high impact activity because they are an effective way of keeping citizens informed on particular topics. However, the work that goes into campaigning is sizable. One reason is that the research behind it takes time, resources and training of staff. Campaigns also need a network of journalists, researchers and the support of other advocates for a campaign to be effective. However, the funding received by CSOs is often project-based and does

not provide enough coverage for supporting research activities.

There's an opportunity to improve the effectiveness and reach of campaigns by expanding the funding mechanisms to cover general support. This could, for example, enable organisations to travel to gather, disseminate and create tools that will allow communities to engage with their work more efficiently. In our stakeholder interviews, a funder suggested using other dissemination methods such as local radio and TV could make campaigns more effective. However, this means campaign organisers will incur additional costs.

> **"One challenge is communication. Digital rights groups tend to speak in jargon. There's no way for communities to understand what they're talking about and this makes campaigns inaccessible." - Funder**

5.3. Role of Litigation

Government agencies are one of the most frequent perpetrators of digital and data rights cases. Out of the 35 listed in DRLI's pending cases, 30 cases involved a public institution or stakeholder. Litigating against infringement of data and digital rights is especially important to establish legal precedents in Nigeria and clarify the interpretation of laws, as government institutions do not uphold or routinely enforce these rights.

5.3.1. Strategic Litigation

Data and digital rights are areas that are in their infancy globally. Many regions are still developing or updating their data and digital rights frameworks. New legislation or emerging practices have a potentially severe impact on the ability of citizens to exercise their rights to privacy and freedom of expression. Whilst legislative frameworks are developing; strategic litigation has a pivotal role to play in how society and the government respond to these issues as the legislative frameworks grow even further.

> **"Another area with gaps is litigation. There is no deliberate effort to pull together and support strategic litigation. A lot of litigation today relies on individual efforts and resources." - Funder**

Strategic litigation—litigation with broad impact and bringing about legislative or policy change—can be a crucial lever to protect human rights in the data and digital rights ecosystem. As a high impact activity, it can help pave the way in creating progressive jurisprudence and the reform of existing repressive laws that give rise to human rights violations. It also helps raise awareness of the weaknesses that exist in the legal systems and understand why and how they can be exploited.

So far, the impact of strategic litigation has not been felt widely in data and digital rights in Nigeria. However, with the current state of the legal system, the effect is still unlikely to materialise soon. To increase the chances of favourable jurisprudence developing, there are a few opportunities that can be explored.

The first step is to increase the pool of knowledgeable professionals (lawyers and judges) in the legal system. If there isn't a consensus that these rights are fundamental, it will be more difficult to uphold when infringements are brought to court. The second step is for those involved in strategic litigation to collaborate to pool resources and knowledge to give the best chances of success. Various groups are engaging in litigation, but their efforts are often fragmented. Some difficulty lies in accessing knowledge bases and funding, and if groups were to collaborate, they could streamline the litigation they engage in and pool their resources.

Another opportunity lies in providing flexibility to litigation funds and supporters to focus on or prioritise new and emerging issues. Organisations such as the Digital Freedom Fund in Europe have noted how the coronavirus pandemic quickly shifted their strategic litigation focus as digital rights organisations had to promptly divert their attention towards a stream of new threats, such as invasive apps or governments abuse of emergency lockdown laws to expand digital

surveillance.[93] While the pandemic may not have raised similar concerns in Nigeria for digital rights cases among stakeholders, the EndSARS backlash to online supporters[94] provides an instance where priorities for strategic litigation had to be quickly refocused.

> **"There's a gap in terms of manpower and developing the jurisprudence—judges also need to be trained...sometimes you get unfavourable judgement because judges don't believe data protection is a fundamental right." - Human Rights Lawyer**

Some stakeholders are already benefiting from flexible funding. DRLI, for instance, highlighted how institutional funding from Omidyar Network has provided opportunities to pick cases to fund and support cases they believed were relevant to the Nigerian context.

