SECURITY PLAYBOOK OF DIGITAL AUTHORITARIANISM IN NIGERIA

VICTORIA IBEZIM-OHAERI
LOTANNA NWODO
NGOZI NWOSU-JUBA

JOSHUA OLUFEMI
OLUSEYI OLUFEMI
TIERS

SECURITY PLAYBOOK OF DIGITAL AUTHORITARIANISM IN NIGERIA

Authors
Victoria Ibezim-Ohaeri | Joshua Olufemi | Lotanna Nwodo | Oluseyi Olufemi | Ngozi Juba-Nwosu | TIERS

Additional research
Charles Mba | Ode Uduu | Phillips Akintola | Olufunso Alufoge | Ohotuowo Ogbeche | Olufunso Alufoge | Omolara Oriye

Edited by
Immanuel Ibe James Anyanwu

Reviewed by
Tony Roberts | Steven Feldstein | Sarah Gordon | Lydia Cocoon | James Savage

Graphics design
Emmanuel Ogunleye

Published by
ACTION GROUP ON FREE CIVIC SPACE

DECEMBER 2021

ACKNOWLEDGEMENT

The Security Playbook is a three-part research study collectively undertaken by eleven (11) members of the Action Group on Free Civic Space (AGFCS) to identify and analyze the use and misuse of the security agenda to shrink the civic space in Nigeria. The eleven organizations are SPACES FOR CHANGE |S4C, Interactive Initiative for Social Impact (Dataphyte), The Initiative for Equal Rights (TIERS), Justice Rights Initiative (JRI), Centre for Citizens with Disabilities (CCD), Vision Spring Initiatives (VSI), World Impact Development Foundation (WIDEF), Rule of Law and Accountability Advocacy Centre (RULAAC), Youths and Environmental Advocacy Centre (YEAC), Building Blocks for Peace Foundation (BBforPeace), SB Morgen Intelligence (SB Intelligence). S4C, Dataphyte, TIERS and VSI co-authored the first part, The Security Playbook of Digital Authoritarianism, focusing on the use of technologies, regulations, and other computerized devices to jeopardize the right to privacy, censor free speech and stifle dissent in the online civic space in Nigeria.

We are grateful to the research teams from the various organizations who took part in gathering primary and secondary data across the six geopolitical zones in Nigeria. The research teams comprise full and part-time staff, consultants, field enumerators, interns and volunteers in these organizations as well as members of the AGFCS all over the country. We are thankful to the external researchers, Lotanna Nwodo and Ms. Ify A., the team at Green Spaces Innovation and InfoTrack Ltd. for extensively reviewing and synthesizing the truckload of reports collated across the country into a common narrative.

Many thanks to the following persons whose backend support and robust fieldwork greatly eased the implementation of this collective action research project: Joshua Olufemi, Oluseyi Olufemi, Ode Uduu and Charles Mba (Dataphyte researchers), Ngozi Nwosu-Juba, Tobi Ayodele, Anita Graham and Folake Kuti (VSI researchers and consultants), Ohotuowo Ogbeche, Olufunso Alufoge, Omolara Oriye, Olumide Makanjuola, Dr Michael Akanji, Akudo Oguaghamba, Juliet Nnedinma Ulanmo, Fisayo Owoyemi, Bala Mohammed Salisu, Olubiyi Oludipe, Amara the Lesbian, Ani Kayode Somtochukwu and Nwamaka Mbagwu (TIERs research team and enumerators); and Zikora Ibeh (S4C's Program Officer, Defending the Civic Space), David Olakunle and Rejoice Imozemeh (S4C's Finance Team) and Olusola Olufemi (S4C's Research and Communications Officer). S4C's Executive Director, Victoria Ibezim Ohaeri, supervised and coordinated this project from start to finish including editing, proofreading and absorbing vital feedbacks on preliminary drafts to ensure a final appreciable work.

We deeply thank friends and allies at various international research and advocacy organizations—specifically Dr. Tony Roberts of Institute for Development Studies (IDS), Steven Feldstein & Sarah Gordon at the Carnegie Endowment for International Peace, Lydia Cocom & James Savage of the Fund for Global Human Rights (FGHR)—who reviewed several drafts of this report and provided guidance for restructuring the order and flow of the overall argument.

The research team leveraged the diversity of connections and expertise within the Action Group on Free Civic Space to reach and capture the disparate experiences of civic actors actively using digital platforms to push for social change in the nearest to the farthest locations across the country. For giving us the wings to fly and laying a solid foundation for the Action Group on Free Civic Space to thrive, we generously thank FGHR for the generous support which made this collective action research project possible. We are super grateful to James Savage and Lydia Cocom of FGHR for offering us invaluable guidance, assistance, support and feedback throughout this journey.

TABLE OF CONTENTS

ACRONYMS

ABU:	Ahmadu Bello University
AGFCS:	Action Group on Free Civic Space
APC:	All-Progressives' Congress
BMC:	Buhari Media Center
BSS:	Business Support Services
BVN:	Bank Verification Number
CAMA:	Corporate and Allied Matters Act
CBN:	Central Bank of Nigeria
CCTV:	Closed Circuit Television
CDD:	Customer Due Diligence
CEIR:	Centralized Equipment Identity Register
CDMA:	Code Division Multiple Access
COVID19:	Coronavirus Pandemic
CSOs:	Civil Society Organizations
CT:	Counter Terrorism
DDOS:	Distributed Denial of Service
DDRR:	Demobilisation, Disassociation, Reintegration Reconciliation
DG:	Director General
DIA:	Defence Intelligence Agency
DMS:	Device Management System
DNFIs:	Designated Non-Financial Institutions
DNCR:	Department of National Civic Registration
DNS:	Domain Name Server
DSS:	Department of State Services
EFCC:	Economic and Financial Crimes Commission
EUGDPR:	European Union General Data Protection Regulation
FATF:	Financial Action Task For
FIU:	Financial Intelligence Unit
FMoCDE:	Federal Ministry of Communications and Digital Economy
FoE:	Freedom of Expression
FRSC:	Federal Road Safety Commission
FTK:	Forensic Toolkit
GAFI:	Groupe d'Action Financiere
GSM:	Global System for Mobile Communications
HRDs:	Human Rights Defenders
IEC:	Information, Education and Communication
INEC:	Independent National Electoral Commission
IPPIS:	Integrated Payroll and Personnel Information System
IP:	Internet protocol
ISP:	Internet service provider
IPOB:	Indigenous Peoples of Biafra
ISPS:	Internet Service Providers
JAMB:	Joint Admission Matriculation Board
JTAB:	Joint Terrorism Analysis Branch
LGBTQ:	Lesbian, Gay, Bisexual or Transgender

MENA:	Middle East and North Africa
NACTEST:	National Counter Terrorism Strategy
NBC:	National Broadcasting Commission
NCC:	Nigerian Communications Commission
NCCP:	Nigerian Cloud Computing Policy
NCDC:	Nigeria Centre for Disease Control
NDEPS:	National Digital Economic Policy and Strategy
NDPR:	Nigerian Data Protection Regulation
NECO:	National Examination Council
NGO:	Non-Governmental Organization
NIMC:	National Identification Management Commission
NIN:	National Identity Number
NITDA:	National Information Technology Development Agency
NPC:	Nigerian Press Council
NPOs:	Non-Profit Organizations
NSA:	National Security Adviser
ONSA:	Office of the National Security Adviser
PLAC:	Policy and Legal Advocacy Centre
PTCIJ:	Premium Times Centre for Investigative Journalism
SARS:	Special Anti-robbery Response Squad
SERAP:	Social and Economic Rights Accountability Project
SIM:	Subscriber Identity Module
SNG:	Save Nigeria Group
SSS:	State Security Services
TELCOS:	Telecommunication Companies
TPA:	Terrorism Prevention Act
UFED:	Universal Forensic Extraction Device
UNIBEN:	University of Benin
UNSC:	United Nations Security Council
UN:	United Nations
VoIP:	Voice over Internet Protocol
VPN:	Virtual Private Networks
WAEC:	West Africa Examinations Council

METHODOLOGY

The Security Playbook is a three-part research study collectively undertaken by eleven (11) members of the Action Group on Free Civic Space (AGFCS) to identify and analyse the use and misuse of the security agenda to shrink the civic space in Nigeria. S4C, Dataphyte, TIERS and VSI co-authored the first part, The Security Playbook of Digital Authoritarianism, focusing on the use of technologies, regulations, and other computerized devices to jeopardize the right to privacy, censor free speech and stifle dissent in the online civic space in Nigeria. The eleven organizations are SPACES FOR CHANGE |S4C, Dataphyte, The Initiative for Equal Rights (TIERS), Justice Rights Initiative (JRI), Centre for Citizens with Disabilities (CCD), Vision Spring Initiatives (VSI), World Impact Development Foundation (WIDEF), Rule of Law and Accountability Advocacy Centre (RULAAC), Youths and Environmental Advocacy Centre (YEAC), Building Blocks for Peace Foundation (BBforPeace), SB Morgen Intelligence (SB Intelligence).

Research teams comprising full and part-time staff, consultants, field enumerators, interns and volunteers in these organizations used a mixed method to gather primary and secondary data from the six geopolitical zones in Nigeria. They conducted extensive desk research studies, incident-tracking, field visits, key informant interviews, focus group discussions, surveys and administered questionnaires to targeted respondents. Incidents tracked and documented on online databases such as the Closing Spaces Database – www.closingspaces.org, Press Freedom Index, CIVICUS Monitor, and other relevant news sources, also helped to provide real evidence of digital suppression and curtailment of internet freedoms in Nigeria.

The AGFCS research team converged in July 2021 to kick off the collaborative study with a strategy meeting aimed at co-creating and agreeing on the research design, methodology, deliverables, reporting timelines and regulatory policies that would guide the implementation of the research project. After three (3) months of intensive study and data collection, researchers converged again in September 2021 to present their preliminary findings to a rich pool of civic space experts, security experts, research consultants, media practitioners, and representatives from local and international non-governmental organizations. The validation meeting afforded stakeholders an opportunity to evaluate, critique, and contribute to the draft report findings and collectively identify entry points for disrupting and reforming the security architecture to defend the civic space in Nigeria.

At regional press conferences held across the country in October 2021 to present the preliminary findings, journalists, civil society practitioners, representatives from relevant government parastatals such as the National Human Rights Commission and members of the public reviewed, critiqued information gaps and offered useful contributions and recommendations. The truckload of data gathered from across the country were reviewed and synthesized into a common report. Synthesized drafts of the research report were further subjected to rigorous scrutiny by independent peer reviewers - comprising experts at Institute for Development Studies (IDS), Carnegie Endowment for International Peace, and the Fund for Global Human Rights (FGHR). They reviewed several drafts of this report and provided technical guidance for restructuring the order and flow of the overall argument.

Ultimately, the three Security Playbook reports join the collection of existing literature on counterterrorism narrative and civic space highlighting opportunities that empower all stakeholders in the Nigerian civic space with the right attitude and information to reconcile national security objectives with democratic values.

INTRODUCTION

This report presents the findings of a three-part study examining the overapplication or abuse of security infrastructure to crack down on civic actors in Nigeria. Undertaken by 12 member organizations of the Action Group on Free Civic Space (AGFCS), the research documents how security rhetoric and misuse of counterterrorism laws and tools are potentially becoming the dominant driver of closing the civic space in Nigeria. In this first part, the report identifies and documents the new technologies, regulations, laws and tactics employed by state actors and their corporate collaborators to repress the constitutionally protected freedom of expression, assembly, association, and the right to privacy.

Currently, Nigeria is facing serious security challenges that threaten to tear its sovereign fabric apart. Religious fundamentalism, insurgency, banditry, farmer-herder conflicts, kidnapping and secessionist agitations ravage several states, with the northern region of the country worst hit by the violent security crisis. Combating the mounting insecurity necessitated huge budgetary allocations to national security, accompanied by the massive procurement of sophisticated crime-fighting technologies and military equipment. State actors have taken advantage of their unfettered access to these new technologies to either expand pre-existing policing powers or award themselves new surveillance powers.

This report builds evidence of a Security Playbook of Digital Authoritarianism by showing how the massive financial resources, equipment and technologies originally procured in the name of counterterrorism and curbing insecurity have been diverted to monitor the movement of citizens, track activities of civic actors online, intercept private communications, restrict online civic space, and limit the ability of civic actors to organize, associate and assemble freely. The popular tactics include legal restrictions, misuse of surveillance technologies, distributed denial-of-service (DDoS) attacks, internet protocol (IP) blocking, internet shutdowns, biometric data collection and social media bans. Others include spying on activists and opposition politicians, and coordinated cyber-attacks, especially the hacking of the servers and websites of media and civil society watchdogs.

State actors could not have recorded considerable successes in their restrictive adventures without the cooperation of telecommunication companies (Telcos), internet service providers (ISPs), content moderation platforms, private companies, including foreign suppliers of surveillance technologies and local as well as state regulatory agencies. The report provides detailed accounts of the specific companies supplying surveillance technologies to the Nigerian state for repressing fundamental human rights. With the limited checks and balances in place to curtail restrictions on open democracy, internet freedoms, privacy and communication rights, surveillance capitalists and technology suppliers are exploiting the drift towards authoritarianism and the regime's lust for unfettered power to make profits. To make matters worse, these restrictions on civic freedoms and privacy rights wear the toga of “national security”, “intelligence” and “secrecy,” making it easier for culprits to escape scrutiny and accountability.

A deep dive into the state's most popular techniques and tactics explains why digital repression, including surveillance abuses in the country is on the rise, and flags the subsequent reforms/steps needed to counter these trends. The report concludes by proffering recommendations to end misuse of digital technologies to stifle dissent, mitigate the effects of illegal surveillance practices, and increase the ability of citizens to freely access information and exercise their legal freedom of expression and right to privacy.

NIGERIA: THE SOCIAL AND POLITICAL CONTEXT

·Nigeria's six geographical regions engulfed by insecurity

Although the northern region is the epicenter of violent crimes, insurgency and terrorism, the country's security landscape has radically transformed over the past five years, with the six geographical regions overwhelmed by varying degrees of internal security challenges. The insecurity in the North-West region particularly devastating the states of Kaduna, Katsina, and Zamfara is caused by a confluence of factors ranging from poorly managed conflicts between Fulani pastoralists and farming communities, proliferation of light weapons, cattle rustling, illegal gold mining activities and Boko Haram-ISWAP's 10-year insurgency. As these conflicts soared, numerous armed groups working independently of each other—collectively identified as "bandits" by the Nigerian government—have emerged.[1] These groups are responsible for kidnappings along highways, mass abductions and indiscriminate attacks on communities. According to reports, at least 1,031 Nigerians were killed, 390 abducted in 205 incidents across 34 states of the country in June 2021 alone. [2]

Historically entrenched injustices against the Igbo of south-east Nigeria are fuelling the separatist agitations in the zone. The situation is worsened by the unwillingness of the Nigerian authorities to revamp the country's federating set-up in ways that address the real and perceived marginalization of the region, and the use of brute force in dealing with their predominantly non-violent agitations. The secessionist campaigners, Indigenous Peoples of Biafra (IPOB), have been proscribed and designated a terrorist organization, with hundreds of members killed by security forces and their leader, Nnamdi Kanu, still in custody and facing terrorism charges. In the oil-rich south-south region, irresponsible oil exploration activities by multinational corporations, environmental degradation, underdevelopment, poverty, youth restiveness and unemployment lie at the root of the protracted violent conflicts in the area. The south-west's determination to take charge of their own economic independence and regional security to curtail the deadly invasion and land encroachments by herdsmen is igniting fresh demands for secession.

Despite the peculiarities in the conditions responsible for the insecurity in different parts of the country, the common denominators are bad governance, widespread injustice, poverty, youth unemployment and political corruption.

·National elections charge the political atmosphere

2023 national elections are lurking around the corner and the political temperature in the country is already charged. Hastily made budgetary revisions and the procurement of surveillance technologies reach their peak whenever the nation prepares for elections. It is the time fierce and obscenely expensive electoral contestations between political heavyweights rouse candidates to know what their opponents are saying or planning to do. Old and new start-ups in surveillance systems around the world latch onto the charged electoral atmosphere to sell spying technologies to willing and ready customers, including heads of federal and state governments in Nigeria gearing up for the national elections. Beyond using the surveillance technologies to spy on opposition politicians to weaken their political capital, the importation of hacking expertise and tools has also become a lucrative industry and conduit pipe for politicians and their cronies to divert and siphon public funds offshore.

1 TheCable, Over 150 groups of bandits operate in the forests, says Masari, September 21, 2021, Accessed via https://www.thecable.ng/there-are-over-150-groups-of-bandits-in-the-forests-says-masari

2 Ihuoma Alo, HumAngle, 1,031 Killed, 390 Abducted In 205 Incidents Across 34 States In Nigeria – Report; https://humanglemedia.com/1031-killed-390-abducted-in-205-incidents-across-34-states-in-nigeria-report/

·Civic actors congregate offline and online, speaking truth to power

It is against this backdrop that civic actors are campaigning against impunity, bad governance, demanding accountability for widespread injustices while mounting pressure on federal and state authorities to address issues of public concern. More recently, new entrants into the civil society comprising both individuals and organizations, including digital groupings and assemblies, are taking on a range of issues, and representing causes, transnational movements and issues-based coalitions. Capitalizing on the advancement in information and communication technologies, civic actors are increasingly congregating online, taking advantage of the social media platforms and hashtags (#) to ask critical questions about democratic governance, campaigning for good governance, reforms, corporate accountability, and numerous other causes. The most popular hashtags coordinated by notable digital movements in Nigeria include #OccupyNigeria, #OccupyNASS, #SaveNigeriaGroup (SNG), #BringbackOurGirls, #ArewaMeToo, #OurMumuDonDo and #EndSARS. More recently, the youth-powered #EndSARS protests moved from online expressions of rage to peaceful street demonstrations in October 2020 that shut down the nation's commercial and political hubs for several days.[3]

·State actors intolerant of criticism are pushing back

State actors and institutions have responded to criticism and heightening accountability demands by engaging various tactics to silence critics, criminalize dissent and undermine important watchdogs working to strengthen democratic processes and institutions. For the most part, they have subscribed to the proliferation of repressive laws designed to limit free expression, assembly and association rights especially on social media platforms.[4] From the indefinite suspension of Twitter in Nigeria in early June 2021 to the Social Media Bill[5] to the Hate Speech Bill,[6] to the proposed legislative amendments to the extant Nigerian Press Council (NPC) Act and the National Broadcasting Commission (NBC) Act currently under parliamentary consideration, laws have been formulated, reviewed or reinterpreted by successive governments to criminalise information sharing. These laws aim to sanction and restrict media content and independent reporting that are critical of the government and public officers on both the print and electronic channels.

