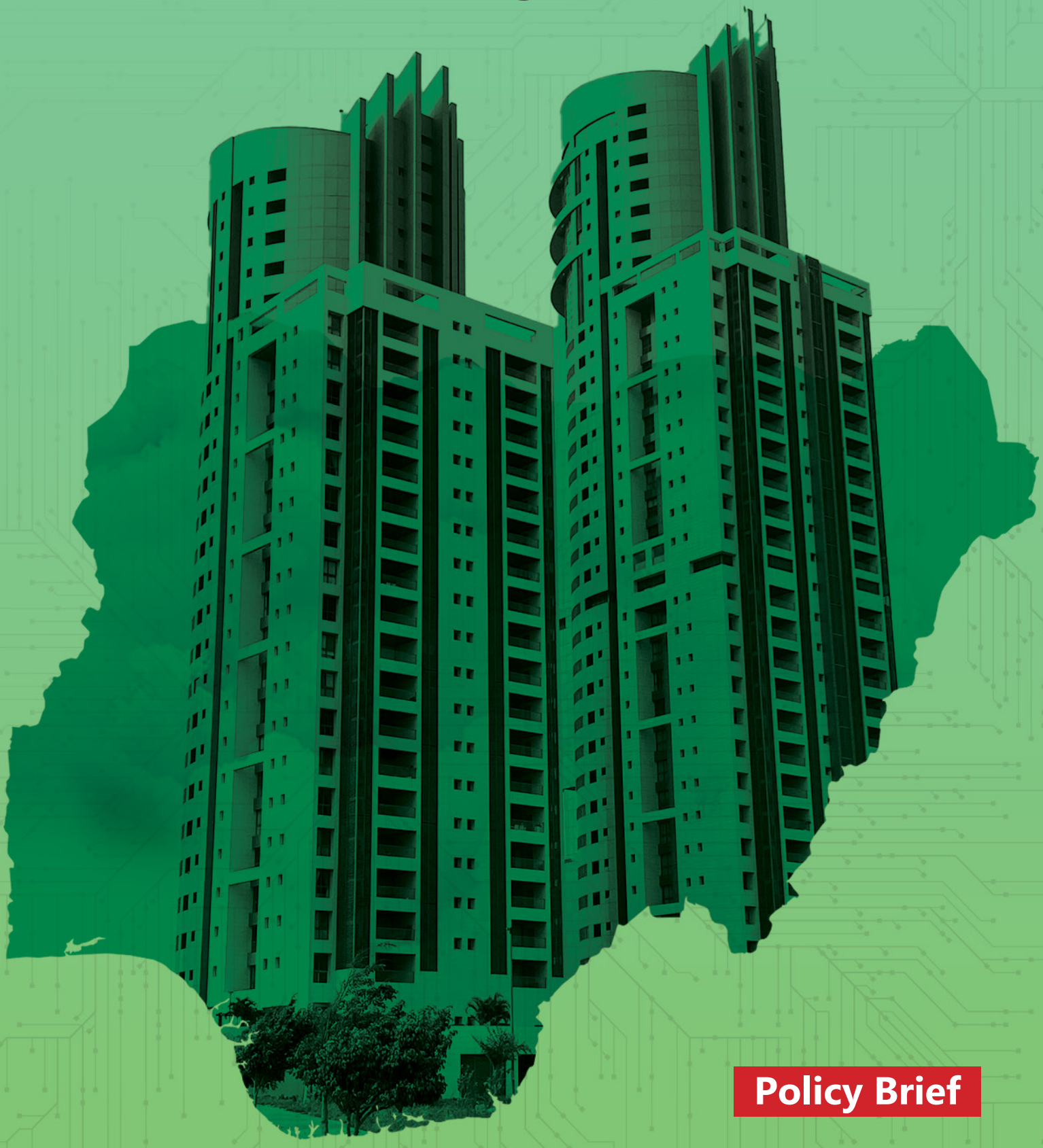
PARADIGM INITIATIVE

Building a Human Rights Compliant Tech Business in Nigeria



Policy Brief

Policy Brief

Building a Human Rights compliant tech business in Nigeria

August 2022.