An additional opportunity for strategic litigation is making submissions to the ECOWAS Community Court of Justice ("CCJ"), which accepts individual complaints about human rights violations. Per ECOWAS Protocol, the CCJ has jurisdiction to hear human rights cases—including disputes between individuals and their member states.[95] Decisions of the CCJ are final and binding under the 1991 ECOWAS Protocol, and member states are required to take all measures necessary to ensure execution of the court's decision.[96] Although ECOWAS instruments do not specify the remedies that the CCJ can provide, past remedies included awards of damages and specific orders such as an order for the immediate release of an illegally detained journalist.[97]

The CCJ is seen as a more favourable court for data and digital rights as its decisions have generally been consistent with existing international law. In June 2020, for example, CCJ issued a pivotal decision for the right of freedom of expression in Togo and other West African states. It ruled that access to the internet has to be protected under the law. By shutting it down during the anti-government protests in 2017, the Togolese government violated human rights.[98] Furthermore, the CCJ accepts amici curiae briefs, allowing third parties to offer additional support in strategic litigation cases by providing legal advice or opinion on data and digital rights. Access Now led a coalition of eight organisations, including CIPESA and Paradigm Initiative, who submitted an amicus curiae brief in the lawsuit filed by Amnesty International and other applicants in response to the 2017 internet shutdowns in Togo.

5.4. Role of Education

For the data and digital rights ecosystem to function efficiently, the actors and participants in the system need to be aware of the rules they are bound by. Thus far, there have not been coordinated and concerted efforts to educate stakeholders on data and digital rights. Instead, small pockets of activities have served as a testbed of education and awareness-raising efforts.

5.4.1. Public Education

Unfortunately, many Nigerians are not aware of their rights, and when they are, there is limited awareness of how those can be enforced. Sensitisation of citizens on what constitutes a violation of their rights and how they can take action against it is necessary for an attitude shift that will inspire widespread grassroots activism and advocacy.

Efforts in campaigning by advocacy groups have helped to inspire activism towards specific issues. For example, AccessNow runs its "#KeepItOn" campaign to fight internet shutdowns. In 2019, ahead of the Presidential elections, there were beliefs that the government would restrict access to the internet, similar to other African countries. As part of this campaign, AccessNow supported the Media Foundation for West Africa to organise regional convening to bring together government officials and other actors.

The nature of campaigns focuses on specific issues—and this arguably makes them more effective.

Almost half of the Nigerian population is rural.[99] Similarly, only half of the Nigerian population has access to the internet.[100] This means that a large part of the population cannot be quickly or cheaply accessed. This is one limitation to widespread public education. As a high impact activity, this makes public

education and awareness-raising the most resource and investment intensive. There are infrastructural issues that hinder the ability to conduct widespread and far-reaching education campaigns.

As noted earlier from our conversations with stakeholders on the effectiveness of advocacy campaigns, we see an opportunity to improve the effectiveness of public education through increased funding to grassroots activists and supporting alternative campaign methods. For instance, this could be by supporting local-language radio-show segments on data privacy and rights.

A successful education and public awareness campaign requires concerted and consistent efforts to organise and implement these activities. As a result, these should preferably be taken on with government stakeholders or other funders such as development/ aid funding organisations who also influence the ecosystem. One example is the World Bank, as its digital identity programme[101] has been a critical driver for data and digital rights laws in Nigeria.

> **"From a human rights perspective people can relate to basic surveillance (i.e. someone looking into your house), there is a general lack of awareness about when the lines are being crossed with digital issues."** - Human Rights Lawyer

5.4.1. Stakeholder Training

As previously explored on the role of stakeholder engagement, there's a lot of learning that needs to be done even within the public institutions in Nigeria. Public servants, lawyers, judges, ministers, senators, private stakeholders alike indicate a knowledge gap where the application and enforcement of data and digital rights are concerned. Besides engaging stakeholders to understand their needs and concerns, training is required to upskill actors where necessary. Advocates are already working with government stakeholders here, for instance, through technical capacity building. BudgIT has worked with government agencies on financial transparency and data accessibility training,[102] and the MacArthur Foundation has worked with agencies such as the EFCC on anti-corruption.[103] These advocates' work is vital in equipping public servants with the skills and knowledge for best practice in data protection and transparency. It's also essential to build these relationships in the public sector and potentially open the door for collaboration in other areas.

6. Building a Community

Throughout the stakeholder engagement process, there was a consistent trend limiting or restricting the ability to collaborate and function as a community. This was the lack of awareness of the activities being conducted by other stakeholders. There appeared to be a knowledge gap regarding other stakeholders' actions, effectiveness, successes or failures and opportunities for collaboration.