With the same vigour deployed to resist offline/street demonstrations against misrule, the Nigerian state is also responding by framing organized online dissent as "terrorism", "treason", "rebellion". In this connection, activists posting commentary critical of the government and political officials on Facebook and Twitter have been arrested, charged with terrorism and jailed. Existing anti-terrorism, cyber laws and data regulations are usually invoked to justify these clampdowns. Broadcast media stations have been slammed with sanctions and fines, ethnic and religious agitators designated as terrorists while extreme force has been used to quell public assemblies in violation of national and international human rights obligations. Between 2015 – 2021, the Closing Spaces Database documented over 300 incidents of crackdowns on the freedom of expression, assembly and association in Nigeria. 106 incidents of clampdowns on freedom of association and assembly were documented during this period. Similarly, the freedom of expression—comprising press freedom (120 incidents) and the freedom of speech

[3] Action Group on Free Civic Space, #EndSARS: POLICE BRUTALITY, PROTESTS AND SHRINKING CIVIC SPACE IN NIGERIA, 2021, Accessed via https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/
[4] Ibezim-Ohaeri, Confronting Closing Civic Spaces in Nigeria, SUR 26 , v.14 n.26, 129 - 140, 2017
[5] Protection From Internet Falsehoods, Manipulations and Other Related Matters Bill, 2019
[6] National Commission for the Prohibition of Hate Speeches Bill 2019

(83 incidents)—bear the highest share of repressive activities in the Nigerian civic environment.[7] Other categories of restrictions documented include digital closure & surveillance, politically motivated crackdowns, restrictive legislation etc.

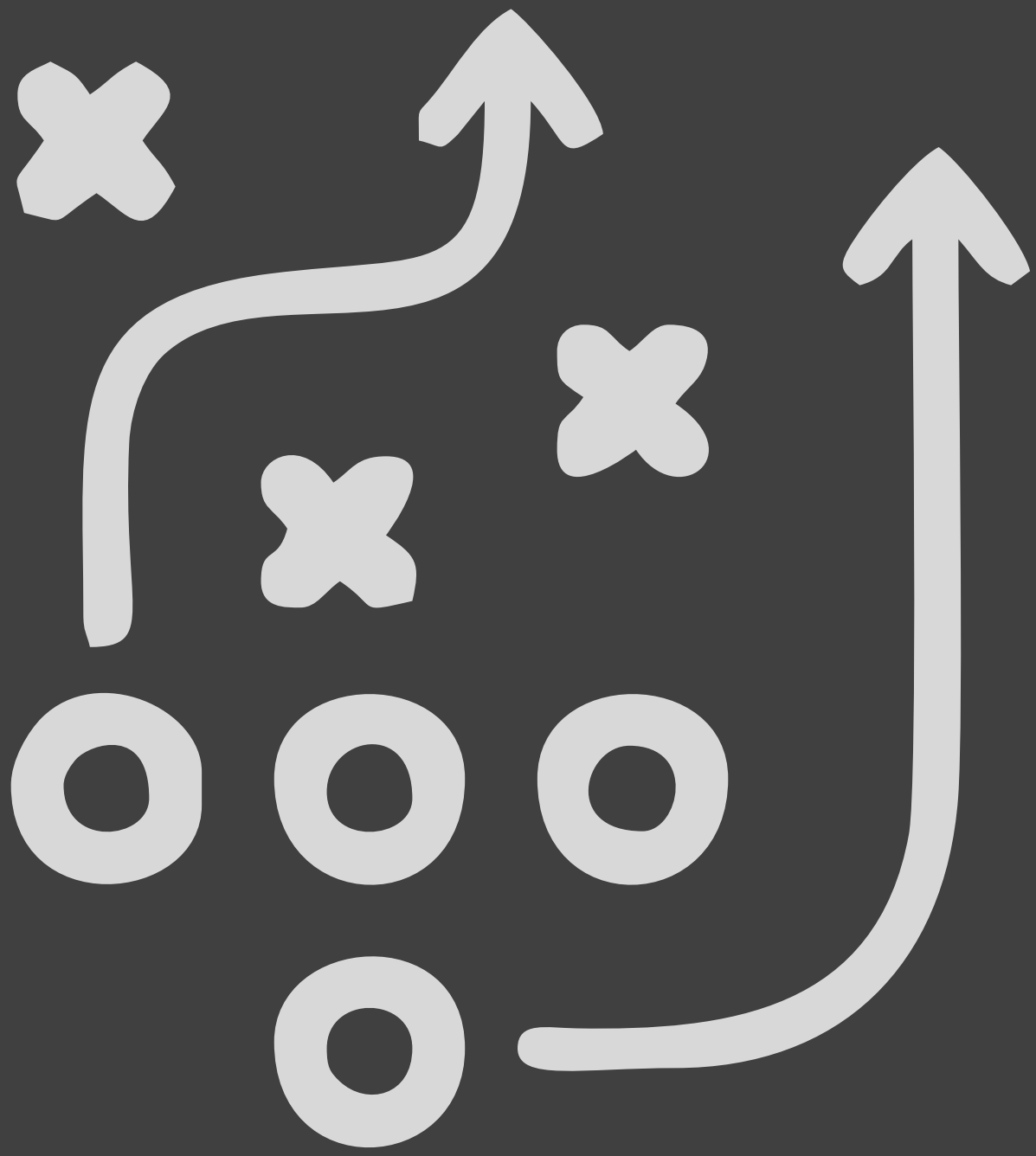
The influence of foreign powers and corporations

In many ways too, global and local geopolitics have given a boost to the abuses of state power. Of special significance is the sharp and soft influences of universalist legal norms framed around the objective of countering terrorism and defending national security. Not only that, some of these repressive tactics have been copied from the playbook of repressive regimes in other jurisdictions. Consistent with the intrusive data gathering patterns observed in other countries like the United States, United Kingdom, Turkey, China, Russia, and several Middle East and North Africa (MENA) countries, Nigeria has introduced initiatives designed to profile individuals and groups (through the capture of the people's biometric signatures and syncing with their financial/banking/voting information, as well as their phone/internet/social media accounts. In addition, private corporations—like the Israel-based company Cellebrite and FTK and the U.S-based Access Data Group—sell sophisticated forensic technologies such as the Universal Forensic Extraction Device (UFED) and Forensic Toolkit (FTK) to law enforcement agencies around the world.[8] There is evidence that these two companies are operating in Nigeria.

There is mounting evidence showing how these biometric information, forensic technology and surveillance gadgets either collected or procured in the name of countering terrorism and threats to national security have been used to curtail internet use, arbitrarily surveil and limit the activities of the political opposition, journalists and against civic actors demanding accountability and pushing for social justice. Some of these technologies have been used to retrieve and decode information from devices such as phones and computers of civil rights campaigners and journalists. Proceeding upon this premise of the misuse of the national security rhetoric coupled with the rising diversion of the counterterrorism architecture, this research looks into this Security Playbook of Digital Authoritarianism to investigate the exploitation of digital technologies to silence dissent, mount surveillance and limit civil society in Nigeria, flagging who is doing what, how they are doing it, and how the targets are pushing back on these curtailments.

7 Closing Spaces Database (www.closingspaces.org), Tracking Civic Space Incidents in Nigeria: 2015-July, 2021 https://closingspaces.org/tracking-civic-space-incidents-in-nigeria-2015-july-2021/

8 Abdulkareem Mojeed, Premium Times, Nigerian military using surveillance technology to spy on Nigerians – CPJ (2019) Accessed via https://www.premiumtimesng.com/news/top-news/359898-nigerian-military-using-surveillance-technology-to-spy-on-nigerians-cpj.html



CHAPTER ONE

NIGERIA'S DIGITAL LANDSCAPE: THE TECHNOLOGICAL BOOM, REGULATIONS AND THE EMERGENCE OF ONLINE CIVIC SPACE

© *Freedom House*

1.1. The Technological Boom of the 90s

Nigeria began to witness significant turnarounds in its digital landscape following the deregulation of the telecommunications industry in the 90s, which dismantled state-run monopolies and opened the markets to new competitors and suppliers of digitized goods and services. The deregulation of telecommunications particularly triggered radical shifts in the country's digital economy, culminating in significant investments by telecommunications companies in mobile telephony and internet services. The ICT sector in Nigeria also witnessed 54,000 kilometres of backbone and middle-mile fibre deployed with significant duplication, and 2G, 3G and 4G deployed at 89%, 75% and 45% respectively. [9]

Telecom operators use four major technologies to support telecommunication services in Nigeria. The technologies are Global System for Mobile Communications (GSM), Code Division Multiple Access (CDMA), Fixed Wired (landline) and Voice over Internet Protocol (VoIP). Four major mobile network operators (MNOs) in Nigeria use the GSM technology to provide telecommunication services to subscribers. They are Airtel, MTN, Globacom and 9Mobile. These MNOs continue to consolidate on their gains and market share,[10] with MTN currently dominating the GSM market with over 73 million subscribers (39.2%). This is closely followed by Airtel with approximately 51 million subscribers (27%).

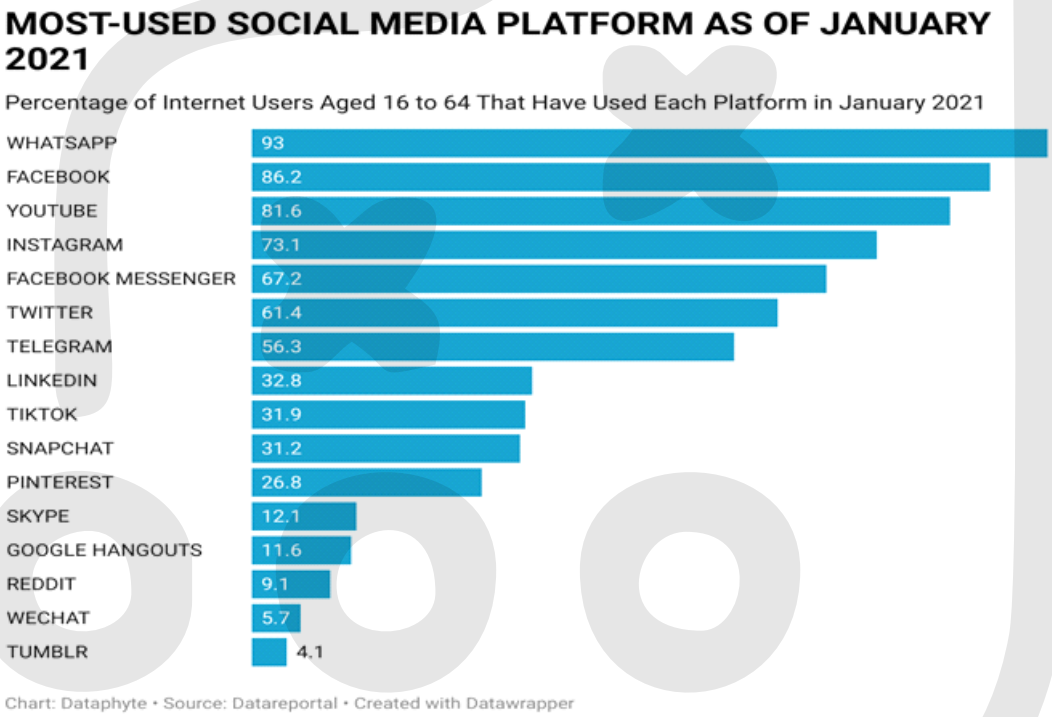
As of December 2000, Nigeria had 450,000 connected fixed lines, no connected digital mobile line, 18 operating Internet Service Providers, 9 active licensed fixed-line operators, and 1 licensed mobile line operator. By 2021, the figure has increased to 298 million digital mobile lines out of which 187 million are active, 65 operating internet service providers, over 80 licensed fixed-line operators and over 14 licensed mobile line operators.

(NCC, 2021b)

9 Nigerian Communications Commission, Challenges of Technology Penetration in an Infrastructure Deficit Economy (Nigeria Perspective), 2021: Accessed via https://www.ncc.gov.ng/documents/976-challenges-of-technology-penetration-in-an-infrastructure-deficit-economy-nigeria-perspective/file

10 NCC Statistics and Reports (Industry Statistics)2021 (ibid). See https://www.ncc.gov.ng/statistics-reports/industry-overview#gsm-2

The evolution of the internet, mobile telephony and the various hybrid telecommunications systems laid the foundation for real-time social connections and political influence on digital spaces to wax stronger. With the youth bulge and massive disruption in the country's technological landscape, many promising startups majoring in fintech, entertainment, media and social activism have sprung up. A new society populated by individuals and groups called netizens (a user of the internet, especially a habitual or keen one.) emerged on these digitalized platforms, popularly known as social media, engaging in free, uncensored expressions. According to one report, Nigerians have an average of seven social media accounts per internet user and spend an average of 3 hours and 41 minutes per day on social media.[11] The most popular social media platforms used in Nigeria are WhatsApp, Facebook, YouTube, Instagram, Facebook Messenger, Twitter, Telegram, and LinkedIn.



As shown in the above table, WhatsApp, Facebook and YouTube platforms are the most-used social media platforms by 93%, 86.2% and 81.6% respectively among users aged 16-64 in 2021. These platforms are followed by Facebook messenger, Twitter and Telegram, while Tumblr is the least used. The Facebook company, nowMeta Platforms, Inc. owns four out of the top five social media favorites of Nigerians, highlighting how much power and control private tech companies have. Not only are these platforms owned and controlled by foreign corporations, concerns for data privacy often emanate from algorithm configurations that are typically trained to gather personal data enabling third parties, especially advertisers, to target their messages and products to specific audiences.

11 Simon Kemp, DATAREPORTAL: Digital 2021:Nigeria, Published 11 February 2021, Accessed via Https://Datareportal.Com/Reports/Digital-2021-Nigeria

1.2. The Era of Hashtags and Digital Assemblies

With more Nigerians owning smartphones and gadgets now than ever, Nigerian civic actors evolved from rallying the populace using placards, pamphlets, posters, print and electronic media to using social media and other digital platforms to expose government's excesses, speak truth to power, demand accountability from powerful state and corporate actors and ultimately mobilize citizens for behavioural, cultural and regime change. Netizens have now revolutionized the traditional organizing techniques usually deployed for street remonstrations and begun to convene digital assemblies to express their widespread disaffection and anger with the underperformance of political and business leaders. In this context, digital assemblies refer to both the spontaneous or organized gatherings of large numbers of concerned citizens or social media users on internet-enabled platforms for the purpose of calling worldwide attention to shortcomings in the society. At these assemblies coordinated by means of digital communication technologies—such as mobile phones, cameras, or social media networking sites and hashtags—civic actors galvanize urgent actions, influence change and spread the word across continents at great speed and less cost. The hashtags of some of the notable digital assemblies in Nigeria include:

#OccupyNigeria: A youth-led national protest against the removal of petroleum subsidy by the Goodluck Jonathan administration in 2012. The Twitter-fuelled protests later spilled over to the streets, snowballing into massive protests around the country, including in major cities like Lagos, Abuja, and Kano.

#OccupyNASS is an organised demonstration led by the Citizen United for Peace and Stability against corruption and insensitivity of the Nigerian legislature and its leadership. The hashtag spiralled into offline demonstrations staged in front of the National Assembly complex in Abuja, Nigeria, demanding among other things, the reduction of the excessive budgetary allocations to federal lawmakers and the immediate resignation of former Senate President Bukola Saraki for alleged false declaration of assets.

#SaveNigeriaGroup (SNG) was formed in 2010 by Nigerian elites in the bid to save Nigeria from possible power hijack following the delay in handing over presidential powers to the then Vice-President after the demise of President Yar'Adua according to the dictates of the Nigerian 1999 Constitution.

#BringbackOurGirls Movement started in the wake of the abduction of about 276 female students from the Government Girls Secondary School, Chibok, Borno State. The hashtags trended heavily on Twitter and mutated into nationwide protests by key civil rights leaders and parents of kidnapped girls, provoking local and international outrage against the rather slow response by the Nigerian government in securing the return of the abducted girls.

#ArewaMeToo campaigns on social media started in February 2019, challenging the culture of silence among young women and girls in northern Nigeria by giving them a platform to talk about age-long abuse and perpetuation of gender injustices, including sexual abuse veiled as religious conservatism. Modelled after the global #MeToo movement, Fakhariyya Hashim first used the hashtag #ArewaMeToo, and many others followed suit to break the silence on sexual abuse in northern Nigeria, leading to arrests and sanctions by both government and religious leaders from the North.

12

12 Idris Uwaisu, DW.COM, Street Debate: How #ArewaMeToo shed light on sexual abuse in Nigeria, published 07.10.2019: https://www.dw.com/en/street-debate-how-arewametoo-shed-light-on-sexual-abuse-in-nigeria/a-50705429

#EndSARS: The term, #EndSARS, first surfaced on social media in 2017 when Nigerian campaigners and activists coined the hashtag to register their displeasure against the incessant human rights violations by officers of the special police unit known as the Special Anti-Robbery Response Squad (SARS). The youth-powered protests moved from online expressions of rage into peaceful street demonstrations in October 2020 that shut down the nation's commercial and political hubs for several days.[13]

#OurMumuDonDo: It started as a hashtag, but metamorphosed into a civil society group led by Charles Oputa, a.k.a Charly Boy. The group campaigned for diverse social justice issues ranging from anti-corruption to good governance and electoral accountability.

Digital assemblies refer to both the spontaneous or organized gatherings of large numbers of concerned citizens or social media users on internet-enabled platforms for the purpose of calling worldwide attention to shortcomings in the society. The increasing power of the social media to trigger public censure prompted governments to unleash attempts to censor and regulate social media platforms.

Exercising the constitutionally protected rights to free speech, assembly and free association, street-based protestations have transmogrified into collective expressions of anger on online platforms. Social media platforms particularly afford a safe and anonymous haven to demand accountability from the government without fear of reprisal attacks as it is so often the case offline.[14] Besides enabling unrestricted interactions between people across the world, the intensity of use and interactions on online platforms began to cause significant shifts in the economic, political, and social relations between individuals, governments and corporate entities. The increasing power of social media to trigger public censure prompted governments to unleash attempts to censor and regulate social media platforms, as was the case with the traditional communication systems such as the radio and television.