Principal author:
Sani Suleiman Sani,

Editorial support:
Jacquiline Rowe
Thobekile Matimbe
Khadija el-usman

Review:
Nnenna Paul-Ugochukwu

Design and Layout:
Kenneth Oyeniyi,

Published By
Paradigm Initiative

Supported by
Global Partners Digital

PARADIGM INITIATIVE
@ParadigmHQ

Summary

Technology is deeply rooted in our daily activities; although this may seem obvious, stressing it serves to remind us how much technology influences our daily interactions and decisions. Additionally, around the world in recent decades, concerns about the harmful effects of corporate activity on human rights have moved to the top of the international agenda, prompting the development of principles, tools and frameworks for business and human rights. These are broadly collected under the well-known United Nations Guiding Principles on Business and Human Rights (hereinafter "UNGP-BHR"), which entrench respect for human rights as a responsibility of businesses of all sizes, types, locations, structures, and sectors.

This policy brief examines the implications of the UNGP-BHR for technology companies in Nigeria, exploring the norms and expectations they must meet in terms of respect and protection for human rights. It provides stakeholders in the tech sector with guidance and assistance on how to perform better against their particular obligations and responsibilities regarding the human rights impacts of their business operations, sharing examples of technology companies' successfully incorporating human rights due diligence into their business activities. It also lays out how tech businesses should assess and manage the potential human rights risks that their product(s) may bring to various user groups.

This brief was developed to build awareness and understanding of the Nigerian tech ecosystem's engagement with human rights issues and responsibilities and to provide clarity and guidance to approach these throughpolicy, and technology design. The focus of this brief is to provide recommendations applicable across the whole technology sector. Human rights issues specific to other business sectors are outside the scope of this brief.

Section 1:
Background

1.1 The Nigerian tech ecosystem

According to new research referenced by the Nigerian Investment Promotion Commission NIPC, Africa-based tech startups have raised more than $2.9 billion since the beginning of 2021, with Nigerian startups raising $1.7 billion, or around 60% of the total[1]. In 2022 alone, Nigeria has seen around 340 new start-up founders and investment of $680 million into the Nigerian tech startup ecosystem[2], demonstrating that the Nigerian tech space is undoubtedly a promising and thriving industry. The sector has shown a continuous increase in investor interest in pushing the country's technological frontiers, and such investment has led to the ranking of many Nigerian tech firms as unicorns around the world, such as the popular talent management company Andela and other fintech companies like Opay, Interswitch and Flutterwave[3].

This pattern does not appear to be changing. As a result, regulators and other public stakeholders are paying closer attention to the nation's thriving tech ecosystem as they work to balance the advantages and disadvantages of the new markets and opportunities brought about by tech innovation and growth. There is a greater need, for example, to find a balance between software licensing and development and IP protections, and the promises of e-commerce and data and privacy risks; as well as between the opportunities brought about by social media, and safeguards for how to manage the spread of illegal content.

This increased pressure from regulators and policymakers can be seen in emerging policy developments in the technology space, such as the Nigeria Film and Video Censorship Board's attempt to regulate streaming platforms or the National Broadcasting Commission's efforts to democratize licensing regime for contents under the code of practice, which ultimately removed exclusivity protection for content[4]. Although the latter development has been overturned by the court, it shows how public stakeholders and agencies are beginning to pay attention to digital and data rights in the context of the Nigerian ICT space.

There is also growing awareness among stakeholders and operators in the Nigerian tech ecosystem of the importance of complying with emerging regulations and incorporating regulators' input into market-facing solutions. This is a promising trajectory for building responsible companies and the sustainability of the tech ecosystem at large.

1 Nigeria Tech Startups Raised $1.7 Billion in 2021
2 See Funding the Nigerian Start-ups: The New Techspace's Flight – THISDAYLIVE
3 SoftBank-Backed Andela Becomes $1.5 Billion Unicorn - Bloomberg
4 Court nullifies amended broadcasting code, says NBC has no power to prohibit exclusive contents | TheCable

1.2 Snapshot of the Nigerian tech policy, legal and institutional ecosystem

The Nigerian tech policy ecosystem features a number of different players proposing regulations and laws with a focus on data privacy, freedom of expression online, consumer rights, and platform governance. The most influential agencies include the Nigerian Information Technology development agency (NITDA), national human rights institutions, and the Central Bank of Nigeria (CBN).

Firstly, the Nigerian National Human Rights Institution and the National Human Rights Commission of Nigeria have led the development of Nigeria's National Action Plan on Business and Human Rights, a common tool for states to implement the UNGP-BHR. Nigeria is one of the few African countries to draft such a NAP[5]. During the drafting process, the Nigerian Human Rights Commission held a series of stakeholder consultations and collated input from CSOs on the need to include specific language about the technology; however, the final draft of the NAP omits these key phrases on the grounds that the draft will adopt a broad approach rather than being detailed.