An issue that has been explored in this report is how the activities of various stakeholders are fragmented. A concerted effort to cooperate is needed. As such, there is an opportunity to form or strengthen a central point of resource and information for Nigeria's data and digital rights community. Attempts have been made towards this goal—predominantly at the regional level. Some of these include AANOIP,[104] the Association for Progressive Communications (APC),[105] and the African Digital Rights Network (ADRN).[106]

> **"Funders should give room for mistakes and allow grantees to be more innovative."** - CSO

However, due to the broad regional focus of these networks and associations, they are not the first point of resource for data and digital rights in Nigeria. A further limitation to collaboration expressed during stakeholder interviews was the competitive nature of advocacy and research work. Naturally, stakeholders conducting advocacy, research and litigation have to compete for funding—and as a result, are forced to differentiate themselves and their work from other groups. This acts as a hindrance to collaboration and requires funders to consider incentives for encouraging collaborations between their grantees. Particularly with smaller and perhaps newer groups or organisations working in data and digital rights.

Building a network or community working together to achieve the same goal would provide more visibility for what other stakeholders are doing, where more support is needed and where resources exist. It will encourage collaboration, and reduce the effort and resources incurred when acting alone. Working together can also exert additional pressure on government stakeholders and reduce the individual overhead required to organise and run events that enhance the proliferation of data and digital rights awareness in Nigeria.

> **"We need to communicate across the aisle to change the system... we need more information sharing and knowledge bases"** - Human Rights Lawyer

6.1. Conclusion

Data and digital rights is a developing area in Nigeria, with all stakeholders—including the private and public sectors—still learning how to navigate this space. Legislation in Nigeria has been developing over the last 20 years, beginning with the rights to privacy and freedom of expression, enshrined in the Constitution. Although the legislation exists, it does not provide sufficient protection to citizens as there are vague provisions in the laws open to exploitation e.g., the definition of "national security". These provisions are abused by public sector actors such as the police, who often use laws like the Cybercrimes Act to target journalists or citizens that criticise the government. There is also poor judicial oversight where personal data is accessed by law enforcement.

In response to these issues, many stakeholders have been advocating for the development of new legislation and protection against abuse. Some CSOs are fighting against these abuses through strategic litigation. However, the nascent nature of data and digital rights in Nigeria means more education is still

needed within the legal sector—to upskill lawyers and judges on how fundamental human rights such as the right to privacy and the right to freedom of expression extend online. Public education also continues to be essential to sensitise and raise awareness for individuals. It remains an important tool for holding the public and private institutions to account.

> **"Now more than ever before, we need capacity building for digital rights lawyers."** - CSO

Finally, better coordination is needed among actors working to address data and digital rights issues in Nigeria—to pool resources and skills and build a self-identifying community of data and digital rights experts. This community will help grassroots organisations identify and shed light on the local priorities. All the relevant stakeholders needed to develop Nigeria's data and digital rights space already exist, but joining forces can help make their efforts more impactful.

Credits

Stears Data

Stears Data creates bespoke research and knowledge solutions to corporates, investors, governments, and individuals who want to understand, position within, or shape the frontiers of the digital economy. Our mission is to be a knowledge and data partner for understanding and making decisions that shape the future of Africa. Our priority areas include technology, digital economy & society, socio-economic development, energy, health, agriculture, and finance.

To learn more, visit www.stearsdata.com and follow on Twitter @StearsData.

Luminate

Luminate is a global philanthropic organisation with the goal of empowering people and institutions to work together to build just and fair societies. We do this by funding and supporting non-profit and for-profit organisations and advocating for policies and actions that will help people participate in and shape the issues affecting their lives, and make those in power more transparent, responsive, and accountable. We prioritise delivering impact in four connected areas that underpin strong societies: Civic Empowerment, Data & Digital Rights, Financial Transparency, and Independent Media.

Acknowledgements

We would like to thank the following participants for participating in our research and insights gathering for this report.