1.3. Laws and Regulations Governing Digital Spaces in Nigeria

The technological boom spurring the expansion of digitalized goods and services prompted the formulation of a wide array of laws, policies and regulations to regulate both the industry and the activities that take place online. Laws governing the activities in the information and communications technology sectors in Nigeria include:

13 Action Group on Free Civic Space, #EndSARS: POLICE BRUTALITY, PROTESTS AND SHRINKING CIVIC SPACE IN NIGERIA, 2021, Accessed via https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/

14 Victoria Ibezim-Ohaeri, Navigating Civic Space in a Time of COVID-19: Reflections from Nigeria, SPACES FOR CHANGE, 2021, Accessed via https://closingspaces.org/navigating-civic-space-in-a-time-of-covid-19-reflections-from-nigeria/

S/No.	Law/Policies	Description
1.	***Nigerian Communications Act 2003***	This law establishes the Nigerian Communications Commission (NCC) responsible for issuing licences to telecommunication companies and imposition of terms and conditions on licences, granting or revoking of permits for connection of customer equipment, determination of principles to guide interconnection arrangements between operators
2.	***National Broadcasting Commission Act, Cap. NII, laws of the Federation, 2004***	This law, formerly a military decree of 1992, and later amended as an Act of the National Assembly in 1999, establishes the National Broadcasting Commission (NBC) to regulate and control the broadcasting industry in Nigeria.
3.	***National Identity Management Commission Act No.23 of 2007***	The National Identity Management Commission (NIMC) established by the NIMC Act No. 23 of 2007 has the mandate to establish, own, operate, maintain and manage the National Identity Database in Nigeria, register persons covered by the Act, assign a Unique National Identification Number (NIN) and issue General Multi-Purpose Cards (GMPC) to citizens of Nigeria as well as others legally residing within the country. The NIMC Act 2007 repeals the law that created the former Department of National Civic Registration (DNCR) and the transfer of its assets and liabilities to the NIMC.
4.	***National Information Technology Development Act (2007)***	This law established the NIMC National Information Technology Development Agency (NITDA) to implement the Nigerian Information Technology Policy and co -ordinate general IT development in the country. NITDA's mandate includes the creation of a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria.
5.	***Cybercrimes (Prohibition, Prevention, etc.) Act, 2015***	The Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. It also ensures the protection of critical national information infrastructure, promotes cybersecurity and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.
6.	***National Digital Economy Policy and Strategy (2020-2030)***	The Federal Ministry of Communications was renamed the Federal Ministry of Communications and Digital Economy (FMoCDE) on the 17th of October 2019, expanding the Ministry's schedule to include the development of Nigeria's digital economy. The National Digital Economy Policy and Strategy (NDEPS) developed by the FMoCDE rests on eight pillars: Developmental Regulation; Digital Literacy & Skills; Solid Infrastructure; Service Infrastructur e; Digital Services Dev elopment & Promotion; Soft Infrastructure; Digital Society & Emerging Technologies; and Indigenous Content Development & Adoption.
7.	***IMEI Policy 2021***	In May 2021, the Federal Ministry of Communications and Digital Economy released a Revised National Identi ty Policy for SIM Registration that requires Nigerians to submit their International Mobile Equipment Identity (IMEI) numbers to a Centralized Equipment Identity Register (CEIR), otherwise known as Device Management System (DMS), which the NCC would manage.
8.	***Nigeria Cloud Computing Policy***	NITDA issued Nigeria Cloud Computing Policy (NCCP) pursuant to Section 6 (a) (b) (c) and (i) of the National Information Technology Development Act 2007, which mandates the agency to issue policies, frameworks, standards and guidelines for the development of IT industry in Nigeria. The policy aims to promote the adoption of Cloud Computing

9	***National Policy for the Promotion of Indigenous Content in the Nigerian Telecommunications Sector***	In alignment with pillar #8 of the NDEPS, the ministry of communication and digital economy issued this policy to among other things, foster collaboration between global original equipment manufacturers (OEMS) engaged in the manufacturing of telecommunications equipment and indigenous players. the policy focuses on four main areas: manufacturing; services and software for the telecoms sector; business support serv ices (BSS); People; and research and development for digital innovation and entrepreneurship
10	***Revised National Digital Identity Policy***	Ministry of Communication and Digital Economy issued this policy in February 2020 and revised in May 2021 mandating the use of NIN for SIM card registration. To mitigate the vulnerability and security risk posed by unidentified network users, the policy responds to the issue of unregistered and improperly registered subscriber identity module (SIM) cards.
11	***National Policy on VSAT Installation Core Skills for Nigerians***	This policy issued by the Ministry of Communication and Digital Economy aims to improve the acquisition of the specialized skills required to drive the infrastructure related pillars of the National Digital Economy Policy and the B roadband Plan. This policy responds to the challenge of inadequate manpower for engagement in the Communication Satellite Industry in the six geo-political zones.
12	***National Broadband Policy (2020-2025)***	Ministry of Communications and Digital Economy issued this policy to support the growth of broadband connectivity in the country.

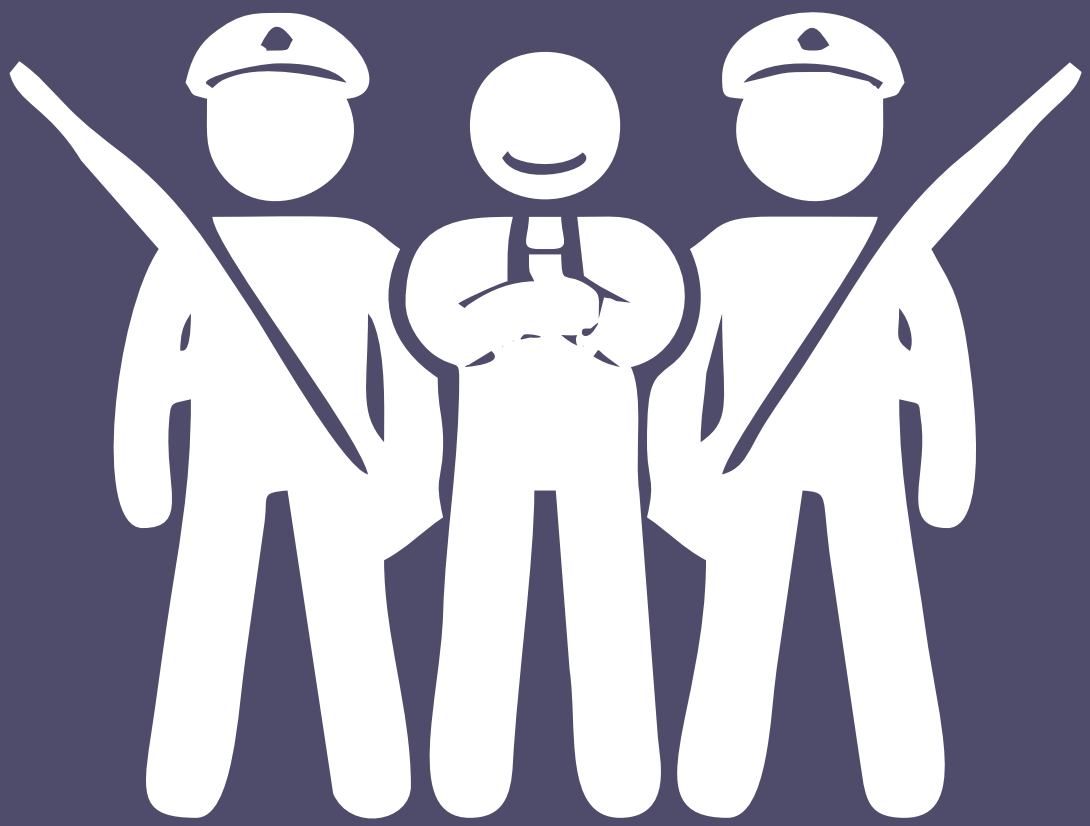
1.4. Overview of industry regulators

Sitting atop the telecommunications industry is the Federal Ministry of Communications and Digital Economy (FMoCDE). Among other things, the Nigerian Communications Act 2003 mandates the FMoCDE Minister to formulate and monitor the general policy implementation for the communications sector towards ensuring the utilisation of the sector as a platform for the economic and social development of Nigeria. The same law also established the Nigerian Communications Commission (NCC) in 2003 as an independent regulatory body for the telecommunications industry in Nigeria, with the FMoCDE as its supervising ministry.

NCC's functions include issuance of licences to telecommunication companies and imposition of terms and conditions on licences, granting or revoking of permits for connection of customer equipment, determination of principles to guide interconnection arrangements between operators, consulting with consumers, commercial and industrial organizations, and summoning persons to appear before the Commission.[15] NCC is also mandated to monitor and report on the state of the Nigerian telecommunications industry, provide statistical analyses and identify industry trends with regard to services, tariffs, operators, technology, subscribers, issues of competition and dominance, etc., with a view to identifying areas where regulatory intervention would be needed.[16] By virtue of this power, telecommunications operators are obligated, under the terms of the licenses, to provide the NCC with such data on a regular basis for analytical review and publishing.

As the table above shows, other major regulators for the telecoms and communications industry include the National Information Technology Development Agency (NITDA), the National Broadcasting Commission, the National Identity Management Commission (NIMC), the Cybercrime Advisory Council and law enforcement agencies such as the Nigerian Police, Economic and Financial Crimes Commission, Nigeria.

[15] Section 3 of the Nigerian Communications Acts (NCA) of 2003
[16] Section 89 Subsection 3(d) of the Nigerian Communications Act 2003 (NCA 2003)



CHAPTER TWO

THE RISE OF DIGITALISED DATA COLLECTION IN NIGERIA

© *Mohidden Blog*

This chapter lays out the tactical, operational, and strategic context of the country's national security and technological environments. It takes a deep look into a plethora of intrusive data collection initiatives of the government, raising new questions about the official justifications and motivations for increasing national capacities to operate biometric databases and undertake digital surveillance and intelligence gathering on a massive scale. Illuminating the role private actors such as telecommunication companies, content moderation platforms, tech corporations etc., play in facilitating data privacy breaches in the country lays the foundation for interrogating the state's collection of large volumes of personal data with little or no safeguards and how that information is used. The interrogations reveal why the massive acquisition and exploitations of these technologies persist in the first place and how they fit a repressive political agenda.

2.1. Biometrics Data Collection in Nigeria

The government's enhanced digital surveillance capacities have been made possible by the collection of big data in the form of biometric data collection, centralized databases, compulsory digital identification programs, data-warehouses, algorithm mapping and so forth. Biometrics have particularly become a key component of international and national counterterrorism efforts. In Nigeria, biometric data is collected for almost every registration process such as the national driver's license, national identity card, international passport, national voter's card, university examination registration, secondary school examinations, opening bank accounts, visa applications etc. Consistent with Nigeria's digital transformation drive enunciated in numerous policy frameworks such as the National Digital Economy Policy and Strategy (NDEPS), initiatives have been rolled out to establish a biometric digital identity for every Nigerian. Some of the notable digital identification initiatives include:

Activities requiring biometrics data collection in Nigeria

State Data Collectors	Activities involving biometrics data
National Identity Management Commission (NIMC)	NIN registration
Joint Admissions Matriculation Board (JAMB)	Conducts university entrance examinations and places suitably qualified candidates in the tertiary institutions
West Africa Examinations Council (WAEC)	Conducts the Senior Secondary Certificate Examination and the General Certificate in Education
National Examination Council (NECO)	Conducts the Senior Secondary Certificate Examination and the General Certificate in Education
Independent National Electoral Commission (INEC)	Voters' registration for all national elections
Federal Road Safety Commission (FRSC)	Issuance and renewal of road driver's licence and vehicle particulars
Nigerian Immigration Service	Issuance and renewal of international travel passport
TELCOS: Telecommunication operator	SIM card registration
Banks	Opening of bank accounts and issuance of Bank Verification Number (BVN)
Port Health/ Nigeria Centre for Disease Control (NCDC)	Administration of Covid-19 vaccine
Foreign embassies	Processing and issuance of travel visas
Integrated Payroll and Personnel information system (IPPIS) Secretariat is a department under the Office of the Accountant-General of the Federation	Processing and payment of salaries and wages directly to the bank accounts of government employees

Backed by numerous federal laws, all the above initiatives are designed to collect demographic and location data of all citizens and legal residents in Nigeria, including capturing of fingerprints, head-to-shoulder facial pictures and a digital signatures. At the completion of enrolment, the data-collecting agency issues cards with advanced security features or assigns randomly chosen non-intelligible numbers to enrollees. The tremendous amount of biometric data collected is primarily driven by the national strategy to issue a unique digital identity to

every person in the country in order to ease the process of identification and traceability, and also give them secure access to online government or private services. Because the data collection function is fragmented and dispersed across a maze of agencies, the NIMC is engaged in the harmonization and integration of data with various agencies across Nigeria to ensure smooth coordination of activities.

"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."

Section 37: 1999 Constitution

2.2. Official Justification for Intrusive Data Collection in Nigeria

The Nigerian Constitution guarantees the right to personal privacy. This guarantee prohibits unlawful intrusion in citizens' homes, correspondences, telephone and telegraphic communications. The exempted circumstances listed in Section 45 of the Constitution where derogation of privacy right is permissible include in the interest of defence, public safety, public order, public morality or public health.[17] Consistent with Section 45, officials have advanced an array of reasons for intensifying data collection initiatives. The major reasons include fraud/corruption prevention, countering terrorism and impersonation, crime detection, revenue mobilization, policy development, expanding e-government service delivery and so forth. A notable example of the digitalized fraud prevention initiative of the Nigerian government is the Integrated Personnel and Payroll Information System (IPPIS) which aims to prevent the duplication of names on the civil service payroll. IPPIS was introduced in 2019 to fight the phenomenon of "ghost workers" within the federal civil service and automate salary payments for transparency and accountability in public expenditure. IPPIS involves the registration, verification and biometric data capturing of all federal servants stored on a database which officials assure to be safe and accessible to only authorized officers.

Concerns over the rising state of insecurity and banditry prompted the December 16, 2020 directive to telecommunications companies and all Nigerian nationals to engage in a compulsory exercise linking all active SIM[18] cards to registered National Identity Numbers (NINs) or face disconnection.[19] Similarly, in 2015, the NCC directed all telecommunications firms to deactivate unregistered or partly registered SIMs.

17 S. 45 of the 1999 constitution.

18 A subscriber identification module widely known as a SIM card, is an integrated circuit that is intended to securely store the international mobile subscriber identity number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices

19 Victoria Ibezim-Ohaeri, Zikora Ibeh, SPACES FOR CHANGE, Briefer: Civic Space During the Second Wave of Corona Virus, https://closingspaces.org/briefer-civic-space-during-the-second-wave-of-corona-virus/

The regulation, according to government, is aimed at ensuring that all subscribers are traceable for security reasons. Official directives hinted that non-compliance would attract disconnection[20] from the subscribed communication networks within two weeks from the day of the announcement.[21]

Other reasons include improving the efficiency and trustworthiness of higher education systems and institutions, ease of authentication, minimizing human error through streamlined data and achieving cost reductions through the efficient use of accurate data, financial and manpower resources for planning and policy development. Above all, the data collections align with the eight-point agenda of the National Digital Economy Policy and Strategy (NDEPS) to digitally transform Nigeria by providing a robust framework and database to support technological and industrialization progress in Nigeria.

The tremendous amount of biometric data collected is primarily driven by the national strategy to issue a unique digital identity to every person in the country in order to ease the process of identification and traceability, and also give them secure access to online government services as well as private services. Despite assurance by officials that the storage of personal data is secure and only accessible to authorized officers, there is growing sentiment that stronger regulations related to privacy needs are imperative.

2.3. Data Privacy Concerns Surge Amid Intrusive Data Collection

Biometrics make it quite easy for every individual to be easily and accurately identified by their unique physical or behavioural traits. What the biometric collection spree currently enforced in Nigeria means is that every Nigerian that is at least 18 years old, would interface with a minimum of seven data collection agencies of the government to be able to exercise the basic rights to vote, bank, drive, call or travel. The large volumes of biometric information stored in government repositories have sparked widespread unease across the country, with many raising data privacy concerns. For instance, leaking and exchanging personal data in order to facilitate targeted online advertising remain popular methods of violating data privacy and exposing users to specific products and commodities without their consent.

There is evidence that large volumes of personal data, including biometric information stored on multiple centralized databases have been frequently compromised, increasing citizens' exposure to privacy intrusions, targeted advertisements, identity fraud and blackmail. Citizens report that they receive a barrage of unsolicited messages, emails and phone calls from telecommunication companies (TELCOs), telemarketers of various products and political campaigners during elections, a sign that personal information stored in numerous databases littered across the country are being accessed, exploited for economic, commercial and political purposes. Findings by The ICIR revealed that the ruling party, the All Progressives Congress, (APC), may have collaborated with the Nigerian Communication Commission (NCC) and the Independent National Electoral Commission (INEC) to access personal information of potential voters without their consent.[22] A notorious hacking incident targeted at the websites and

[20] Adeyemi Adepetun, The Guardian, Despite security concerns, FG again extends NIN-SIM link deadline by three months, 26 July 2021; Accessed via https://guardian.ng/news/despite-security-concerns-fg-again-extends-nin-sim-link-deadline-by-three-months/

[21] This Day (December 16, 2020) "FG Directs SIM Card be Linked to National Identity Number" Accessed February 20. 2021 via https://www.thisdaylive.com/index.php/2020/12/16/fg-directs-sim-card-be-linked-to-national-identity-number/

[22] Olugbenga Adanikin, ICIR, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, February 2019, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy - International Centre for Investigative Reporting (icirnigeria.org)

databases of two Nigerian universities—Ahmadu Bello University (ABU), Zaria and the University of Benin (UNIBEN), Benin City—publicly released students' and staff personal data which include admission lists and course registration details, leaving students, lecturers, and administrators vulnerable to identity theft and misuse of their personal data by cybercriminals.[23] Recently, NCC warned about the activities of an Iranian hacking group, Lyceum, orchestrating cyberespionage attacks in the African telecoms space, targeting telecommunication companies, internet service providers, and ministries of foreign affairs in Africa.[24]

Collaborations between the government and big tech corporations to support contact-tracing and other pandemic-related services add fuel to the growing skepticism about diminishing data privacy.[25] Despite assurances by officials that the storage of personal data is secure and only accessible to authorized officers, there is growing sentiment that stronger regulations related to privacy needs are imperative. For instance, a coalition of civil rights groups in Edo State approached the courts in Benin City seeking a declaration that the SIM-NIN linkage exercise constitutes a breach of citizens' right to privacy guaranteed by the 1999 constitution.[26]

2.4. How Intrusive Data Collection Enhances Surveillance

Personal data is the fuel for government's surveillance operations. Biometric collection offers the advantages of convenience, enhanced security, and ease of identity authentication, making it easier to digitally track and monitor the social, political, and economic activities of every person in the country. Human rights concerns have been raised where governments use biometric data for profiling and mass surveillance.[27] Corroborating the misuse of personal data for arbitrary surveillance, a new study finds evidence of extensive and invasive biometric data collection practices and use in Nigeria and a number of other countries.[28] Among other reasons such as the dearth of strong regulations for protecting biometric use and for restricting inappropriate surveillance, the report ranked Nigeria as the nineth-worst country in terms of collection, storage and use of biometric data.