In terms of regulators of tech companies in Nigeria, the Nigerian Information and Technology Development Agency (NITDA) is a state agency under the Ministry of Communication and Digital Economy that is in charge of regulating and promoting ICT development, and serves as the country's supervisory body in that regard, spearheading many compliance activities. It has issued a number of regulations relating to data privacy, including the Nigerian Data Protection Regulation (NDPR) in 2019, which is Nigeria's most important data protection policy document to date. It also issued two public advisories in 2020; one about data processing during Covid-19[6], and another about WhatsApp's privacy policy[7].

Outside of data privacy, NITDA has also recently issued a new code of practice for interactive computer service platforms and Internet intermediaries. This has proved controversial, with human rights defenders arguing that the process did not follow a proper consultation and that the draft code does not adequately safeguard the human rights of Nigerian internet users as highlighted by Paradigm Initiative in its response memo[8].

The Central Bank of Nigeria (CBN) is another active regulator in the Nigerian tech space. It has issued over 15 key relevant regulatory guidelines and frameworks for Nigeria's banking and finance sector[9] which affected Fintech, Lendtech, and Wealthtech startups, as well as e-commerce platforms. Some of these guidelines and regulations require regulated entities to adhere to privacy and data protection standards. There have also been increased calls to regulate the activities of companies in the digital lending industry after numerous complaints of violations of human and data rights and consumer protection laws. This has led to interest from the Federal Competition and Consumer Protection Commission (FCCPC) in extending the exercise of its regulatory powers over consumer rights on digital services – especially the telecommunications

5 Globalnap.org
6 NITDA inaugurates committee on Covid-19
7 NITDA's whatsapp privacy policy
8 NITDA Code Response Memo - Paradigm Initiative
9 TechHive advisory CBN guidelines

sector and financial services – as it discloses that the telecommunications sector ranked third in their complaints chart and that digital lending companies attracted a series of complaints for their violations of privacy, exploitative interest rates and absence of consumer feedback and complaints mechanisms[10].

When it comes to federal laws and legislation, The Data Protection Bill 2020 is the most recent proposal on data protection. The Bill seeks to improve data protection in Nigeria and to address the recurrent issue of abuse and misuse of data in the absence of an institutional framework[11]. The 2021 proposed Nigeria Startup Bill is also worth mentioning since it is a collaborative effort between Nigeria's tech sector and the Presidency to harness the potential of the digital economy through co-created rules. The goal is to give startups more regulatory certainty, easier access to funding, and a more conducive environment in which to grow and scale by reducing friction between regulators and ecosystem operators. The bill also proposes the creation of a National Council for Digital Innovation and Entrepreneurship, which would be responsible for cooperating with various regulatory organizations to guarantee that entrepreneurs receive assistance and incentives[12].

1.3 UNGP compliance for technology companies

All companies have come under more pressure in recent years to manage their operations so that their actions or policies do not violate others' human rights. Technology companies, in particular, have faced criticism for failing to minimize negative consequences for consumers' human rights. Often, technology companies' products or practices have resulted in direct human rights abuses; for example, in the deployment of biased Artificial Intelligence (AI) tools, the facilitation of hate speech spreading online, or the use of encrypted messaging services for organising human trafficking. However, sometimes, human rights violations have resulted not from the technology company's product or policies per se, but from forced compliance with a government request, for example, to surveil or hand over user data or to censor particular types of speech online. As a result, the lack of consistency and, in some cases, outright clashes between local and international laws and standards can pose a real problem for businesses trying to adhere to their responsibilities under the UNGP-BHR.

10 See Ikigai and TechHive's 2022 State of tech policy in Nigeria report
11 See also the state of tech policy in Nigeria report
12 Stakeholders webinar on the Nigerian startup bill https://www.youtube.com/watch?app=desktop&v=fJ4E6N7E41M

The UNGP-BHR

In 2011, the United Nations Human Rights Council unanimously endorsed the UN Guiding Principles on Business and Human Rights (UNGP-BHR), a set of standards that expound on the State's duty to protect individuals from human rights abuses by technology companies, the corporate responsibility to respect human rights, and the duty to remedy abuses. This document marked a milestone in international norms and principles of how human rights must be respected while conducting business operations, prescribing appropriate behaviour and measures to be undertaken by companies from all industries and by states.[13]

In order to provide more detailed guidance on how to implement the UNGP-BHR in the technology sector, the UN founded the B-Tech project following a consultation with members of civil society, business, governments, and other experts with the aim of providing authoritative advice and tools. The B-Tech project is devised according to four strategic emphasis areas; addressing human rights risks in business models, human rights due diligence and end use, accountability and remedy and lastly smart mix of measures of policy responses to human rights challenges linked to digital technologies[14].