- Access Now
- Amnesty International (Nigeria)
- Branch International
- BudgIT
- CCHub
- DAI
- Dataphyte
- Digital Forensic Research Lab
- Digital Rights Lawyers Initiative
- Ford Foundation
- Independent Researchers
- Indicina
- Journalists
- MacArthur Foundation
- Nigerian Communications Commission
- OAL Law/Human Rights Law Service
- Omidyar Network
- Paradigm Initiative
- Research ICT Africa
- Ex-Mozilla Fellow
- Tope Adebayo LLP

Endnotes

1 As detailed in Freedom House's assessment of Nigeria's internet freedom in 2019. See https://www.justice.gov/eoir/page/file/1234686/download

2 Paradigm Initiative recently released a Digital Rights and Privacy report for Nigeria, which outlines some of their current activities in this space. See https://paradigmhq.org/download/digital-rights-and-privacy-in-nigeria/

3 Olanrewaju, O. An Evaluation of the Knowledge and Perception of the Concept of Human Rights by Residents of Selected Suburban Communities of Lagos, Nigeria. J. Hum. Rights Soc. Work 5, 185–190 (2020). https://doi.org/10.1007/s41134-020-00121-5

4 Tisne M., It's time for a Bill of Data Rights, MIT Technology Review, 2018. See https://www.technologyreview.com/2018/12/14/138615/its-time-for-a-bill-of-data-rights/

5 In February 2020, the EU announced a new plan to create a pan-European market for personal data through a mechanism called a data trust. A data trust is a steward that manages people's data on their behalf and has fiduciary duties toward its clients. See https://www.technologyreview.com/2020/08/11/1006555/eu-data-trust-trusts-project-privacy-policy-opinion/

6 Requiring individuals to take ownership of personal data in what is regarded as a "personal data economy" has been argued to potentially result in unequal access to privacy and could encourage predatory and discriminatory behavior—even though it provides a semblance of control. See https://columbialawreview.org/content/paying-for-privacy-and-the-personal-data-economy/

7 Digital rights are Human Rights, Digital Freedom Fund, 2020. See https://digitalfreedomfund.org/digital-rights-are-human-rights/

8 United Nations Declaration of Human Rights. See https://www.un.org/en/about-us/universal-declaration-of-human-rights

9 Digital rights are Human Rights, Digital Freedom Fund, 2020. See https://digitalfreedomfund.org/digital-rights-are-human-rights/

10 GSM Association, The Mobile Economy: Sub-Saharan Africa 2019, GSM Association, 2019. See https://www.gsma.com/subsaharanafrica/resources/the-mobile-economy-sub-saharan-africa-2019

11 4 ways digitisation can unlock Africa's recovery, World Economic Forum, 2020. See https://www.weforum.org/agenda/2020/06/4-ways-digitisation-can-unlock-recovery-in-africa/

12 CIPESA, State of Internet Freedom in Africa 2018: Privacy and Data Protection Challenges in the Digital Era. See https://cipesa.org/?wpfb_dl=278

13 CIPESA, State of Internet Freedom in Africa 2020: Resetting Digital Rights Amidst The Covid-19 Fallout. See https://cipesa.org/wp-content/uploads/2020/10/State-of-Internet-Freedom-in-Africa-2020.pdf

14 Based on IMF country data for Nigeria, 2020. See https://www.imf.org/en/Countries/NGA#countrydata

15 Number of internet users in Nigeria from 2015 to 2025, Statista. See https://www.statista.com/statistics/183849/internet-users-nigeria/

16 Distribution of web traffic in selected African countries as of October 2020, by device, Statista. See https://www.statista.com/statistics/685188/african-countries-online-traffic-channel-share/

17 Nigeria Country Profile, Freedom on the Net 2020, Freedom House. See https://freedomhouse.org/country/nigeria/freedom-world/2020

18 Nigerians protest at NASS over Anti-Social Media Bill, The Citizen Online, 2015. See https://thecitizenng.com/nigerians-protest-at-nass-over-anti-social-media-bill/

19 Oyegbade H., COVID-19: Facebook Post Lands Man In Jail, Daily Trust, 2020. See https://dailytrust.com/covid-19-facebook-post-lands-man-in-jail

20 Aminu H.U., Police Arrest 3 For Insulting President Buhari, Masari On Social Media, Daily Trust, 2020. See https://dailytrust.com/police-arrest-3-for-insulting-president-buhari-masari-on-social-media