Beyond the findings of independent studies, certain recent developments suggest that the rising fears about the abuse of personal information by state actors are well-founded. The clampdown on protesters in the wake of the October 2020 #EndSARS protests against police brutality, particularly the monitoring of their financial activities and locations, which culminated in the freezing of some protesters' bank accounts, cryptocurrency ban and the confiscation of some activists' passports, vividly illustrate how intrusive data collection makes surveillance and targeting of civic actors quite easy for governments. The protestors/holders of the frozen accounts are currently facing criminal charges on the grounds that they are suspected to be involved in "terrorism financing using their bank accounts." [29]

The government's surveillance operations are enabled by a horde of private actors comprising tech corporations, telecom operators, internet service providers, content moderation platforms and related initiatives. They assist governments to perpetrate privacy breaches using tracking apps, GPS devices, drones, facial recognition technologies, content moderation platforms, intercepting communications and outrightly

23 Emmanuel Paul, Techpoint, Hackers have access to data from Nigerian and Kenyan universities, June 1, 2020; Accessed via https://techpoint.africa/2020/06/01/nigerian-kenyan-universities-hacked/

24 Temitayo Jaiyeola, The Punch, NCC Warns Nigerians of Iranian Hackers' Possible Attacks (16 November 2021), Accessed via https://punchng.com/ncc-warns-nigerians-of-iranian-hackers-possible-attacks/

25 Nigeria Governors' Forum, Governors, MTN partner to use data to halt spread of COVID-19, https://nggovernorsforum.org/index.php/homepage/73-featured-news/1564-governors-mtn-partner-to-use-data-to-halt-spread-of-covid-19

26 Biometric Update, Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit, February 2, 2021, Accessed via https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit

27 Financial Nigeria, Nigeria risks lower score on biometric data practices, February 2021; Accessed via http://www.financialnigeria.com/nigeria-risks-lower-score-on-biometric-data-practices-feature-403.html

28 Comparitech, Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it, January 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/

29 Human Rights Watch, ibid.

With over 400 incidents of clampdowns on civic actors in Nigeria documented on the Closing Spaces Database[30] between 2015-2021, the frequency of restrictions not only points to a surge in targeted surveillance, but also raises fears that official justifications—especially combating insecurity and terrorism—may not be the only reason for these massive data collection initiatives. Civil society organisations and citizens generally are concerned that surveillance could be normalised and abused by authorities, especially in the absence of adequate legal protections.[31]

2.5. The Role of Private Telecom Companies in Enhancing Surveillance and Data Privacy Breaches

The government's surveillance operations are enabled by a horde of private actors comprising tech corporations, telecom operators, internet service providers, content moderation platforms and related initiatives. They assist governments to perpetrate privacy breaches using tracking apps, GPS devices, drones, facial recognition technologies, content moderation platforms, intercepting communications and outrightly releasing personal data.The government's surveillance operations are enabled by a horde of private actors comprising tech corporations, telecom operators, internet service providers, content moderation platforms and related initiatives. They assist governments to perpetrate privacy breaches using tracking apps, GPS devices, drones, facial recognition technologies, content moderation platforms, intercepting communications and outrightly releasing personal data. A new report exposed how tech corporations like Google collect vast amounts of personal data on a continuous basis.[32] Personal data is collected whether users interact directly with Google services and products such as Google Search and Google Maps, or during indirect interaction when the Google Chrome browser might be running in the background. In fact, Google data collection majorly occurs when users are not directly engaged with any products. Similarly, Facebook's Mr. Zuckerberg has also had to face the United States' congress to explain the company's handling and harvesting of user information for pecuniary gains.

Regulatory obligations and profit-making stand out as the predominant motives for private sector participation in data breaches and surveillance initiatives. On the regulatory side, certain regulations and legislations impose obligations on private actors, especially tech corporations to render assistance to the government's surveillance agendas based on national security, disaster management, crime prevention and detection, public safety or other considerations. On the profit side, the online ad industry procures loads of personal data to achieve aggressive

30 www.closingspaces.org
31 Ridwan Oloyede, Surveillance Law in Africa: a review of six countries: Nigeria Country Report, published by the Institute for Development Studies, Accessed via https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Nigeria%20Country%20Report.pdf?sequence=7&isAllowed=y

marketing objectives and the targeting of ads to specific groups of users.[33] The various methods through which private actors facilitate the government's use of technology to silence dissent are detailed below:

Regulatory action: Using the power and force of regulation, regulators have been found to coerce private companies to interrupt access and intercept private communications of targeted civic space actors. The Twitter ban in Nigeria represents the most glaring example of how state authorities use the force of regulation to interrupt access to targeted communication sites perceived to be sympathetic to anti-government rhetoric. In June 2021, Nigeria's President Muhammadu Buhari's post on Twitter threatened to deal with the Igbo people inhabiting the country's southeast, reminding them about the destruction and loss of lives that occurred during the Biafran Civil War. The now-deleted tweet evoked sad emotions, especially the degrading remark about the millions of people, most from the Igbo ethnic group that died during that war between 1967-1970. To actualize the Twitter ban days after the tweet was deleted on the social media app, the Nigerian Communications Commission (NCC) directed all mobile network operators and internet service providers to block access to Twitter. Blocking works by blacklisting a specific site or server or URL, such that traffic going to or coming from a certain server is barred.

Using the power and force of regulation, regulators have been found to coerce private companies to interrupt access and intercept private communications of targeted civic space actors. To avoid NIMC's regulatory sanctions, telecom operators are to disconnect the lines of their mobile phone subscribers who fail to link their SIM cards with their National Identification Numbers (NINs). This incident came a year after the Nigerian Communications Commission (NCC) carried out SIM registration audit, with the help of telecom operators, which led to the disconnection of about 9.2

Early this year, mobile telecommunications companies—MTN, Glo, and 9mobile—ostensibly acquiescing to the instruction of regulatory bodies, also blocked access to People's Gazette,[34] following certain publications on the platform exposing corrupt practices in Ebonyi State.[35] In a related development, the National Identity Management Commission (NIMC) threatened to withdraw the operating licenses of telecommunication companies that fail to disconnect lines that are not synchronised with NINs. In other words, the only way telecom operators can avoid NIMC's regulatory sanctions is by disconnecting the lines of their mobile phone subscribers who fail to link their SIM cards with their National Identification Numbers (NINs).[36] This incident came a year after the Nigerian Communications Commission (NCC) carried out SIM registration audit, with the help of telecom operators, which led to the disconnection of about 9.2 million unregistered SIMs nationwide.

The way telecom operators succumb to the dictates of regulatory bodies is identical to the way regulatory bodies dance to the whims and caprices of powerful state executives and official institutions. An example is the blockade of domain names of Naij.com— apparently considered as pro-Biafra news outlet—at the behest of the Office of the National Security Adviser.[37] All of these evince how private telecommunication companies acquiesce to repressive regulatory

33 Emma Woolacott, Forbes, Ad Industry Accused Of 'Massive' Privacy Breach, Accessed via https://www.forbes.com/sites/emmawoollacott/2019/01/28/ad-industry-accused-of-massive-privacy-breach/?sh=73c6bc076822

34 Editor. (2021, January 26). Clampdown on Peoples Gazette as telcos block access to news website. The Guardian. https://guardian.ng/news/clampdown-on-peoples-gazette-as-telcos-block-access-to-news-website/

35 Nimi, P. (2021, January 30). AUDIO: Governor Umahi threatens to kill Peoples Gazette reporters over Ebonyi corruption story. Peoples Gazette. https://gazettengr.com/audio-governor-umahi-threatens-to-kill-peoples-gazette-reporters-over-ebonyi-corruption-story/?utm_source=ReviveOldPost&utm_medium=social&utm_campaign=ReviveOldPost

36 Emmanuel Elebeke, Vanguard, Disconnect all SIMS not connected to NIN by Dec 30, FG orders telcos (December 15, 2020) Accessed via https://www.vanguardngr.com/2020/12/fg-orders-telcos-to-disconnect-all-sims-not-connected-to-nin-by-dec-30/

37 Alabi, S. (2017, November 17). President Buhari's Secret War on Free Speech. Paradigm Initiative. Here, A leaked memo signed by Nigerian Communications Commission's Director of New Media and Information Security, Haru Al-Hassan, and Head of Legal and Regulatory Services also recommended the blocking of twenty-one (21) websites sympathetic to the Biafran secessionist agitations. See https://paradigmhq.org/president-buharis-secret-war-on-free-speech/.

orders as part of their corporate survival strategy. Human rights mechanisms have expressed concerns about mandatory SIM card registration as interfering with individuals' freedom of expression online by rendering individuals susceptible to arbitrary surveillance. In particular, the UN Special Rapporteur on Freedom of Expression (FoE) has specifically recommended that, "States should refrain from … requiring SIM card registration for mobile users.[38] Disconnecting individuals is equally an excessive sanction that will lead to censorship of communication." [39]

Network shutdowns: Security-driven network shutdowns are also commonplace. Based on a request by the Nigerian military in advance of planned operations against organised armed groups in the North West region of Nigeria, the Nigerian Communications Commission (NCC) on September 3, 2021, ordered all telecommunications companies to shut down their services in the North West, especially, Katsina, Sokoto and Zamfara states.[40] A similar network blackout was also enforced in at least 13 local government areas of Katsina State to check "banditry" and terrorism. Kaduna State is adopting the same strategy when it announced plans to disrupt communication lines in order to launch an offensive against militants hiding in some local government areas in the state.[41] State actors claim that such blackouts make it difficult for bandits to use landlines to plan attacks and demand ransom.

While crime-fighting is the lawful reason advanced for network shutdowns, clauses inserted in the provisions of draft statutes give off official intention to apply the same measures to restrict access to the social media. Section 12 of the proposed Protection from Internet Falsehoods, Manipulations and Other Related Matters Bill, 2019[42] granted law enforcement departments (the Nigerian Police Force) the power to issue an access blocking order by directing the Nigerian Communications Commission (NCC) to order the internet service provider to disable access to users in any online location that false communication emanates from. When this directive is issued, the NCC must give the internet access service provider an access blocking order.

Releasing subscribers' information and records: In 2013, NCC published a Regulatory Guideline for Provision of Internet Service[43] which mandates cooperation between service providers and law enforcement officers. Not only that, the NCC Act empowers the National communication Commission to "establish and maintain a central database of all registered subscribers' information." The licensed Telecommunication Companies are expected to "transmit all subscriber information captured and registered within the preceding month … to the Central Database." In this connection, service providers are obligated to release and transmit all subscriber information and phone records in their custody to relevant authorities. Centralized databases pose particularly acute risks, as they increase the potential for data breaches and open the door for generalized surveillance.[44]

In July 2020, Babatunde Olusola, a Chemical Engineering student of Ladoke Akintola University (LAUTECH), Ogbomoso, Oyo State, was detained for over 54 days for creating a parody Twitter account of former Nigerian President, Goodluck Jonathan. The Special Anti-Robbery Squad (SARS) traced and arrested him using information on his call log obtained from telecommunication service providers. ~ Sahara Reporters

38 See United Nations Human Rights Council, A/HRC/29/32, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" May 22, 2015, para. 60.
39 Victoria Ibezim-Ohaeri, Zikora Ibeh, SPACES FOR CHANGE, Briefer: Civic Space During the Second Wave of Corona Virus, https://closingspaces.org/briefer-civic-space-during-the-second-wave-of-corona-virus/
40 Abubakar Ahmadu Maishanu, Premium Times, Why we shut down telecommunications networks in Zamfara – Governor, September 6, 2021, Accessed via https://www.premiumtimesng.com/regional/nwest/483366-why-we-shut-down-telecommunications-networks-in-zamfara-governor.html
41 Premium Times, Kaduna to shut down telcos over insecurity, 29th September 2021, Accessed via https://guardian.ng/news/kaduna-to-shut-down-telcos-over-insecurity/
42 Sponsored by Senator Mohammed Sani Musa (APC Niger East), 2019
43 National Communication Commission. Guidelines for the provision of internet service. https://www.ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file
44 Privacy International, Biometrics Collection Under the Pretext of Counter-Terrorism, 2021, Accessed via https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism

Retention and interception of communication details: Furthermore, the Cybercrime Act ensures the retention and interception of communication details of anyone upon request. It also mandates operators of commercial cybercafes' (or internet cafes) to keep up-to-date information on all users which are available to government officials on demand. Under this law, service providers are required to retain traffic and content data for two years[45] while law enforcement agents can request the data from service providers, of which they are mandated to comply. Cybercafés in Nigeria are usually small sole-proprietorship businesses run informally on street corners. They engage staff who are unskilled, with little or no IT knowledge.[46] Apart from placing an onerous burden on commercial business centers to monitor and keep register of their customers, the enforcement involves private citizens using these centers to surrender their personal information to numerous informal businesses that lack adequate data storage capabilities and respect for personal privacy. Compounding the situation, many cybercafés have been sealed off by security agencies based on the allegation of cybercrimes perpetrated using their café networks while cybercafe operators are now required to register with the Economic and Financial Crimes Commission (EFCC).[47]

Release of subscriber records and information: A very sensitive provision to note is the legal requirement for licensees like telecommunication companies, network facilities providers and internet service providers to surrender "subscriber information on the Central Database" to security agencies upon a written request received by the Commission from an official … not below the rank of an Assistant Commissioner of Police or a coordinate rank in any other Security agency."[48] This provision creates a gap that can be exploited to gather intelligence indiscriminately and target civic actors. It also paves way to monitor citizens' use of social media and communication apps, movements, financial transactions. The information can be surrendered to the authorities at any time as required by law. Records obtained from telecommunication companies were used to track and arrest journalists in 2020.[49]

Lawful interception of communications: Furthermore, the Lawful Interception of Communications Regulations 2019 recognizes and authorises lawful interception of communications and access to individuals' data without a warrant.[50] Besides vesting the National Security Adviser (NSA) and the State Security Services (SSS) with the power to request the disclosure of protected encrypted communications,[51] licensees, comprising telecommunication companies, network facilities providers and internet service providers, are prohibited from providing or installing any communications services which do not have the capacity to be monitored and intercepted.[52]

NCC Guideline for Provision of Internet Service empowers the National Communications Commission to "establish and maintain a central database of all registered subscribers' information. Service providers are obligated to release and transmit all subscriber information and phone records in their custody to relevant authorities. Centralized databases pose particularly acute risks, as they increase the potential for data breaches and open the door for generalized surveillance.

45 Section 38(1) of the Act
46 Oluwafemi Osho and Solomon A. Adepoju, Cybercafés in Nigeria: Curse to the Internet?(2016)Accessed via http://ceur-ws.org/Vol-1830/Paper84.pdf
47 Proshare, EFCC to register cybercafes, others; Accessed via https://www.proshareng.com/news/Investors-NewsBeat/EFCC-to-register-cybercafes,-others/1424
48 Section 146 of the NCC Act
49 Rozen, J. (2020, February 13). How Nigeria's police used telecom surveillance to lure and arrest journalists. https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/
50 Section 4-9 of the NCC Act
51 Federal Government of Nigeria. (2019c). Lawful interception of communications regulations.
52 106(12), 105-118. Available at https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/839-lawful-interception-of-comunications-regulations-1/file
Section 11 of the Lawful Interception of Communications Regulations 2019

Disclosure of registered identity information: Section 26 of the National Identity Management Commission Act 2007 prohibits access to individuals' information contained in the national identity database except with the authorization of the Commission in certain circumstances, such as national security, prevention or detection of crime and related matters. Despite the legal prohibitions, the Commission is still authorised to disclose information of registered members to a third party without consent in the exempted circumstances. Situations that fall within the realm of national security are undefined, which can be exploited to demand and receive information on registered individuals.

Disclosure of registered identity information for commercial, political and health purposes: The coronavirus pandemic (COVID-19) of 2020 provided the government an added opportunity to introduce new legal rules and unleash a new wave of restrictions on democratic freedoms, especially the freedom of assembly and association. The Control of Infectious Diseases Bill 2020 introduced by the federal parliament at the peak of the COVID-19 lockdown granted powers to the Director-General (DG)of the Nigerian Centre for Disease and Control (NCDC) to conduct public health surveillance programmes and epidemiological investigations of people, animals, or vectors to determine the existence or likelihood of an outbreak of an infectious disease. Had that law been passed, healthcare professionals would be obligated to reveal or obtain information about patients notwithstanding any existent rule of contract to officials investigating into any outbreak or preventing a possible outbreak of an infectious disease. Apart from health surveillance, identity information has also been exploited for political gains. A recent study exposed how tacit collaborations among the ruling party, the All-Progressive Congress (APC), the Nigerian Communication Commission (NCC) and the Independent National Electoral Commission (INEC) enable the party to access personal information of potential voters without their consent[53]

Pulling down posts and disinformation: Other than spyware companies, contents moderation platforms also play major roles in facilitating digital repression in Nigeria. During the #EndSars protests, Facebook and Instagram pulled down posts on the protests as fake news, thus hampering the publicity of the protests and injuring its credibility in the process.[54] In the past, Facebook has also come under fire for allowing the platform to be weaponized for targeted disinformation campaigns that exposed opposition politicians and civic actors to some harm, especially during election seasons. For instance, substantiated media reports provide evidence of the use of Facebook to coordinate a trolling campaign against opposition politician, Atiku Abubakar, a former vice-president and President Muhammadu Buhari's main opponent. Their disinformation campaign included a banner image of Mr Abubakar as Darth Vader, the notorious "Star Wars villain".[55] Those behind the attack created a chain of fictitious Facebook pages that reached some 2.8 million users and engaged over 5,000 followers on Facebook, fuelling concerns whether Facebook is undermining democracy in Africa.[56] Tech giants like Facebook and Google have also voiced out their opposition to the inclusion of "intrusion software," and "IP network surveillance systems" in the Wassenaar rules amendment in 2013, complaining that the language is too broad and will affect the internet's ability to defend itself.[57] [58] [59]

53 Olugbenga Adanikin, ICIR, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, February 2019, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy - International Centre for Investigative Reporting (icirnigeria.org)

54 QuartzAfrica, Facebook and Instagram made missteps on Nigeria's EndSARS protest while Twitter boosted it, https://qz.com/africa/1922372/facebook-hurt-nigerias-endsars-protest-while-twitter-boosted-it/

55 Samuel Ogundipe, Premium Times, Election: Facebook shuts down Israeli firm for pushing Buhari propaganda

56 Larry Madowo, BBC, Is Facebook undermining democracy in Africa? (2019) https://www.bbc.com/news/world-africa-48349671

57 ZDNet: Wassenaar Arrangement: When small words have the power to shatter security (2017)

58 https://www.zdnet.com/article/wassenaar-arrangement-when-wording-may-break-the-us-security-industry/ Facebook US Public Policy: https://www.facebook.com/uspublicpolicy/posts/1047027321981746

59 https://www.theverge.com/2015/7/20/9005351/google-wassenaar-arrangement-proposal-comments

2.6. An Unfolding Repressive Agenda

With the level and intensity of demographic, location and biometric data collection currently going on Nigeria, the following trends validate suspicions of a foreseeable rise in data privacy breaches and the surveillance of citizens as well as the civil society:

Pro-government online trolls: The enlistment and deployment of more vicious online trolls to attack individuals and civic organisations that call the government to account. Blackmail and threats against civic actors operating online and offline is rife. These trolls, bankrolled by political cronies and loyalists, promote pro-government rhetoric and propaganda to drown voices of dissent. By way of illustration, the handle @ishakaa has for too long, trolled leading human rights organizations in Nigeria such as the Policy and Legal Advocacy Center (PLAC), Civil Society Situation Room and other groups calling out the failings of government. @ishakaa's campaigns on Twitter accuse civic actors of terrorism financing, corruption, treason and so forth. Recent research by Carnegie Endowment for International Peace identified about 360 of pro-government NGOs in Nigeria whose core role is to curry the favour of the government by chanting the accolades of those in power including the military.[60] The intention is to undermine the critical works of genuine civil society organizations, while covering up the gaps in governance and shortfalls of government regarding the responsibilities they are mandated to deliver to Nigerians.