The B-Tech Project observes that the UNGP's power lies in its potential to incite new ways of thinking. The UNGP-BHR makes space for new and innovative forms of collective action by all stakeholders and also recognises the complementary role of states and companies in the effective implementation of human rights frameworks in today's highly networked world[15].

Hence, a major obstacle to compliance with UNGP-BHR in Nigeria is the underreporting of digital human rights violations, which results in some issues going unrecognized or, even when reported, leaving out crucial details about the type of corporate action taken or the range of stakeholders impacted. It is logical that businesses would prefer to keep their challenges and unfavourable outcomes on their human rights indices, such as reported infractions, product flaws, and so on, hidden. But this has resulted in a shortage of study data on the types and prevalence of human rights abuses caused by technology companies in Nigeria, which in turn makes it difficult for effective policy breakthroughs.

Another obstacle to compliance is the lack of understanding of the UNGPs-BHR, especially among small and medium-sized businesses[16]. It is crucial that businesses learn to assess government requirements, including – but not limited to – those for anonymous data disclosure, authorized intercepts, data removal, and other things. They may need to defend human rights and resist attempts to halt services or restrict access.

13 National guidance document on BHR
14 OHCHR | B-Tech Project
15 https://www.ohchr.org/en/business-and-human-rights/b-tech-project
16 Humanizing the Business and Human Rights (BHR) Debate – Humanistic Management Network

Section Two

2. Conducting a responsible tech business in Nigeria

To comply with the UNGPs-BHR, technology companies in Nigeria must demonstrate that they are taking reasonable steps to prevent, mitigate and remediate harms to human rights caused by their products or services. Whilst there is no one size fits all framework for all tech businesses, each business can mould its human rights due diligence activities around its unique business model as well as its socio-economic and political context.

This brief highlights two lenses – technology and policy – through which businesses can work to apply the guiding principles to their specific business operations and practices. It isn't sufficient to only follow rules and regulations in order to be seen as compliant; the effectiveness of these standards depends on how successfully and consistently they are applied throughout the organizations' operational activities. Additionally, companies must modify them so that observing them will serve the actual demands of their business.

2.1 Policies

Policies communicate the connection between the company's visions and values and its day-to-day operations. In meeting the corporate responsibility to respect human rights, businesses are expected to express their commitment to meet this responsibility through a statement of policy or a policy commitment. The policy commitment explains how the company understands its responsibility to respect human rights, specifies the expectations and direction for those who are supposed to adhere to or implement the policy, and the strategies it intends to employ to ensure respect for human rights across its policies, processes, and value chains.

The policy on human rights must also address how the business is conducting the two types of processes required by the UNGP-BHR; due diligence and remediation. A due diligence process identifies impacts and potential impacts on human rights, establishes a reporting system to detect and address human rights issues, and accounts for how the business will prevent or mitigate any human rights violations. As part of human rights due diligence activities, there may be a need to conduct internal capacity-building on human rights, to develop robust processes for addressing serious human rights risks once detected, or to incorporate specific narrow and technical questions on the human rights implications of any new technologies into impact assessments prior to deployment. Whether it's protected speech, internet connectivity, algorithmic impacts, or business models, each must be thoroughly investigated as part of a

complete due diligence process[17].

A remediation process is the procedures that must be followed in order to prove that a right to remedy exists and to identify the type of remedy that must be offered in order to comply with international standards. Among the Guiding Principles, Principle 29 states, "To make it possible for grievances to be addressed early and remediated directly, business enterprises should establish or participate in effective operational-level grievance mechanisms for individuals and communities who may be adversely impacted." Principle 30 stipulates "Industry, multi-stakeholder and other collaborative initiatives that are based on respect for human rights-related standards should ensure that effective grievance mechanisms are available"[18].

To meet international law standards on remedies for breaches of human rights, the remedy must be an effective one as mentioned. The key elements of an "effective" remedy in international legal terms are that the remedy should be provided in a timely manner and without any undue delay (particularly important in cases where the value or usefulness of a remedy will decline or disappear over time); proportionate to the gravity of the breach and the harm suffered; and delivered in such a way that there is "full and effective reparation"[19]

In view of this, policy tools must advance in tandem with a company's technological capabilities this is to say that, the more complex or far-reaching the technological services and products that the company provides, the more robust and nuanced its human rights policies and due diligence processes must be, and the more it needs to invest in its employees' understanding of human rights risks and its remediation mechanisms for its customers. Sometimes information sharing between companies is useful to see how they've approached a similar problem or the principles or process they took on a particular issue. However, a "copy and paste" strategy is unlikely to be effective or lead to full compliance with the UNGP-BHR as different companies have different needs and obstacles