21 UN Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet: Resolution Adopted by the Human Rights Council, 2016, A/HRC/RES/32/13. See https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

22 Tracking by Paradigm Initiative has revealed a continued spike in arrests of dissenting and critical voices in Nigeria, with an initial peak observed in 2017. See https://paradigmhq.org/download/dra19/

23 Efobi N. and Ekop N. (AELEX), Legal systems in Nigeria: overview, Practical Law, 2021.

24 Masud M.K., Peters R., Powers D.S., Dispensing justice in Islam: Qadis and their judgements, Brill, 2006.

25 Schedule 2, Part I, Constitution of the Federal Republic of Nigeria, Act No. 24, 5 May 1999.

26 Obilade AO.,The Nigerian legal system, Sweet & Maxwell, 1979.

27 Although federal legislation overrides state legislation, it is argued that a systemic issue exists in Nigeria's approach to federalism and whether a secular nation at a federal level can accommodate non-secular state laws set at a regional level. See Mazrui A., McMahon E.R. and Sinclair T.A., Shariacracy and federal models in the era of globalization: Nigeria in comparative perspective, 2005.

28 The Arabic term hisbah is integral to the Islamic socioeconomic scheme and policing, functioning as a way to maintain public law and order and supervising the behavior of people. See Olaniyi R.O., Hisbah and Sharia law enforcement in metropolitan Kano, Africa Today, 2011.

29 "Political Shari'a"? Human Rights and Islamic Law in Northern Nigeria, Human Rights Watch, 2004. See https://www.hrw.org/report/2004/09/21/political-sharia/human-rights-and-islamic-law-northern-nigeria

30 Oxford Dictionary of Islam. See http://www.oxfordislamicstudies.com/article/opr/t125/e851

31 "Political Shari'a"? Human Rights and Islamic Law in Northern Nigeria, Human Rights Watch, 2004. See https://www.hrw.org/report/2004/09/21/political-sharia/human-rights-and-islamic-law-northern-nigeria

32 Amnesty International has documented the progress of Yahaya Sharif-Aminu's case, and has called for a retrial. See https://www.amnesty.org/en/documents/afr44/3568/2021/en/

33 Information about Rahama Sadau's charge, including a memo from the office of the Inspector General of Police, calling the Kaduna State police to take action on this incident. See https://www.premiumtimesng.com/news/top-news/425055-rahama-sadaus-photos-man-alleges-blasphemy-police-ig-orders-action.html

34 Constitution of the Federal Republic of Nigeria, Act No. 24, 5 May 1999. See http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm

35 Wachter S., Privacy: Primus Inter Pares - Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights, 2017. See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903514

36 Section 45, Constitution of the Federal Republic of Nigeria, Act No. 24, 5 May 1999. See http://www.nigeria-law.org/ConstitutionOfTheFederalRepublicOfNigeria.htm

37 Adibe R et al., Press Freedom and Nigeria's Cybercrime Act of 2015: An Assessment, 2017. See https://journals.sagepub.com/doi/10.1177/000203971705200206

38 Freedom of Information Act, 2011, CBN Archives. See https://www.cbn.gov.ng/FOI/Freedom%20Of%20Information%20Act.pdf

39 Nigerian Communications Act, 2003, Federal Republic of Nigeria Official Gazette. See https://www.uspf.gov.ng/files/Nigerian_Communications_Act_2003.pdf

40 National Information Technology Development Agency Act, 2007, NITDA. See https://nitda.gov.ng/wp-content/uploads/2020/11/NITDA-ACT-2007-2019-Edition1.pdf

41 See list of licensed DPCOs, https://nitda.gov.ng/wp-content/uploads/2021/04/V7.2-DPCO-LIST-12042021.pdf

42 Adeboye A., Digital Rights and Privacy in Nigeria, Paradigm Initiative. See https://paradigmhq.org/download/digital-rights-and-privacy-in-nigeria/

43 Although a regulator, NITDA also has a mandate to develop the information technology sector in Nigeria and it conducts activities such as setting up digital job creation centres, IT capacity building and setting up IT hubs. See https://nitda.gov.ng/mandate/

44 Paradigm Initiative calls for NIMC to suspend mandatory registration. See https://paradigmhq.org/paradigm-initiative-calls-on-nimc-to-suspend-nin-enforcement-activities/