The local media is replete with numerous instances of political trolls gaslighting and spreading fake news within Nigeria's social media space, including aides to President Muhammadu Buhari.The Buhari Media Centre (BMC) has at various times been accused of trolling critics of President Muhammadu Buhari[61] on social media and they usually go to the extremes to malign their targets.[62][63] Columnist Prof. Farooq Kperogi alleged that the BMC started with only about 40 people who have multiple fake social media accounts. But it's now an entire propaganda and mind-management industry that employs thousands of people.[64]

Proliferation of restrictive legislative proposals seeking to enlarge governmental power to surveil and control the civic space. Examples include the Social Media Bill, Hate Speech Bills, NITDA Amendment Act Bill etc., and National Commission for the Prohibition of Hate Speeches Bill 2019[65]—popularly known as the Hate Speech and Social Media Bills. The Social Media Bill sponsored by Senator Mohammed Sani seeks to prohibit the digital transmission of false statements and empowered law enforcement departments (the Nigerian Police Force) to order the internet service

60 Mathew T.Page, Fake Civil Society: The Rise of Pro-Government NGOs in Nigeria, Carnegie Endowment for International Peace, (2021) Accessed via
61 https://carnegieendowment.org/2021/07/28/fake-civil-society-rise-of-pro-government-ngos-in-nigeria-pub-85041
62 Queen Esther Iroanusi, ANALYSIS: How Nigerian politicians, supporters use fake news as campaign strategy
https://www.premiumtimesng.com/news/headlines/311532-analysis-how-nigerian-politicians-supporters-use-fake-news-as-campaign-strategy.html
63 https://www.premiumtimesng.com/opinion/466420-digital-authoritarianism-and-the-echoes-of-decree-4-by-bamidele-ademola-olateju.html
64 Farooq Kperoogi, BMC Trolls Think They Can Get Me Fired From My Job, https://www.farooqkperogi.com/2020/01/bmc-trolls-think-they-can-get-me-fired.html
https://tribuneonlineng.com/the-buhari-propagandocracy-and-the-rhetoric-of-fake-news/
65 SPACES FOR CHANGE: Factsheet: Everything You Need To Know About The Hate Speech Bill,
https://closingspaces.org/factsheet-everything-you-need-to-know-about-the-hate-speech-bill/

provider to disable access to users in the online location that false communication emanated from. Likewise, the Hate Speech sponsored by Senator Aliyu Sabi Abdullahi criminalized various forms of expression that could stir up ethnic hatred and equally make it possible to sentence to death by hanging anybody convicted of spreading hate speech.

Inconsistencies between restrictive surveillance laws and human rights provisions: The Nigerian Constitution and Freedom of Information Act 2011 provide for the protection of civic freedoms (rights to free expression, assembly, association and personal privacy) and legalises free access of public information to citizens. Section 37 of the 1999 Nigerian Constitution specifically protects the privacy of the telephone conversation and telegraphic communication of citizens without interference. As we shall see in subsequent chapters, numerous federal legislations vest enormous power on state security agencies to conduct surveillance operations for various reasons, in stark contrast with the constitutional guarantees of personal privacy. These surveillance regimes are inconsistent with privacy guarantees while numerous legal provisions have been invoked to justify clampdowns by state actors such as the Official Secrets Act, Cybercrime Act, Terrorism Act, Criminal Code and Penal Code –especially those relating to treason, sedition etc.[66]

Framing Facebook commentary as terrorism: Hardly any week passes in Nigeria without a Facebook user being arrested on account of Facebook commentary critical of the government and charged for terrorism. Ali Yakubu,[67] Amudat Babatunde,[68] Joseph Odok,[69] Ambrose Nwaogwugwu[70] and Emperor Ogbonna[71] were charged with terrorism on account of Facebook posts that were critical of state executives. The swiftness with which bloggers, activists and commentators are arrested, prosecuted and jailed on account of critical commentary posted on social media strongly corroborates that a well-coordinated surveillance operation is effectively going on, monitoring the activities of citizens online. Particularly undergirding this inference is the huge disconnect between merely critical commentary on social media and the terrorism c-harges frequently slammed on their authors.

Network shutdowns are rampant in the northern region of the country. Communication blackouts have in the past been enforced in Zamfara, Katsina, Kaduna, Borno purportedly to check "banditry" and terrorism. In addition to the adverse impacts on social and economic activities in those areas, communication and internet shutdowns prevent civic actors from organizing public assemblies and inhibit online gatherings and protests.

> The Director-General (DG) of the Nigeria Centre for Disease Control (NCDC) may, during investigating into any outbreak or preventing a possible outbreak of an infectious disease, require healthcare professionals to reveal or obtain information about patients notwithstanding any existent rule of contract. ~ Control Of Infectious Diseases Bill 2020

Declining privacy rights and repression of civil liberties: CIVICUS downgraded Nigeria from "obstructed" to "repressed" in its People Power Under Attack 2019 report.[72] Between 2015 – 2021, the Closing Spaces Database' analytics documented over 300

66 Henry Ojelu, Vangaurd, Lawyers divided over superiority of FOI to Official Secret Act, September 6, 2018, https://www.vanguardngr.com/2018/09/lawyers-divided-over-superiority-of-foi-to-official-secret-act/
67 Closing Spaces Database, Businessman Jailed For Allegedly Calling Adamawa Governor 'Father Of All Thieves', Accessed via https://closingspaces.org/incident/businessman-jailed-for-allegedly-calling-adamawa-governor-father-of-all-thieves/
68 Closing Spaces Database, DSS Files Terrorism Charges against Blogger who Streamed Igboho's House Raid on Facebook; https://closingspaces.org/incident/dss-files-terrorism-charges-against-blogger-who-streamed-igbohos-house-raid-on-facebook/
69 Closing Spaces Database, Nigerian Lawyer Slammed with Terrorism Charges for Criticising State Governor, Please see: https://closingspaces.org/incident/nigerian-lawyer-slammed-with-terrorism-charges-for-criticising-state-governor/
70 Closing Spaces Database, At Last, PDP New Media DG, Nwaogwugwu Granted Bail In High Court, ,
71 https://closingspaces.org/incident/at-last-pdp-new-media-dg-nwaogwugwu-granted-bail-in-high-court/
72 TV360: 70 Days in Custody; The Case of Emperor Ogbonna, https://www.youtube.com/watch?v=-7AIhPYzCOY&feature=youtu.be
CIVICUS, People Power Under Attack, December 2019. Please see https://civicus.contentfiles.net/media/assets/file/GlobalReport2019.pdf

incidents of clampdowns on freedom of expression have been documented during this period. Similarly, freedom of expression—comprising press freedom (120 incidents) and the freedom of speech (83 incidents)—bears the highest share of repressive activities in the Nigerian civic environment.[73]

The categories of persons at the receiving end of the attacks on free expression, assembly and association rights have exponentially expanded in this age of social media where ordinary citizens publish their thoughts and influence others on matters concerning the polity. Journalists, charities, activists and potentially all users of social media are at risk. Various research conducted by Nigeria's leading research organization on civic space—Spaces for Change—noted as follows:[74]

> *The denial of civil and political liberties, surveillance and arrests of bloggers or political opponents, violations of personal or physical integrity rights, restriction of freedoms of expression on mainstream and internet media, are all unhealthy signals that indicate a repressed or closed civil society. When these signals are recurrent, they obstruct public participation in democratic engagement, bringing about an environment of state repression. Obstructions of this nature are reminiscent of the repressive tactics traditionally utilized by military regimes. As evidence would subsequently show, civilian administrations are increasingly, resorting to these tactics to coerce associational and non-associational entities into submission.*[75]

Influx of mass surveillance and augmented data-collection technologies: The influx of sophisticated surveillance and intelligence paraphernalia at the behest of federal and state governments is a growing source of concern. Numerous surveillance companies such as Isreali-owned Circles, Cellebrite and FTK and the U.S.-based Access Data Group are operating in Nigeria. The entrance of these companies into Nigeria's unregulated internet surveillance market widens the range of Nigerians susceptible to surveillance and privacy abuses.[76] Comparitech's study of biometric data collection in 96 countries assigned points to countries based on the severity of biometric use, collection and access. Nigeria was given a score of 11 points out of a maximum of 31 for not just insufficiency of strong regulations for protecting biometric use but also for more intrusion and extensive use of surveillance.[77] Also, the presence of big data corporations and their collaboration with government actors, enabled by numerous legal provisions, continues to bolster the government's tracking, internet censorship and monitoring capabilities.

Numerous surveillance companies such as Isreali-owned Circles, Cellebrite and FTK and the U.S.-based Access Data Group are operating in Nigeria. The entrance of these companies into Nigeria's unregulated internet surveillance market widens the range of Nigerians susceptible to surveillance and privacy abuses.

Weak data privacy enforcement systems: Despite enacting the Nigerian Data Protection Regulation (NDPR) 2015, compliance lags. Official data collectors in Nigeria have failed to publish their privacy policies, as required by section 2.5 of the NDPR. In December 2019, the NITDA issued notice of non-compliance with the provisions

73 Closing Spaces Database (www.closingspaces.org), Tracking Civic Space Incidents in Nigeria: 2015-July, 2021 https://closingspaces.org/tracking-civic-space-incidents-in-nigeria-2015-july-2021/

74 Spaces for Change "Closing Spaces for Democratic Engagement and Civil Society in Nigeria". Available at https://spacesforchange.org/wp-content/uploads/2017/06/Beyond-FATF.-Trends-Risks-and-Restrictive-Regulation-of-Non-Profit-Organisations-in-Nigeria.pdf, accessed 26 September 2021

75 Ibid., p. 13

76 Ogala, E. (2016, June 9). Ibid.

77 Comparitech, ibid.

of the NDPR to about 100 companies, some of which were in the sensitive fintech sector.[78] Incidents of violations have not attracted serious consequences for the unlawful intrusion and exploitation of personal data as espoused under section 2.10 of the NDPR.

Influence of international regulations, powerful countries and repressive regimes: Between 2001 and 2018, at least 140 governments, including Nigeria, adopted counter-terrorism legislations and such new and multiple legislative and administrative measures are defended by reference to new or perceived threats, or simply to comply with new international requirements.[79] Furthermore, a comparative study of state practices evinces that the stances of powerful economies and their interpretation of the international counterterrorism (CT) framework influence the practices obtained in less powerful countries. Nigeria has for the most part, either retained very repressive post-colonial legislations or modelled new laws after those in the United Kingdom. Nigerian courts continue to apply English law decisions after half a century of their independence from England. In interpreting Nigerian laws, the Nigerian judiciary are also known to make references to decisions of courts in England. As such, the English interpretation of their CT obligations under international law would invariably influence the position in Nigeria. Even beyond direct colonial ties, global interconnections enable Nigeria to copy and paste laws and practices from other countries, especially countries which they consider as internationally important. A notorious example of copy-and-paste practices includes Nigeria's Infectious Diseases Bill which was copied[80] from Singapore.

CONCLUSION

As we have seen, a world of difference exists between the reasons advanced for the massive digital collections of personal data and what the state really does with the data. There is also a clear difference between the original intent of legal provisions and how the government enforces them. Combating insecurity and terrorism has clearly been weaponized as a tool of repression of civil societies contrary to the original purpose and stated objectives. What access to advanced technologies and tech-powered big data has done is to make it easy for state actors to take advantage of the popular refrains like the "War on Terror" to support, allow and justify privacy invasions and the abuse of civil liberties. And once coated with the balm of "national security", it confers an automatic, and often unchecked license on state actors to do whatever that is necessary to ensure public safety against harm with much less scrutiny.

State actors do not act alone. Wielding the regulatory sledgehammer in an era of big data, state authorities extract and enjoy the cooperation of diverse corporate actors to execute their restrictive and authoritarian agendas. Regulatory sanctions have been invoked to punish uncooperative actors. Where regulation is not in the mix, concerns regarding personal data leakages and privacy breaches by tech and financial corporation—propelled by profit maximization—continue to be on the top burner.

Another lesson to draw from the misuse of the national security rhetoric is the nexus between the form of government operated in a country and its propensity to abuse. Countries with

78 Tope Adebayo, Techpoint, Navigating data privacy issues in targeted online advertising, https://techpoint.africa/2020/07/22/data-privacy-online-advertising/

79 Fionnuala Ní Aoláin "Promotion and protection of human rights and fundamental freedoms

80 while countering terrorism". Available at https://undocs.org/A/74/335, accessed 26 September 2021, p. 3 Nigeria copies and pastes new laws from Singapore | World | The Times

strong institutions are better able to apply CT norms without irremediable impact on civil liberties. Strong and independent institutions act in the best interest of the citizens, checkmate executive and regulatory overreach and lower chances of hijack by government actors for a repressive agenda. Nothing has made the climate of unregulated surveillance and privacy intrusions to fester in Nigeria more than the absence of strong checks and balances to checkmate potential abuse and actual excesses of the government. In fact, a strong and representative legislature and an independent judiciary are necessary antidotes to the abuse of CT legislation and enforcement. The growing level of suppression of the civil society made possible by the weaknesses within the country's judicial, parliamentary and political systems is not only fueling the massive drift towards authoritarianism, but is also integrally linked to the expansion of digital repression in Nigeria.

CHAPTER THREE

LEGAL IMPETUS FOR DIGITAL REPRESSION IN NIGERIA

© Techpoint Africa

What are the methods, laws, tactics, measures used to justify the arbitrary and flexible use of the terms, 'terrorism', 'extremism', 'national security' to surveil, suppress democratic freedoms and crush dissent? Which entities or processes within and beyond government chiefly invoke these advanced technologies and apply overbroad methods? In this chapter, we explore an array of legal and policy provisions that give express legal backing to the government's intrusive data-collection and surveillance activities. Most of these provisions are embodied in criminal and security laws, and other regimes designed to address transnational challenges-including terrorism, drug flows, organized crime and proliferation of weapons of mass destruction. From there, we examine how these laws are applied in practice and the kinds of harm victims targeted by the misuse of abuse of the security paradigms face.

3.1. Laws Enabling State's Data-collection and Surveillance Operations

A host of national security agencies are statutorily-mandated to prevent, detect, and protect Nigeria from internal and external threats—whether of a military or a non-military nature—against its territorial or political sovereignty. Amid the surge in organized crimes, particularly the mutation of the Boko Haram-led insurgency into full-blown terrorist activities,

the Terrorism Prevention Act (TPA), first passed in 2011, and modelled after international standards, guides the implementation of the diverse counterterrorism initiatives in Nigeria. In addition to specifying punitive measures for various offences that fall within the purview of terrorism, the TPA aggregates provisions of preexisting security laws relating to the suppression of terrorist activities. The Office of the National Security Adviser (ONSA)[81]—solely appointed and answerable to the Presidency—oversees Nigeria's counterterrorism initiatives embodied in the National Counterterrorism Strategy (NACTEST) and coordinates the activities of all security and law enforcement formations. The ONSA's coordination role includes hosting the Counter-Terrorism Centre (CTC), Joint Terrorism Analysis Branch (JTAB) and the Behavioural Analysis and Strategic Communication Unit enabling it to facilitate intelligence sharing and cooperation amongst agencies.

As the implementers of counterterrorism initiatives within Nigeria, the ONSA and the agencies within that office, particularly the State Security Service (SSS)—now known as the Department of State Services (DSS)[82]—are powerful vehicles for enforcing the country's security, including surveillance objectives. The overt and covert operations of state security agencies to investigate and prevent crime, enforce rules, preserve the peace and counter terrorist activities are backed by numerous laws. Consistent with these mandates, their security operations are equally influenced by the proliferation of technological applications, for improving the effectiveness of their intelligence, data-handling and military capacities. Some of the laws backing their operations are detailed below:

Examples of Laws Enabling State's Data-gathering and Physical Surveillance Operations

No	Name	Description
1	Official Secrets Act 1962: Sections 1 – 3, 4	Official Secrets Act provides for the protection of sensitive official information. Sectio n 4 empowers the state to make regulations for controlling mail forwarding agencies, especially the manner in which any person conducts any organisation for receiving letters, telegrams, packages or other matter for delivery or forwarding to any other person. Violators are deemed to have acted for a purpose prejudicial to the security of Nigeria.
2	Nigerian Communication Act 2003: Sections 4-9, Sections 146 -149	Empowers NCC to "establish and maintain a central database of all registered subscribers' information." The licensed Telecommunication Companies are expected to "transmit all subscriber information captured and registered within the preceding month … to the Central Database." The National Provisions in S.146 -149 obligate telecom operators to cooper ate with state authorities to frustrate the commission of crimes, to protect public revenue and preservation of national security, including allowing authorised interception of communications.

81 Known as Coordinator on National Security under the National Security Services Act

82 See Premium Times "FACT-CHECK: How Nigeria's secret police, SSS, is violating the law and illegally parading itself as DSS." Available at https://www.premiumtimesng.com/investigationspecial-reports/209343-fact-check-nigerias-secret-police-sss-violating-law-illegally-parading-dss.html, accessed 26 September 2021

3	Constitutional provisions: S.37 - Rights to privacy and family life; S.38 - Freedom of thought, conscience, and religion; S.39: Freedom of expression & press; S.40: Peaceful assembly and association; S.41: Freedom of movement	Section 45 of the 1999 constitution permits state authorities to derogate from the aforementioned rights only in the interests of defense, public safety, public order, public morality or public health, or to protect the rights or freedoms of others.
4	Cybercrime (Prohibition and Prevention) Act 2015: Section 38(1-6)	Empowers the government to designate certain computer systems, networks, (whether physical or virtual) and or computer programs critical national information infrastructure. Service providers are required to keep all traffic data, subscriber information, non-content information and content data for a period of 2 years. Information preserved, held or retained can be released at the request of any law enforcement agency.
5	Terrorism Prevention Act: Section 29	Vests relevant law enforcement agencies with the power to conduct intelligence gathering and intercept communications to prevent terrorist acts and detect offences related to them, subject to the approval of the Attorney General of the Federation, Inspector General of Police, and the Coordinator of National Security.
6	Freedom of Information Law 2011	Provides for free access of public information to citizens. It also provides for the protection of personal privacy, including that of serving public officers from adverse consequences of disclosing certain kinds of official information without authorisation and establishes procedures for the achievement of those objectives.
7	Criminal Laws: Criminal Code Act, 1995 ○ Sedition: Section 50-53 ○ Defamation of Character: Sections 373-376	Seditious intentions refer to acts that aim to cause hatred or contempt or excite disaffection against the person of the President or of the Governor of a State or the Government of the Federation; or to raise discontent or disaffection amongst the citizens or other inhabitants of Nigeria; or promote feelings of ill-will and hostility between different classes of the population
8	Regulation 8 (1) of the Nigerian Communications (Enforcement Process, etc.) Regulations, 2019	It obligates telecom operators to keep records of call data under the Cybercrimes Act and the consumer code of practice regulations, and to make available "basic" and "non-basic" information that "may be required upon request by law enforcement agency.