2.2 Technology

Beyond amending internal company policies to ensure appropriate due diligence and remediation mechanisms are in place for potential human rights impacts, it may also be necessary for companies and stakeholders to critically evaluate the human rights impacts of the technology, service or product itself and to make changes to technological systems to adhere to human rights standards. Sometimes companies will voluntarily amend their technology or products to address human rights impacts, but it may also be necessary for governments to require them to do so, for example, by mandating a Privacy or Safety by Design approach. Such approaches call for the embedding of safeguards for technology users in the initial stages of design processes and not as an afterthought or when urgently needed to mitigate emerging risks.

A 'Safety by Design' approach indicates that users can easily navigate and use safety controls and that content policies are understandable to all and fairly enforced. It also

17 Human Rights Due Diligence
18 BHR lawyers- engagement and remedy guidelines
19 B-tech access-to-remedy-concepts-and-principles

demands that technology service providers take responsibility for any safety risks that emerge from their products[20]. A "Privacy by Design" approach means integrating data protection measures and key privacy safeguards into all stages of development and design of a technology product. It emphasizes that privacy is determined by context and that different safeguards should be embedded to protect diverse sets of users[21]. This approach is also legally required by the Nigerian Data Protection Regulation (NDPR).

Whilst these approaches to human-rights-respecting technology design have certainly resulted in some positive amendments by companies around the world, and in Nigeria, companies must tread carefully because technical safeguards incorporated into the settings and interfaces of these technologies can only protect human rights to a limited level, and may not defend against misuse of the services for malicious purposes.

Synopsis

Some companies selling artificial intelligence software or technologies suggest that they can be used to eliminate unconscious bias and discrimination from public and private decision-making processes, such as automated hiring programmes. Yet a closer investigation into the technological mechanisms underpinning such products shows that sometimes the AI tool may, in fact, embed discriminatory assumptions made by programmers or biases in the underlying data used to train it and may therefore reinforce, rather than reduce, discrimination.

As a result, human rights bodies have issued standards and guidance on how human rights, including the right to freedom from discrimination, should be safeguarded in AI development, and it may be that a comprehensive governance framework is needed to fully address the risks of such systems[22]. An AI company offering automated hiring programmes should, through its due diligence processes, examine all stages of the chain of product development, including data collection, labelling and categorizing machine training and testing, and deployment in real-life contexts, investigating the potential for discrimination at each stage of the processes and amending the technical processes accordingly.

20 Digital inclusion is not just an add-on for tech policy and development

21 See also Enhancing Internet freedom and human rights through responsible business practices - Government.se

22 Danish report on tech giant and human rights

Section Three:
Policy Recommendations for tech companies and relevant stakeholders

3.1 Recommendations for the tech community

Senior executives and people holding strategic positions at tech companies should have a thorough understanding of both international and national regulations and tools regarding human rights that apply to their business types and act accordingly.

Tech companies should make sure their operations are transparent. This may be achieved through annual transparency reports, clear terms of use and customer service agreements, notification of decisions that affect customers, publication of any government requests, etcetera. Certain strategic, operational actions must undoubtedly stay classified, but instruments like the UNGP-BHR reporting form may be quite helpful in assisting them in carrying out their mandate.

Investment communities, for example, Angel Investors, seed funders and incubators in Nigeria, should ensure that the companies under their programs have a policy plan to respect human rights and that relevant measures are integrated into product design, corporate business strategy, risk management, and reporting.

Tech corporations should involve civil society organizations more in their human rights policy formulation in order to double-check their compliance with UNGP-BHR and other frameworks in their business models and daily operations. One of the advantages of this is, in the event that "unreasonable" requirements are made by governments, businesses can easily coordinate with the CSOs and make combined submissions.

3.2 Recommendations for government

To ensure compliance with their responsibilities under the UNGP-BHR, government regulators, as well as lawmakers, should hire specialists or confer with consultants in the area of safeguarding human rights. The quality of tech policy-making could be improved through greater access to expertise and a better understanding of critical and emerging technologies at all levels of governance, including the interdependencies of these technologies with broader social, security, economic, and environmental systems. This will enable them to seek assistance as needed in order to verify that their actions and procedures are compliant.

For the sustainability of government regulation of the tech sector with respect to human rights, the regulators should engage as much as possible with tech companies and digital rights CSOs geared towards charting a way forward for all parties in the country's development and economic interest. This will inevitably advance the democratization of the governance and regulatory process in the sector.