45 Enabling Digital Development, World Development Report 2016, The World Bank. See http://documents1.worldbank.org/curated/en/896971468194972881/310436360_20160263021000/additional/102725-PUB-Replacement-PUBLIC.pdf

46 Committee on the Rights of the Child Fifty-fourth session, Convention on the Rights of the Child, 2010. See https://www.refworld.org/pdfid/4c32dea52.pdf

47 The Data Protection Bill is a proposed Act to establish a Data Protection Commission responsible for the protection of personal data, rights of data subjects, regulation of the processing of personal data and other related issues. See https://www.ncc.gov.ng/docman-main/legal-regulatory/legal-other/911-data-protection-bill-draft-2020/file

48 These concerns were raised in stakeholder conversations.

49 This is discussed in Privacy International's report on the state of data protection across Africa. See https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa

50 On June 17, 2019 a Nigerian man identified as Jeffrey Ewohime allegedly destroyed seven cars and property at the Nigerian High Commission in London over a delay in releasing his passport to him by officials of the Nigerian High Commission. Responding to the situation, the Nigeria Immigration Service took to its Twitter handle @nigimmigration to display an already issued International Passport in the name of the alleged vandal. See https://globalfreedomofexpression.columbia.edu/updates/2019/06/nigerian-immigration-service-and-the-burden-of-data-protection/

51 Twitter post by the Presidential Task Force, which lists the passport details of the 100 travellers penalised. See https://twitter.com/DigiCommsNG/status/1345602993987735552

52 The Committee to Protect Journalists has reported on the Nigerian military targeting journalists' phones, computers with "forensic search" for sources. See https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/

53 This list details the subject matter, and litigants of the DRLI's pending cases. See https://digitalrightslawyers.org/wp-content/uploads/2021/02/drli-cause-list.pdf

54 Cowrywise released a statement detailing the breach that occurred, and the actions they took to rectify it. See https://cowrywise.com/blog/official-statement-from-cowrywise-customer-support-team/

55 TechCabal wrote an article detailing additional safety features that could have reduced the risk of this breach occuring. See https://techcabal.com/2020/09/09/fintech-app-cowrywise-funmi-oyatogun/

56 Nairaland forum, where individuals are complaining about their experience using Sokolaon. See https://www.nairaland.com/5689187/beware-sokoloan and https://www.nairaland.com/6335310/how-got-badly-disgraced-sokoloan/4

57 Rest of World reported on lending apps that publicly shame customers when they are late on loan payment. See https://restofworld.org/2020/okash-microlending-public-shaming/

58 The issue of individuals giving up privacy for access to quick loans was discussed in an article published by TechCabal. See https://techcabal.com/2019/10/14/in-search-of-quick-loans-nigerians-give-up-privacy/

59 Oral evidence from a stakeholder who does extensive research on data rights in Nigeria.

60 Open Data Watch Rankings, 2020. See https://odin.opendatawatch.com/Report/countryProfileUpdated/NGA?year=2020

61 Green, Ben, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford. 2017. Open Data Privacy (2017). Berkman Klein Center for Internet & Society Research Publication. See https://dash.harvard.edu/handle/1/30340010

62 Ibid.

63 The Open Data Charter published an article detailing the evolution of Open Data, and how decision makers in the public sector can derive impactful benefits from the third wave of open data. See https://medium.com/opendatacharter/connecting-the-past-present-and-future-of-re-using-data-to-advance-societal-goals-298d8dad36f5

64 Techpoint article analysing what this refusal means for digital rights in Nigeria. See https://techpoint.africa/2019/03/27/nigerian-president-declines-digital-rights-bill-assent/

65 Protection from Internet Falsehoods and Manipulation and Other Related Matters Bill, 2019, National Assembly. See https://www.nassnig.org/documents/billdownload/10965.pdf

66 Oral evidence from a funder.

67 The Atlantic Council's DRF Lab conducted research on two networks of Nigerian Twitter accounts that were amplifying pro-government content and appeared to be staging an online suppression campaign to delegitimize the nationwide #EndSARS protests against police brutality. See https://medium.com/dfrlab/nigerian-government-aligned-twitter-network-targets-endsars-protests-5bb01a96665c