9	Part V of the Mutual Assistance in Criminal Matters Act 2019	Empowers the authorities to carry out the interception of telecommunications and postal items and surveillance, including covert electronic surveillance. Nigeria can also exchange surveillance information with other countries where it relates to the identification and loca tion of criminal offenders, obtaining evidence, securing the production of official or judicial records, interception of postal orders, interception of telecommunications and so forth.
10	National Identity Management Commission Act 2007: Section 26	Disclosure of registered information contained in the database is prohibited except with the authorization of the Commission in the interest of national security or for the purpose connected with the prevention or detection of crime.
11	Corporate and All ied Matter Act (CAMA) 2020: S.119 & 120	Persons who hold significant control in any type of company are required to disclose particulars of such control within 7 days of acquiring such significant control. All affected companies must inform the Corporate Affairs Commission within one month of receipt of the information, disclose the information in their annual returns to the Commission and update their registers of members with the appropriate details. By this section, CAMA mandates the disclosure of beneficial interests in a company, even where such interests are held through nominal holders or in trust.
12	Lawful Interception of Communications Regulations: 2019/Section 10	By Section 10, NCC can direct licensees to install interception capabilities that allow or permits interception of communications and they are bound to comply with the notice and such duty shall be enforceable in the court of law by civil proceedings initiated by the Commission.
13	Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011: Sections 19 & 20	This law requires telecommunications firms to register all subscribers.

How do state agents misuse the above security laws? The laws listed above have gained notoriety for providing a legal foundation for the suppression of civil rights and freedom under the pretext of counterterrorism or protecting national security. Top on this list is the constitutional exception to human rights guarantees in Section 45 of the Constitution of the Federal Republic of Nigeria which legitimizes derogations to personal liberties in certain circumstances such as in the interest of defence, public safety, public order, public morality or public health. This constitutional provision is the foundation for the anecdote that constitutional rights are not "absolute". National security agencies often latch onto this constitutional provision to restrict civic activities under the banner of defending national security.

The Terrorism Prevention Act, amended in 2013 ("TPA"), and the regulations made thereunder, add to the list of major drivers of the misuse of CT architecture in Nigeria. Though enacted in compliance with Nigeria's international CT obligations and under immense pressure from FATF, the biggest flaw of the TPA is the failure to clearly delineate what amounts to terrorism. The definitional uncertainty has opened the doorway for the government to brand any dissenting group of persons or movements as "terrorists" and then visit the consequences prescribed under the law upon such persons or movements. Persons accused of terrorist activities face immediate repercussions even before being found guilty of the offence such as arrest without bail, freezing of accounts and incalculable reputational damage.

Nigerian NGO, Spaces for Change, hosts an online database that documents past and current crackdowns on the civic space, including how security laws are misused to restrict the civic space.[83] The database also reveals persistent and varying, but broad-based approaches for restricting the Nigerian civic space. According to Spaces for Change, one of the most misused tactics for advancing repressive agendas is the overbroad interpretation or application of existing CT and security laws and regulations. A classic example is the robust use of the Cybercrimes (Prohibition etc.) Act of 2015 to press terrorism charges and prosecute critics[84] and commentators[85] on Facebook[86] and Twitter for making posts critical of state executives. Bloggers and active citizens are the primary targets of the overbroad legal enforcements by the Department of State Security (DSS).[87] This law—Cybercrimes Law of 2015—also provided the impetus for the defunct Special Armed Robbery Squad (SARS) to execute a reign of terror on citizens through indiscriminate arrests of young Nigerians who were in possession of electronic gadgets such as computers and sophisticated phones on the supposed suspicion that they were cybercriminals.

Other ways security and CT laws are misused include making new laws where none exist to justify their action;[88] abuse of government discretionary powers;[89] and the diversion of the country's legal security structures.[90] In the next paragraph, we discuss how the state is pushing for more legislative and regulatory powers to expand its surveillance, punitive and repressive agendas.

3.2. The State's Thirst for More Power

Despite the litany of existing enactments at the federal and state levels granting unfettered powers on state actors to surveil citizens and restrict their civic freedoms at the altar of national security, the Nigerian federal legislature is littered with assorted legislative proposals seeking to increase governmental powers to regulate the social media, control the digital spaces, undertake surveillance operations and intrude upon personal privacy. The numerous bills before the federal legislature containing amendment proposals for expanding state's regulatory powers underscore the popularity of weaponizing legislation to silence dissent. Where legislative measures are foiled by pushback by civil society, alternative routes can be explored to achieve the same objectives. One such alternative route is using fake news or disinformation as an excuse for imposing restrictive measures. The fake news narrative was used to ban social networking sites like Twitter. While it is true that the desire to revamp national

83 See www.closingspaces.org

84 Closing Spaces Database, Nigerian Lawyer Slammed with Terrorism Charges for Criticising State Governor, Please see: https://closingspaces.org/incident/nigerian-lawyer-slammed-with-terrorism-charges-for-criticising-stategovernor/

85 Closing Spaces Database, At Last, PDP New Media DG, Nwaogwugwu Granted Bail In High Court, , https://closingspaces.org/incident/at-last-pdp-new-media-dg-nwaogwugwu-granted-bail-in-high-court/

86 TV360: 70 Days in Custody; The Case of Emperor Ogbonna, https://www.youtube.com/watch?v=7AIhPYzCOY&feature=youtu.be

87 Victoria Ibezim-Ohaeri, Galvanizing Collective Action to Protect Nigeria's Civic Space, published by Shehu Musa Yar Adua Foundation, 2021, https://yaraduafoundation.org/files/Galvanizing%20Collective%20Action.pdf

88 Over the years following FATF Recommendation 8, the government has sought to enact various restrictive legislation including several bills for the regulation of NPOs in Nigeria; the Bill Prohibiting Frivolous Petitions which would have required citizens to depose to affidavits in law courts before posting any statement on social media with respect to the government or its officials; regulations increasing the cost of data in another bid to restrict citizen activities online; etc.

89 Twitter has been a preferred platform for civil engagement in Nigeria and was a major driver of the #EndSARS movement, #RevolutionNow, and so forth. However, following Twitter's censoring of a tweet by the Nigerian President for being inciting, Nigeria suspended Twitter in Nigeria on 4 June 2021. See Brookings "Nigeria's Twitter ban is a misplaced priority." Available at https://www.brookings.edu/blog/africa-in-focus/2021/08/11/nigerias-twitter-ban-is-a-misplaced-priority/, accessed 26 September 2021

90 See the typologies in Section 2.2

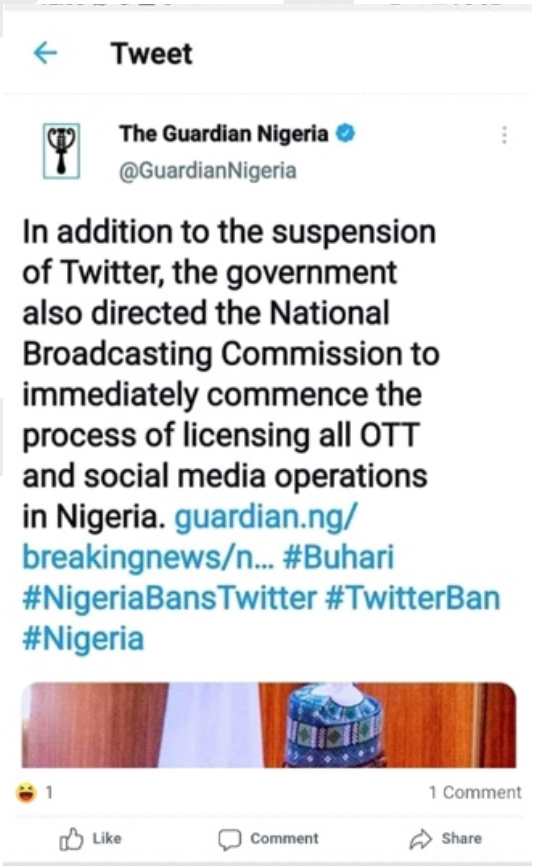
information infrastructure to keep up with the pace of modern technological innovations has necessitated policy and legal reforms, the authorities are equally capitalizing on the reforms to sneak in restrictive provisions designed to increase national revenues and give themselves more control over the activities of civic actors and businesses. Some notable amendments being considered are:

NITDA Act Amendment Bill: Recent proposals to amend the NITDA Act seeks to expand the agency's statutory functions to include the power to fix licensing and authorization charges, collect fees and penalties and issue contravention notices and non-compliance with the Act.[91] The agency will also reserve the right to "enter premises, inspect, seize, seal, detain and impose administrative sanctions on erring persons and companies who contravene any provision of the Act," subject to a court order.[92]

Social Media Bill: Similarly, Section 12 of the proposed Protection from Internet Falsehoods, Manipulations and Other Related Matters Bill, 2019[93] granted law enforcement departments (the Nigerian Police Force) the power to issue an access blocking order by directing the Nigerian Communications Commission (NCC) to order the internet service provider to disable access to users in any online location that false communication emanates from. When this directive is issued, the NCC must give the internet access service provider an access blocking order.

Hate Speech Bill: The National Commission for the Prohibition of Hate Speeches Bill 2019—popularly known as the Hate Speech Bill criminalized various forms of expressions that could stir up ethnic hatred. Proposed sanctions include death sentence for specific offences. The bill also contains vague offences such as those "likely to be prejudicial to Nigeria's security, public safety, tranquillity, public finances and friendly relations of Nigeria with other countries."[94]

National Broadcasting Commission Amendment Bill: Two contentious bills seeking to restrict media and journalistic initiatives are currently going through parliamentary consideration. In the first part, one of the bills sponsored by Unyime Idem (PDP, Akwa-Ibom), in March 19, 2020, is seeking to regulate tariff of digital satellite service providers. It wants to achieve this aim by giving the National Broadcasting Commission (NBC), the powers to review broadcasting codes and regulate the tariff charged by digital television platforms. If passed, digital satellite service providers like DSTV, StarTimes, TSTV, GOTV and others will have their subscriber fees regulated.[95]



91 See Section 6
92 See NITDA amendment Bill: https://drive.google.com/file/d/1fOTMidYbICS10alwWpjdDdgyCBhGUNM7/view
93 Sponsored by Senator Mohammed Sani Musa (APC Niger East), 2019
94 Section 4 of the Bill
95 Bakare Majeed, Premium Times, Groups reject bill seeking to empower NBC to regulate DSTV, Startimes' tariffs, Accessed via https://www.premiumtimesng.com/news/top-news/468179-groups-reject-bill-seeking-to-empower-nbc-to-regulate-dstv-startimes-tariffs.html

Nigerian Press Council (NPC) Act Amendment Bill: Another bill stirring controversy is the proposed amendment of the Nigerian Press Council (NPC) Act. The proposed amendment vests the Executive Secretary of the Council Board with unfettered administrative powers, whittling down the powers of the council board to a mere "advisory capacity on a part-time basis without direct interference in the day-to-day administration of the council". Not only that, the President and the Minister of Information will now appoint the Chairman of the Press Council Board. Subjecting the leadership of the associational body for journalists to full state control sparked widespread suspicion of political interference and strangulation of media operations. The tide of restrictive legislations, the intense surveillance of social media and online spaces, the wave of arrests of bloggers and social critics are all combining to present a renewed momentum to shrinking the space for free expression, for dissent and for mobilization.

3.3. How States Apply Security Laws on Civic Actors

There are four major ways the Nigerian state applies security laws to repress the activities of the civil society. The most popular is by (1) recharacterizing organised dissent as terrorism; (2) proscription of self-determination movements; (3) criminalizing free expression and (4) restrictions on open democracy. Multiple terminologies—like human rights defenders (HRDs), civil society leaders, critics, activists, social movements, feminists, social movements, journalists, humanitarian workers—are popularly used to refer to the considerable number of civic actors and organizations taking institutionalized and non-institutionalized forms of action to demand accountability, push for social change, promote and defend human rights in Nigeria. Regardless of the operational nomenclature adopted, they all form part of the Nigerian civil society movement and have become key drivers of policy, working together with the government at all tiers to provide new ideas to strengthen democracies and contribute to solving some of the pervasive socio-economic and political problems ravaging the country.

1. Recharacterizing organised dissent as terrorism

Accusing social justice campaigners of terrorism is the most popular strategy used to suppress organized dissent. The Nigerian government has used the TPA liberally in clamping down on civil society and frightening activists to silence. This practice of labelling civil society activists as terrorists is not new. This has been a longstanding strategy deployed by state actors globally to discredit the personalities and statements of activists. In Nigeria, this narrative has been used by both military and democratic governments to suppress opposition and accountability

How States Apply Security Laws on Civic Actors

- Recharacterizing organised dissent as terrorism.
- Proscription of self-determination movements
- Criminalizing free expression
  Restrictions on open

campaigns. In 1967, the Yakubu Gowon-led military government arrested Nobel Laureate Mr. Wole Soyinka, for his criticism of his administration. Soyinka and 11 dissidents were charged with terrorism and treasonable offence in 1997 by the Sani Abacha-led administration, and in 2004, for criticizing the re-election of President Olusegun Obasanjo.

In the aftermath of the #EndSARS protests, the government of Nigeria, through the Central Bank of Nigeria ordered the freezing of bank accounts belonging to forefront campaigners pursuant to Section 13(1)(a) and(b) of the TPA and Regulation 31(2)(a) and (3)(b) of the Central Bank of Nigeria Anti-Money Laundering/Combating the Financing of Terrorism Regulations, 2013 ("CBN CT Regulation").[96]

> *Section 13(1)(a) and(b) of the TPA provide as follows: "Any person or entity who, in or outside Nigeria- (a) solicits, acquires, provides, collects, receives, possesses or makes available funds, property or other services by any means to (i) terrorists, or (ii) terrorist groups, directly or indirectly with the intention or knowledge or having reasonable grounds to believe that such funds or property will be used in full or in part in order to commit an offence under this Act or in breach of the provisions of this Act, (b) possesses funds intending that it be used or knowing that it will be used, directly or indirectly, in whole or in part, for the purpose of committing or facilitating the commission of a terrorist act by terrorist or terrorist groups, commits an offence under this Act and is liable on conviction to imprisonment for life imprisonment."*

The relevant provisions of the CBN's CT Regulation relate to taking actions to prevent laundering money for financing of terrorism. As argued by the CBN in the court proceedings, "There is a grave allegation that the defendants are involved in suspected terrorism financing via their bank accounts in contravention of the provisions of extant laws and regulations." The aforesaid transactions undertaken by the defendants, using their bank accounts, can cause significant economic and security harm to the public and the Federal Republic of Nigeria if left unchecked".[97] Without mentioning what the suspected terrorist actions were, and without having to justify that the actions were terrorist in nature, the court granted CBN's request to freeze the protestors' accounts for 180 days subject to renewal.[98] According to one of the victims of this order, no investigation was carried out into the accusation that she was involved in terrorism financing or money laundering during the pendency of the freezing order.[99]

96 Nairametrics "#EndSARS: CBN says funds in frozen accounts may be linked to terrorist activities." Available at https://nairametrics.com /2020/11/11/endsars-cbn-says-funds-in-frozen-accounts-may-be-linked-to-terrorist-activities/, accessed 26 September 2021

97 Ibid.

98 Ibid. Another report states that the freezing order was for 90 days – Premium Times "#EndSARS campaigner threatens to sue CBN for unlawful freezing of account." Available at https://www.premiumtimesng.com/news/top-news/441925-endsars-campaigner-threatens-to-sue-cbn-for-unlawful-freezing-of-account.html, accessed 26 September 2021

99 Premium Times, ibid.

2. Proscription of self-determination movements

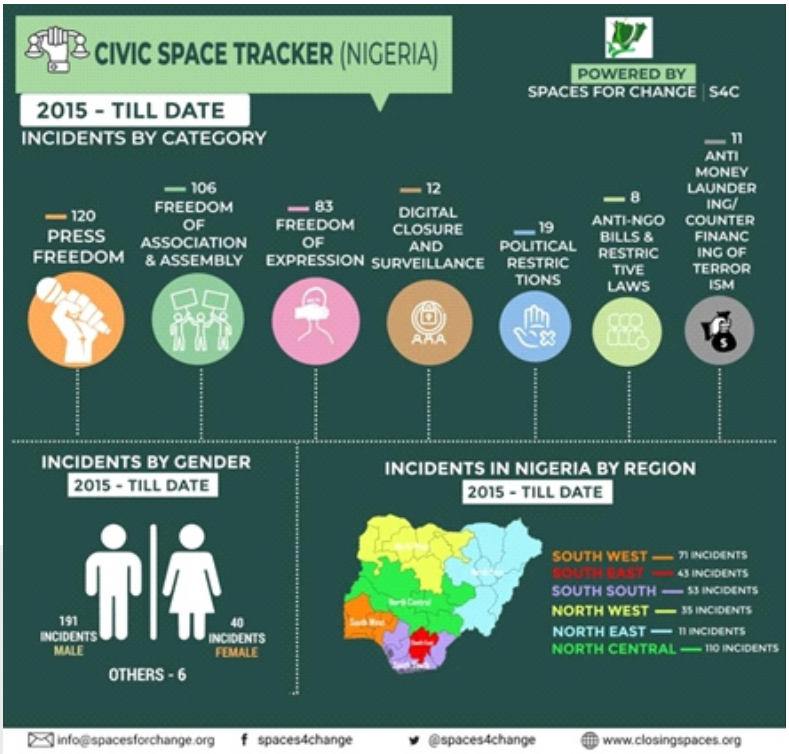
Another notable way the government weaponizes the TPA is through its power to proscribe organisations or groups as terrorists. Popular examples of organisations proscribed as terrorist groups based on questionable criteria are the Islamic Movement in Nigeria also known as the Muslim Brotherhood, and the Indigenous People of Biafra (IPOB). By so doing, the government has been able to recharacterize legitimate religious and democratic movements as terrorist groups and therefore visit upon them the consequences stipulated under the TPA. The Nigerian government proscribed and designated IPOB as a terrorist group in 2017 while the group leader, Nnamdi Kanu was arrested by Nigerian security forces on 19 October 2015 and again in 2021, on charges of terrorism. The bloodshed visited upon IPOB agitators as chronicled in a heart-wrenching report by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; Special Rapporteur on extrajudicial, summary or arbitrary executions; Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association; and Special Rapporteur on minority issues, pursuant to Human Rights Council resolutions 40/16, 44/5, 43/4, 41/12 and 43/8.[100]

In contrast, the country has been quite lenient to actual Boko Haram terrorists. The Operation Safe Corridor[101] and the Demobilisation, Disassociation, Reintegration Reconciliation (DDRR) programme implemented in the Northeast Nigeria[102] shows the willingness of the government to deal civilly with "repentant" Boko Haram terrorists than with other groups whose proscription was for the political objective of suppressing civil liberties and self-determination movements. The government also sends the signal that allies enjoy some level of protection from CT measures. Recently, a Minister in the government whose previous rhetoric expressed support for Al Qaeda was not relieved of his post.[103]

3. Criminalizing free expression

The Closing Spaces Database documented 120 incidents of clampdowns on journalists and pressmen alone from 2015 to date on account of their free expressions through the news media.[104] The clampdowns comprise arrests,[105] detentions, threats,[106] sanctions, office raids, shutdowns, physical attacks/harassments[107] and prosecution carried out by various security and government agencies such as the Nigerian Army, the Police Force, Special Anti-Robbery Squad (SARS), State Security Services or Department of State Security (DSS) and various state governments.[108] The Closing Spaces Databases contain serial documentations of incidents of shutting down broadcast stations based on "inciting broadcasts"[109] or "orders from above"[110] or "publishing false information."[111] Just as the SSS/DSS leads crackdown operations and

100 See https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25563
101 See the Preventing and Countering Violent Extremism Policy Framework and National Action Plan. Available at https://ctc.gov.ng/about-ctc/, accessed 26 September 2021
102 See "Counter-Terrorism Centre Strategic Report 2018." Available at https://ctc.gov.ng/wp-content/uploads/2020/03/REVIEW-OF-ACT-Inner-2019.pdf, accessed 26 September 2021
103 Vanguard "Presidency's defence of Isa Pantami." Available at https://www.vanguardngr.com/2021/05/presidencys-defence-of-isa-pantami/, accessed 26 September 2021
Closing Spaces Database: wwww.closingspaces.org
104 Asadu, C. (2018, March 13). The police on Tuesday arrested Abdullahi Krishi, House of Representatives correspondent of Daily Trust. TheCable. https://www.thecable.ng/just-police-arrest-daily-trust-reporter-national-assembly
105 .News24. (2017, September 23). Nigerian journalist detained over report on flood camp protest. News24. https://www.news24.com/news24/Africa/News/nigerian-journalist-detained-over-report-on-flood-camp-protest-20170923
106 Media Rights Agenda(MRA). (2005, July 29). Airport security officers prevent newspaper editor from travelling. Ifex. https://ifex.org/airport-security-officers-prevent-newspaper-editor-from-travelling/.
107 See also Sahara Reporters. (2020, September 7). Aisha Buhari Attacks Daily Trust Artist, Bulama, Over Cartoon On Daughter's Lavish Wedding. Sahara Reporters. http://saharareporters.com/2020/09/07/aisha-buhari-attacks-daily-trust-artist-bulama-over-cartoon-daughter%E2%80%99s-lavish-wedding
108 Closing Civic Spaces in Nigeria. (2021). Incidents of closing civic spaces and human rights violation in Nigeria. Available at https://closingspaces.org/
109 Sahara Reporters. (2019, March 2). EXCLUSIVE: NBC Shuts Down Jos Radio Station After 'Order From Presidency'. Sahara Reporters . http://saharareporters.com/2019/03/02/exclusive-nbc-shuts-down-jos-radio-station-after-order-presidency
110 John, C. (2018, March 13). Presidency bars PUNCH, others from covering Buhari's Benue
111 Ameh, G. (2018, December 20). Journalist remanded in prison over report against Kebbi govt. Daily Post. https://dailypost.ng/2018/12/20/journalist-remanded-prison-report-kebbi-govt/



prosecutions premised on violations of cybercrime and terrorism legal regimes, the National Broadcasting Commission (NBC) takes the lead in slamming fines[112] and shutting down broadcast media stations. Reporters have also been forced to delete pictorial[113] or video evidence[114] of these infractions for various reasons such as violating the provisions of the Penal Code.[115] Other notable methods adopted by security agencies across the country to repress civic engagements online, as well as to surveil civic actors and intrude[116] on personal privacy include cutting off internet access, destruction of equipment/properties and property/asset takeovers.[117]

Defamation of character is another legal euphemism used to justify the misuse of security laws to repress free expression. For reporting about a protest by displaced persons about the diversion of relief materials from a camp for flood victims, Emmanuel Atswen, a reporter with the state-run News Agency of Nigeria (NAN) was arrested and detained in September 2017. The reporter was arrested on the ground of defamation of character and falsehood on the orders of[118] Benue State Commissioner for Water Resources and Environment involved in the relief efforts. In the same vein, a Premium Times reporter, Mr. Ogundipe, was arrested for allegedly publishing the Inspector-General of Police's interim report on the investigation on the former Director-General of DSS, Lawal Daura. The report was based on the contents of documents regarded as inimical to state and national security. He was arraigned and charged for "criminal trespass, theft … and having possession of Police Interim Investigation report" under sections 352, 288, and 319(a) of the Nigerian Penal Code.[119]

112 Premium Times. (2022, October 26). #EndSARS: SERAP fumes as NBC fines Channels, AIT, Arise TV. Premium Times. https://www.premiumtimesng.com/news/more-news/423160-endsars-serap-fumes-as-nbc-fines-channels-ait-arise-tv.html

113 Adejumo, K. (2020, January 15).

114 Committee to Protect Journalists. (2016, May 23). Nigerian journalists detained for investigating alleged water theft. Committee to Protect Journalists. https://cpj.org/2016/05/nigerian-journalists-detained-for-investigating-wa/

115 Adejumo, K. (2020, January 16). Police Interrogate PREMIUM TIMES' Journalist Over Report Exposing Islamic Cleric Who Raped 16-Year-Old. https://www.premiumtimesng.com/news/more-news/372729-police-interrogate-premium-times-journalist-over-report-exposing-islamic-cleric-who-raped-16-year-old.html

116 Media Rights Agenda (MRA). Nigeria: armed men attack TV crew, vandalise vehicles and broadcast equipment. IFEX. https://ifex.org/nigeria-armed-men-attack-tv-crew-vandalise-vehicles-and-broadcast-equipment/

117 See also Ojoye, T. (2019, January 8). Military invasion of Daily Trust, indefensible. Punch. https://punchng.com/military-invasion-of-daily-trust-indefensible/

118 The Bridge News. (2018, July 15). Armed policemen take over Ekiti Radio, TV stations. The Bridge News. https://www.thebridgenewsng.com/2018/07/15/armed-policemen-take-over-ekiti-radio-tv-stations/
Vanguard, Police arrest NAN reporter for "defamation of character, falsehood", https://www.vanguardngr.com/2017/09/police-arrest-nan-reporter-defamation-character-falsehood/

119 Vanguard, Police arrest NAN reporter for "defamation of character, falsehood", https://www.vanguardngr.com/2017/09/police-arrest-nan-reporter-defamation-character-falsehood/
Committee to Protect Journalists, Nigerian journalist jailed for refusing to reveal source, August 2018, Accessed via https://cpj.org/2018/08/nigerian-journalist-jailed-for-refusing-to-reveal/

4. Restrictions on open democracy

Before the era of digital revolution, the laws mostly misused to target critics range from sedition and defamation provisions to those relating to treason. Treasonable felony remains popular till date. Rallies have been criminalised, suppressed or repressed while arrests have been made of self-determination agitators in the southwest region.[120] At least one person has been reportedly killed in one of the rallies.[121] Subsequently, a leading figure of the self-determination group, Sunday Adeyemo, has had his house raided on ground of gun running and treason.[122] Since then, self-determination agitations and rallies have seen renewed repression. Added to this is the state propaganda against agitators for self-determination as criminals, anti-state and political agents.[123]

Police units are also notorious for arresting, detaining and forcing detainees to reveal their news sources following hours of gruelling interrogation.[124] The Official Secrets Act is usually invoked to support these inactions by the police. The Official Secrets Act restrains public officers from transmitting any classified matter to unauthorized persons. Determined to know how a Nigerian journalist had access to classified information that reportedly embarrassed the Swiss Government, the State Security Service arrested and detained the Bureau Chief of Daily Independent newspaper, Tony Ezimakor, insisting he must disclose his sources as a precondition for his freedom.[125]

Open democracy is further restricted when state agents use national security buzzwords to recolour purely democratic agitations. During the #ENDSARS protest in October 2020, officials and loyalists of the government framed the #ENDSARS movement as a campaign for regime change to topple the current political administration.[126] Such rhetoric not only discredits the legitimate grievances of #EndSARS supporters, but also taints the peaceful agitations with the same ethnic and regional brush used to characterize serious security breaches and felonies such as treason, rebellion or inciting revolt or violence against a lawful authority. These narratives provide justifications for the deployment of highhanded responses including military to suppress peaceful assemblies and open democracy.

CONCLUSION

As we have seen, the use of legislative measures to stifle dissent never goes out of fashion. This chapter has provided a very broad overview of the legal environment enabling digital repression to flourish in Nigeria, highlighting how the enactment of security laws facilitates and augments cracks in the civic space. Whether it is the campaign activities of the Free-Zakzaky Islamic religious group or the non-violent agitations of Indigenous People of Biafra (IPOB) or the good governance demands of the #RevolutionNow protesters or the youthful remonstrations of #EndSARS, security forces have consistently used security laws to justify the use of maximum force to repress organized dissent.

120 Oluwakemi Adelagun, Premium Times, Police disperse Yoruba nation agitators; July 3, 2021, Accessed via www.premiumtimesng.com/regional/ssouth-west/471408-police-disperse--yoruba-nation-agitators.html. accessed 27 July, 2021

121 Oluwakemi Adelagun, Premium Times,Woman shot at Yoruba Nation rally, July 3, 2021; Accessed via www.premiumtimesng.com/regional/ssouth-west/471423-woman-shot-at-yoruba-nation-rally.html. accessed 27 July, 2021

122 Chinedu Asadu, DSS confirms raid on Igboho's house, declares him wanted, July 1, 2021; Accessed via https://www.thecable.ng/breaking-dss-launches-manhunt-for-sunday-igboho-after-recovering-arms-ammunition-from-his-house

123 www.vanguardngr.com/2021/07/igboho-fg-beninese-lawyers-battle-over-extradition-in-court/amp. accessed 29 July, 2021

124 Ebuzor, C. (2018, August 14). Premium Times journalist detained over a story. Pulse Nigeria. Accessed via https://www.pulse.ng/news/local/samuel-ogundipe-premium-times-journalist-detained-over-a-story/xbesbp0

125 Ogundipe, S. (2018, March 4). SSS wants detained Nigerian journalist to disclose sources before release. Premium Times. https://www.premiumtimesng.com/news/headlines/260695-sss-wants-detained-nigerian-journalist-disclose-sources-release.html

126 Vanguard, #EndSARS: Northern Governors sue for peace, condemn violence, October 23, 2020; Accessed via https://www.vanguardngr.com/2020/10/endsars-northern-governors-sue-for-peace-condemn-violence/

No doubt, existing security laws, especially the TPA and the Cybercrimes Act, are necessary in a clime ravaged by organized crime. However, it is particularly worrying to see that these laws have not been deftly applied against the real criminals, but rather, are overstretched to rope targeted actors into the ambit of security-based misdemeanors. Famous cybercriminals such as Ramon Abas (AKA, Hushpuppi); Obinwanne Okeke (AKA Invictus Obi), to mention but a few—both of whom are currently facing prosecution abroad—were neither apprehended nor prosecuted under the law in Nigeria. Evidence is also emerging of collusion between cybercriminals and top law enforcement agents.[127]

The way security laws have been applied on a wide range of civic actors establish the connections between the existing legal apparatus with the government's repressive intent. Consequently, most forms of organized dissent in the country—whether religious, regional, political—have been met with stiff resistance and their organizers have become frequent targets of political crackdowns by the Nigerian government.

The way security laws have been applied on a wide range of civic actors establishes the connections between the existing legal apparatus with the government's repressive intent. Nigerians had hoped that the return to civil rule would birth a new era where civil liberties are upheld and respected by state agents. As the chronicle of security-related crackdowns on civic actors detailed in this chapter demonstrates, the return to democratic rule in 1999 did not end the culture of civil society repression. Instead, the aggression towards civil society has assumed different dimensions: it is now anchored on strong legal foundations and neatly executed with the aid of technology-enabled methodologies.

127 BBC News "Abba Kyari: The Nigerian super sleuth wanted in the US." Available at https://www.bbc.com/news/world-africa-58079504, accessed 26 September 2021

CHAPTER 4

THE MASSIVE ACQUISITION OF INVASIVE TECHNOLOGIES IN NIGERIA: DRIVERS, SUPPLIERS AND VICTIMS

© *NgGossips.com*

In the bid to rout unabating terrorism in certain regions of the country, banditry, cybercrimes and other forms of organized crimes, federal and state governments have doubled up budgetary allocations, public spending and procurements on invasive technologies and communications systems. Although these massive acquisitions are made in the name of security, this chapter examines the huge disparities that exist between the stated official motivations and actual use of these technologies for advancing purely political agendas, corrupt enrichment and to foster a climate of digital repression. From that discussion, we delve deeper into understanding how these trends have advanced (what incentives, motivations have led to their uptick) and what the implications are for the civic space in Nigeria.

Beginning from 2010, there has been a marked increase in the influx and use of sophisticated surveillance and hacking technologies for suspected nefarious ends. Motivations for these acquisitions vary, but evidence shows these procurements are largely driven by partisan and political considerations on the one hand, and the fight against terrorism on the other. A third reason for these massive acquisitions is political corruption, made possible when political elites award supply contracts to allies and cronies, circumventing due process and public procurement regulations for pecuniary gains.

4.1. Drivers & Forces Behind the Massive Acquisition of Invasive Technologies

Elections: Weakening the Political Opposition

National elections are primary drivers of surveillance operations. It is the time fierce and obscenely expensive electoral contestations between political heavyweights prompt candidates to know what their opponents are saying or planning to do. Old and new start-ups in surveillance systems around the world latch onto the opportunity to sell spying technologies to willing and ready customers determined to spy on and weaken the oppositions' political base. One such start-up is Circles, a surveillance firm reputed for its abusive spyware technology system with a capacity to listen to phone conversations and also monitor the location of phones around the world.[128] The Circles' spyware sold only to nation-states can be connected locally using in-country telecommunications infrastructure, or its cloud system known as the "Circles Cloud".

Corroborating the attacks on opposition politicians, an excerpt from a media report provides deep insight into how politicians used CIRCLES 3G to violate opposition targets' personal privacy, geolocation information and websites without any consequences.

> *"Our investigations show that in the run up to the December 2015 elections in Bayelsa, Mr. Dickson used this spying tool to track his prime challenger, Timipriye Sylva. Mr. Dickson did not stop at Sylva, he also tracked phone numbers belonging to Mr. Sylva's wife, aides and loyalists. This piece of technology was also deployed in hunting down Tonye Ekio who was incarcerated by the governor, late 2013, over a Facebook post that was critical of Mr. Dickson's government. An ex-militant, Africanus Ukparasia, also known as "General Africa", was also a target of Mr. Dickson's surveillance. Although Circles sold the technology to Mr. Dickson with an apparent understanding to use it within his territory, the governor used it to eavesdrop on targets far away from Bayelsa. For instance, some of the daily target reports seen by PREMIUM TIMES shows Mr. Dickson tracing Mrs. Sylva's phone numbers to locations in Abuja. Another report shows him tracing a target called E-Genle to a location outside the country."*

Along with using spying tools to track their prime challengers, targeted surveillance is often extended to family members of the opposition, including their wives, children, aides and loyalists in the run-up to elections. Those covering the intense political horse-trading and

128 Marczak, B. Scott-Railton, J. Rao, S. Anstis, S. Deibert, R. (2020, December 1). Running in circles: Uncovering the Clients of cyberespionage firm circles. The Citizen Lab. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

intrigues, or monitoring the outcomes of the elections are not spared. In 2015, an intrusive cyberattack on the servers of Premium Times shut down the news platform's operations for four days. This prevented the online news outfit from briefing local and global observers with live updates on Nigeria's 2015 presidential and National Assembly elections.[129] At least, three online newspapers—Premium Times, Gazette[130] and Sahara Reporters[131]—have accused the federal government of using hacking tools to shut down their websites at different times.

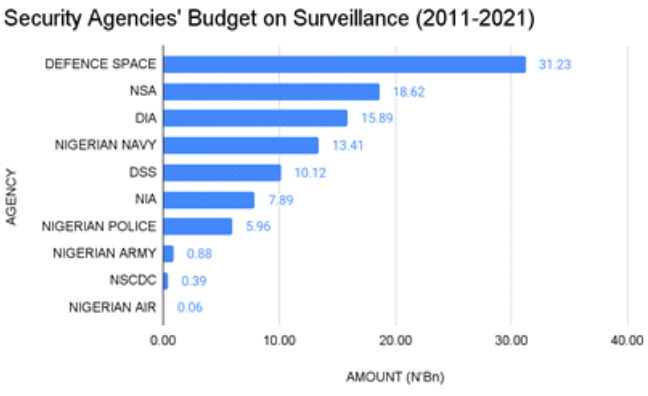
As state governments were amassing spying and hacking devices to achieve political ends, the federal government also intensified its digitalized undercover activities through humongous budgetary provisions and acquisition of sophisticated surveillance hardware and software developed for counter-terrorism purposes.

-Acquisitions for countering Boko Haram insurgency and terrorism

As state governments were amassing spying and hacking devices to achieve political ends, the federal government also intensified its digitalized undercover activities through humongous budgetary provisions and acquisition of sophisticated surveillance hardware and software developed for counter-terrorism purposes. Countering terrorism—especially the Boko Haram-led terrorist activities in northeastern Nigeria— provides states with the safest legal justification for these acquisitions. In this connection, federal agencies have made heavy policy and resource commitments for surveillance. For instance, the 2013 budget included provisions for the purchase of a Wise Intelligence Network Harvest Analyzer System, Open-Source Internet Monitoring System and Personal Internet Surveillance System at a cost of N9.496 billion ($61.26 million).[132] Between 2011 and 2021, government security agencies have budgeted at least N104.46 billion for tracing and monitoring communication systems.