68 At the onset of the EndSARS protests on October 8, the Feminist Coalition began receiving donations to support protests through a fund set up by a Nigerian online payment processing company, Flutterwave. The payment link for the fund became inoperative on October 13, and media reports said it was to block funding channels for the protests. See https://www.hrw.org/news/2020/11/13/nigeria-punitive-financial-moves-against-protesters

69 Human rights academics conducted a study to assess the Cybercrime Act 2015 and its implications for online press freedom in the liberal authoritarian state of Nigeria. See https://journals.sagepub.com/doi/10.1177/000203971705200206

70 News reports detailing the harassment of journalists during coverage of the EndSARS protests. See http://saharareporters.com/2020/11/08/group-condemns-arrest-journalist-endsars-protesters-abuja and https://www.premiumtimesng.com/news/headlines/424446-endsars-how-police-killed-20-year-old-nigerian-journalist.html

71 Premium Times reported on the fines issued to broadcast stations as the Socio-Economic Rights and Accountability Project (SERAP) has condemned them as unconstitutional and illegal fines. See https://www.premiumtimesng.com/news/more-news/423160-endsars-serap-fumes-as-nbc-fines-channels-ait-arise-tv.html

72 Paradigm Initiative, Digital Rights and Privacy in Nigeria, 2019. See https://paradigmhq.org/download/digital-rights-and-privacy-in-nigeria/

73 Executive Budget Proposal, 2020, Budget Office of the Federation. See https://www.budgetoffice.gov.ng/index.php/2020-executive-budget-proposal?task=document.viewdoc&id=732

74 These and other budgetary allocation to national surveillance projects were detailed in Freedom House's assessment of Nigeria's internet freedom in 2019. See https://www.justice.gov/eoir/page/file/1234686/download

75 Section 24, Cybercrimes (Prohibition, Prevention etc), 2015.

76 Section 146, Nigeria Communication Act, 2003.

77 Section 147, Nigeria Communication Act, 2003.

78 There have been various news articles detailing the detainment of Samuel Ogundipe. See https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/

79 A news article by Sahara Reporters detailed the detainment of the prominent lawyer, Modupe Odele, involved in EndSARS activities. See http://saharareporters.com/2020/11/03/immigration-officials-detained-me-seized-my-passport-stopped-me-leaving-nigeria-lawyer

80 Nigeria's public universities rely primarily on government funding, which usually comes to less than 10% of the national budget at the federal level, below the African average and UNESCO's minimum recommendation of 15%. See https://www.stearsng.com/article/how-to-better-fund-nigerian-education

81 DRLI wrote an article on the utility of seeking redress through class-action for consumer rights violations, which analysed the history and effectiveness of class-action in Nigeria. See https://www.mondaq.com/nigeria/class-actions/904364/the-increasing-need-for-utility-of-class-actions-in-seeking-redress-for-consumer-rights-violations-in-nigeria

82 Amnesty International has documented numerous human rights violations in Nigeria, including in relation to digital rights such as freedom of expression online. See https://www.amnesty.org/en/latest/news/2019/11/nigeria-sowore-bakare-and-jalingo-declared-prisoners-of-conscience/

83 Announcement of the second Africa Digital Rights Fund was made by CIPESA in 2020. See https://cipesa.org/2020/01/the-africa-digital-rights-awards-usd-152000-to-advance-digital-rights-in-18-african-countries/

84 Paradigm Initiative has coordinated important campaigns and lobbying efforts around the Social Media Bill. See https://paradigmhq.org/open-letter-to-the-nigerian-senate-on-the-matter-of-the-frivolous-petitions-prohibition-bill-aka-social-media-bill/ and https://paradigmhq.org/tag/saynotosocialmediabill/

85 The NCC runs public consultation as part of its internet governance functions, which invites the public to provide their input on matters having to do with ensuring the availability of affordable, reliable, accessible and efficient internet and internet based services in Nigeria. See https://ncc.gov.ng/technology/internet/internet-public-consultations

86 Public institutions in Nigeria do form steering committees, one example being NIMC's to fast-track the implementation of the Strategic Roadmap for accelerating digital identity development for Nigeria. Often, however, these committees do not have sufficient representation of non-government stakeholders. See https://nimc.gov.ng/fg-inaugurates-steering-committee-for-nigeria-digital-identity-for-development-ecosystem-project/

87 Privacy International, in collaboration with Paradigm Initiative, has also made press releases around concerns for the regulation of data and digital rights environment in Nigeria. See https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf

88 CIPESA provides an example where it published an open letter to Nigerian senators in 2015 urging them to reconsider and reject the proposed Social Media Bill. It is hard to measure the effect of this specific letter but it added to the support for the campaign against the bill. See https://cipesa.org/2015/12/open-letter-to-the-nigerian-senate-on-the-matter-of-the-frivolous-petitions-prohibition-bill-aka-social-media-bill/

89 Paradigm Initiative recently released a Digital Rights and Privacy report for Nigeria, which outlines some of their current activities in this space. They also include further details on the areas that raise concerns—particularly on the implementation of a

Data Protection Bill. See https://paradigmhq.org/download/digital-rights-and-privacy-in-nigeria/

90 These were outlined in a conversation between Paradigm Initiative's Program Manager and Omidyar Network. See https://omidyar.com/partner-spotlight-paradigm-initiatives-vision-for-ensuring-good-id-and-data-protection-in-nigeria/

91 According to Olufemi Daniel, the NDPR Desk Lead at NITDA, one such reservation is around the provisions relating to storage of personal data in Nigeria and fines associated with its violation. They believe it to be "draconian" and hampering innovation. See https://guardian.ng/news/data-protection-bill-ll-strengthen-nigeria-data-protection-regulation-nitda/

92 Amnesty has followed cases of journalists that have been threatened and harassed by Nigerian government for criticism. Journalists have often had to go into hiding because they fear for their safety. See https://www.amnesty.org/en/documents/afr44/1896/2020/en/ and https://www.amnesty.org/en/documents/afr44/1866/2020/en/

93 This was noted in Digital Freedom Fund's notes from its 2021 Strategy Meeting. See https://digitalfreedomfund.org/new-format-new-world-our-strategy-meeting-2021/

94 The DRLI has helped bring a case against the Attorney General of the Federation for the arrest, detention and brutality of the now deceased journalist Pelumi Onifade for his recordings of the #EndSARS protests. Calls have also been made by international organisations for an investigation. See https://en.unesco.org/news/nigeria-unesco-director-general-calls-investigation-death-journalist-pelumi-onifade

95 Article 9 of the 1991 ECOWAS Protocol and 2005 ECOWAS Supplemental Protocol.

96 The Justice Initiative Fact Sheet: ECOWAS Community Court of Justice. See https://www.justiceinitiative.org/publications/ecowas-community-court-justice

97 Manneh v The Gambia (2008) AHRLR 171 (ECOWAS 2008).

98 ECOWAS Togo court decision: Internet access is a right that requires protection of the law. https://www.accessnow.org/ecowas-togo-court-decision/

99 Nigeria's rural population as a percentage of the total. See https://tradingeconomics.com/nigeria/rural-population-percent-of-total-population-wb-data.html

100 Number of Nigerians with access to the internet. See https://www.statista.com/statistics/183849/internet-users-nigeria/#:~:text=In%202020,%20Nigeria%20had%2099.05,reach%2065.2%20percent%20in%202025

101 The objective of the project is to increase the number of persons with a national identification (ID) number, issued by a robust and inclusive foundational ID system, that facilitates their access to services. See https://www.worldbank.org/en/news/loans-credits/2020/02/18/nigeria-digital-identification-for-development-project

102 A stakeholder mentioned in their interview that they work with some government agencies to upskill them.

103 A funder mentioned in their interview that they work with anti-corruption agencies in Nigeria to assist them with transparency and accountability.

104 AANOIP is a network for interdisciplinary scholarly engagement that carries out research and aims to bring together research from scholars working on the various themes to bring into focus and foster discourse on key issues as it relates to enabling the African digital economy. See https://aanoip.org/

105 The APC focuses on empowering and supporting individuals working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technologies (ICTs). See https://www.apc.org/en/about

106 The ADRN, funded by the UKRI and GCRF, aims to produce a better understanding of the actors and technologies involved in the opening and closing of civic space online, and to build the capacity of citizens to exercise, defend and expand their rights online and offline. See https://www.ids.ac.uk/projects/african-digital-rights-network/