The security provisions in the budget are to be allotted to various security agencies tasked with ensuring national security such as:

- Defence Space Administration (DSA)
- National Security Adviser (NSA)
- Defence Intelligence Agency (DIA)
- Nigerian Army
- National Intelligence Agency (NIA)
- Department of State Services (DSS)
- Nigeria Police Force (NPF)
- Nigerian Security and Civil Defence Corps (NSCDC)
- Nigeria Prisons



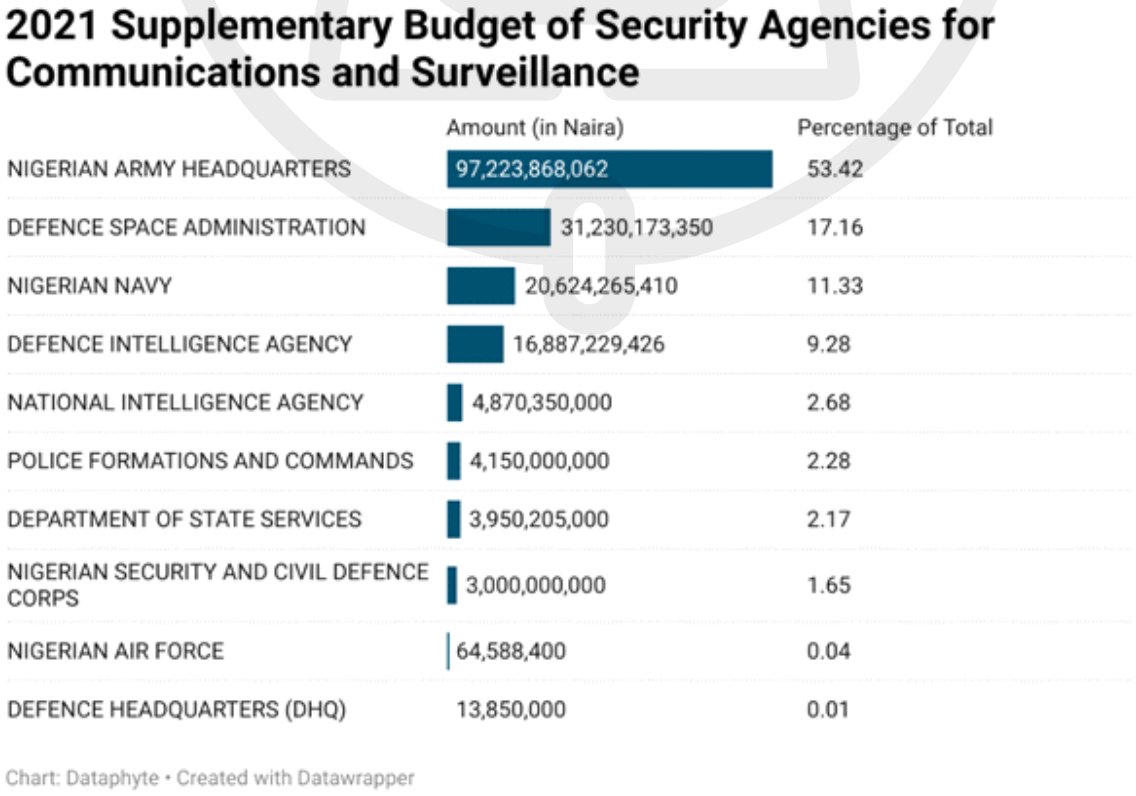
129 Ogala, E. (2015, April 5). How PREMIUM TIMES survived massive cyber attacks during presidential election coverage. Premium Times. https://docs.google.com/document/d/11CrFKOiRnsOAIuTDkFuJT9lOekFOnbR_Nj1LrhqaRW0/edit

130 Qurium, Nigeria Attempts to Silence the Investigative Media Peoples Gazette by Ordering Blocking, –Nigeria attempts to silence the investigative media Peoples Gazette by ordering blocking Qurium Media Foundation

131 Victor Ekwealor, Sahara Reporters Targeted In A Website Hack Techpoint Africa, January 11, 2017:

132 Ogala Emmanuel, Premium Times, EXCLUSIVE: Jonathan awards $40million contract to Israeli company to monitor computer, Internet communication by Nigerians | Premium Times Nigeria (premiumtimesng.com)

Analysis show that the Defence Space Administration planned to spend N31.23 billion on surveillance. This figure represents 29.9% of the total figure of N104.46 billion for the years under review. The Office of the National Security Adviser (ONSA) budgeted N18.62 billion while N15.89 billion was set aside for the Defence Intelligence Agency (DIA). Recently too, the Nigeria federal legislature approved the procurement of 4.87 billion naira worth of surveillance technologies "to intercept Thuraya mobile calls and solution" and WhatsApp's voice and text messages.[133] In the 2021 supplementary budget, the National Assembly also approved the request of 7.46 billion naira from the Nigeria's Defence Intelligence Agency (DIA) to launch a purported "independent lawful interception platform – voice and advanced data monitoring". These supplementary budgetary provisions are additions to the N30.82 billion originally budgeted for in the 2021 budget.



-Political corruption

Corruption is another major driver of the massive acquisitions of security-based technologies, hence the exponential rise and proliferation of surveillance capitalism in Nigeria. Beyond spying on opposition politicians to weaken their political capital, the importation of hacking expertise and tools has become a lucrative industry and conduit pipe for politicians and their cronies to divert and siphon public funds offshore. Politicians and their cronies have used own private companies to secure shady cybersecurity contracts intended to shut down online media platforms perceived to be sympathetic to opposition politicians.[134] Because these contracts are mostly awarded in violation of the due process, value for money and procurement regulations, they are brazenly inflated and stripped of open and competitive bidding.

133 Ode Uduu and Charles Mba, Dataphyte, Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians, Accessed via Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians | Dataphyte

134 Ogala Emmanuel, Premium Times, INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack 'unfriendly' websites, January 18, 2016; Accessed via https://www.premiumtimesng.com/investigationspecial-reports/196964-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websitesinvestigation-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websites-2.html

Most of these contracts were ultimately used to secure the services of different security firms to monitor political opponents' communication and obstruct the online presence of newspapers considered unfriendly to the re-election campaign of the administration. Despite overwhelming evidence of monumental corruption, the veil of "security", "intelligence" and "secrecy" surrounding the contract negotiations makes it easier for culprits to escape scrutiny and accountability. Although numerous national statutes—such as the Nigeria Constitution, the NCC Act and specifically the Nigeria Data Protection Regulations 2019—codify legal protections against privacy invasion, these protections are often subordinated to "national security". Public statements credited to the incumbent President Muhammadu Buhari and Abubakar Malami, the current Attorney-General of the Federation insist that "the Constitution is subservient to national security." These statements energise and embolden state agents to invoke national security[135] as an excuse to breach data protection protocols and award contracts to cronies for the implementation of arbitrary surveillance operations.

Company/Owner	Country	Buyer and User	Date	Purpose (How Do they work)	Value	Sources
Circles	Bulgaria	Mr Ifeanyi Okowa as Governor of Delta State	2016	3G communication interception meant listen to phone conversation and to monitor the location of phones anywhere in the world	About N63 million as two years maintenance fee	Premium Times, CitizenLab, IDS Surveillance Law in Africa: A review of six countries
Circles	Bulgaria	Nigerian Police Force	2010	3G communication interception meant listen to phone conversation and to monitor the location of phones anywhere in the world	N63 million annually to maintain	Premium Times, CitizenLab
Hacking Team	Italy	Seriake Dickson as Governor of Bayelsa State	2013	To hack computers and phones in Nigeria	N98 million	Premium Times, CIMA, CitizenLab
Mi Marathon Resources Limited via M.I. Smart Solutions, a subsidiary of MI Marathon	Australia	NSA, Jonathan Administration	April 2014	Contract to supply a stealth and intrusive GSM mass surveillance called Engage GI2 Tactical Solution developed by Verint	N335.1 million (USD1.6 million)	Premium Times
Romix Technologies in Cyprus together with Packets Technologies AD, an Israeli company operating out of Bulgaria and Romix Soilfix Nigeria Ltd, owned by Mr. Okupe and Ilan Salman, an Israeli	Cyprus	NSA, Jonathan Administration	June 2014	Supply and installation of cyber intelligence system software to carry out Distributed Denial of Service (DDoS) attacks on websites believed to be critical of Mr. Jonathan, ahead of the elections.	N398 million ($2 million)	Premium Times
Mi Marathon owners by Salman and Maoz Steinhauer	Australia	NSA, Jonathan Administration	April 2014	Fiber optic Landing Solution to create a backdoor access to all fibre optic cables landing in Nigeria for the office of the National Security Adviser.	N712.2 million ($3,580,000)	Premium Times
Elbit Systems, Israel	Israel	Jonathan Administration	April 2013	Wise Intelligence Technology (WiT) system to monitor computer, Internet communication by Nigerians	$40million	Premium Times; Roberts, Mohamed Ali, Farahat, Oloyede (2021) Surveillance

Circles	Bulgaria	Mr Uduaghan as Governor of Delta State	Feb 2012	3G communication interception meant listen to phone conversation and to monitor the location of phones anywhere in the world	N1.5 billion and an annual N31.9 million maintenance fee.	Sahara Reporters
Circles	Bulgaria	Seriake Dickson as Governor of Bayelsa State	July 2012	3G communication interception meant listen to phone conversation and to monitor the location of phones anywhere in the world	N1.7B and an annual N31.9M maintenance fee & N98 million	Premium Times, CitizenLab
V&V Limited and Circles	Nigeria and Bulgaria	Mr Rotimi Amaechi as Governor of Rivers State	June, 2010	Circle's spyware used to listen to phone conversation and to monitor the location of phones anywhere in the world	N2.3 billion	Premium Times
ZTE Corporation via China Eximbank	China	Government of Nigeria	August 7, 2010	Commercial contract for the Nigeria National Public Security Communication System Project. The second subcomponent = Video Surveillance Subsystem, comprising the installation of approximately 2,000 solar-powered CCTV cameras in Abuja and Lagos to monitor and reduce criminal activities including attacks, kidnappings and killings.	$470 million	AIDDATA
Unknown		Kaduna State Government under ElRufai		Mobile call monitoring and communication interception using geo-position interceptor and location of GSM, UMTS system	N2.55 billion	Premium Times
MPD Systems.	USA	Mr Rotimi Amaechi as Governor of Rivers State	2008	To purchase a C4i (Command, Control, Communications, Computers, and Intelligence) technology from an Israeli military security firm,	N.A	Premium Times
Unknown		DMI, Buhari Administration	2021	To intercept Thuraya mobile calls and solutions and Whatsapp's voice and messages.	N4.87 billion ($11.88 million)	Dataphyte; Roberts, Mohamed Ali, Farahat, Oloyede (2021) Surveillance
Unknown		DIA, Buhari Administration	2021	An independent lawful interception platform – voice and advanced data monitoring.	7.46 billion ($	Dataphyte

From the above table detailing the supply chain of makers and buyers of invasive technologies, different categories of actors emerge on the contractual scene. On the supply side, you have the makers/manufactures, the vendors and middlemen. On this side too, the Israeli-owned company, Circles, stands tall as the highest supplier to Nigeria, with clients spanning states, federal and independent security agencies. Circles

telephone tracking technology is primarily delivered through its start-up called V&V Limited. Other companies participating actively on the supply side are Elbit Systems, Romix Technologies, together with Packets Technologies AD, another Israeli company operating out of Bulgaria.

Different categories of actors emerge on the contractual scene. On the supply side, you have makers/manufactures, the vendors, and middlemen. On the demand side, there are customers or state agents who use the technologies to violate the privacy rights of citizens.

Circles' operations were first noticed in 2010 ahead of the 2011 general elections upon a state governor's request.[136] Under the cover of state policing, the same governor moved from the Circles spyware and ventured into the procurement of the C4i (Command, Control, Communications, Computers, and Intelligence) technology from an Israeli military security firm—MPD Systems—to monitor citizens' communication. Shortly afterwards, it became the regional pastime of South-south governors, especially Akwa-Ibom, Bayelsa,[137] and Delta States,[138] to purchase surveillance and spying technologies. Other states outside the region later followed. By failing to take appropriate steps to restrain the wrongful acts of these foreign suppliers, Nigeria is clearly in breach of its duty to ensure that individuals and communities do not suffer from harm caused by business-related abuses. Suppliers take advantage of the weak regulatory and importation controls that characterize many poor countries to perpetrate lawlessness and conduct their operations in a manner that increases the vulnerability of citizens to physical and mental hazards.

Another interesting finding is China's incursion into the Nigerian technology market, offering soft loans to the federal government to purchase their communications and surveillance equipment. Months after the government of Nigeria signed a $470 million commercial contract with the Chinese-owned ZTE for the Nigeria National Public Security Communication System Project on August 7, 2010, the China Eximbank and the Government of Nigeria signed a $399.5 million preferential buyer's credit (PBC) agreement for the same project. The project's second subcomponent—Video Surveillance Subsystem—involved the installation of approximately 2,000 solar-powered CCTV cameras in Abuja and Lagos to monitor and reduce criminal activities including attacks, kidnappings and killings.[139]

In the wake of the Twitter ban, the Nigerian government, through the office of the Presidency, reached out to the Cyberspace Administration of China (CAC) to discuss plans to build an internet firewall similar to the internet filtering system China operates, called the Great Firewall. The internet firewall is expected to create a separate network for the Nigerian Internet, giving the government greater control over social media platforms such as Twitter and Facebook.[140] If this firewall is installed, the Nigerian government will be able to block virtual private networks

136 Ogala, E, ibid.

137 Ogala Emmanuel, Premium Times, INVESTIGATION: Bayelsa Governor hires world's most ruthless hackers for N100M to hack computers, phones in Nigeria, Accessed via https://www.premiumtimesng.com/investigationspecial-reports/186391-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-computers-phones-in-nigeriainvestigation-bayelsa-governor-hires-worlds-most-ruthless-hackers-for-n100m-to-hack-c.html

138 Ogala, E. (2016, June 9). INVESTIGATION: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others. Premium Times, Available at, https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html

139 China Aid Data: https://china.aiddata.org/projects/30450/

140 Foundation for Investigative Journalism, EXCLUSIVE: Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall (2021) Accessed via https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

(VPN), which many Nigerians are using to access Twitter while the ban is in force. This firewall initiative is not just evidence of the government's determination to control online speech, but also shows how cooperation and bilateral relations with countries like China known for their authoritarian strategies and with a track record of suppressing the civic space facilitates digital repression in Nigeria.

Because corrupt enrichment often lies at the core of these transactions, politicians secure these contracts through companies incorporated as special purpose vehicles (SPVs) or through legal partnerships with the supplying companies, holding out the SPVs as their local partners. For instance, Romix Soilfix Nigeria Ltd., owned by a Nigerian politician, partnered with the Israelis Ilan Salman and Mi Marathon, owners of Salman and Maoz Steinhauer firm, to supply and install cyber intelligence system software designed to carry out Distributed Denial of Service (DDoS) attacks on websites critical of the then president ahead of the elections. Details of the execution of the contract worth over 3 million dollars remain sketchy, and no one has been held accountable.

On the demand side, there are customers or state agents who use the technologies to violate the privacy rights of citizens. State and federal governments, comprising mainly the federal security agencies, are the major patrons of surveillance technologies in Nigeria. Under the pretext of checkmating insecurity and banditry, state budgets are replete with budgetary provisions for the purchase of surveillance technologies. While Kaduna State government's 2017 budget earmarked N2.55 billion naira to procure mobile call monitoring and communication interception technologies,[141] CCTV equipment, drones, and geo-position interceptor and location of GSM, South-south's Delta and Bayelsa State governments took surveillance and communication interception programs to new heights with the acquisition of a latest tracking technology that allows them decrypt telephone calls made over 3G networks in real time.[142]

An analysis of the procurement timelines in Section 4.2 above shows that the actual and attempted purchases predominantly happened in 2010, 2014, 2016, 2018 and now 2021. These are averagely, one or two years before the general elections, and for the most part, acquired to monitor or intercept conversations of opponents and to obstruct free flow of communications over the airwaves. Bayelsa government's procurements were more brazen. The contracts, classified as "intelligence", were channeled through an Israeli company, NICE, and then V&V Nigeria, to procure Hacking Teams' most invasive and ruthless intrusion software called Remote Control Systems which can track the exact position of a user, even when abroad. These accounts validate the findings of a recent report which exposed African governments using an Israeli surveillance platform to snoop on private communications of citizens.[143] Nigeria was listed among states where security agencies are deploying technology supplied by the Israeli telecom surveillance company, Circles, to snoop on communications of opposition politicians, journalists and protestors. By extension, these "culprits in government" perpetrate clandestine hacking and surveillance on citizens, media outlets, opposition politicians with impunity.

141 Premium Times. (2016, October 21). Kaduna to spend N2.55 billion on drones, surveillance equipment in 2017. Premium Times, Available at https://www.premiumtimesng.com/regional/nwest/213304-kaduna-spend-n2-55-billion-drones-surveillance-equipment-2017.html

142 Ogala, E. (2016, June 9). INVESTIGATION: How Governors Dickson, Okowa spend billions on high tech spying on opponents, others. Premium Times, Available at, https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html

143 University of Toronto's Citizen Lab, Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles, December 1, 2020

4.2. Exploiting Spying Technologies to Stifle Dissent

Now that the actors—buyers and suppliers—behind the massive acquisitions of spying surveillance technologies and hackware have been established, the next is to determine how these technologies procured under the pretext of security and counterterrorism are now being diverted to stifle dissent from opposition, activists, media and civil society in general. Recent trends suggest that the diversion of security technologies for unrelated purposes may not be unconnected to vandalization and non-usage of these facilities. In Lagos, records show that no crime has been detected with the aid of the 13,000 Closed Circuit Television (CCTV) cameras, 6,000 streetlights and security sensors for surveillance and crime prevention installed across the state.[144] To save these surveillance gadgets from falling into disuse, they are diverted from tackling serious or potential security threats to spying the political opposition and other civic actors such as:

-Journalists and press men

A 2018 report used three case studies to illuminate how police authorities use phone records to lure and arrest journalists on account of their journalistic undertakings.[145] This tactic often involves the seizure of journalists' mobile phones and computers, and the use of forensic technology with capabilities to extract and decode every ounce of data stored within digital devices. Investigations reveal that security forces use Universal Forensic Extraction Device (UFED) and Forensic Toolkit (FTK)—sold by the Israel-based company Cellebrite and FTK sold by the U.S.-based AccessData Group—to retrieve information from the devices.[146]

Security agencies—like the State Security Service (SSS)—statutorily-mandated to undertake surveillance operations have been heavily criticised for operating with utmost secrecy, crass impunity, and total disregard for the rule of law.[147] Records further reveal how law enforcement agents easily obtain call records of individuals from network providers without a judicial warrant, consistent with the NCC Act of 2003. Asides the security agencies, telecoms regulators—like the Nigerian Communication Commission (NCC) and the National Information Technology Development Agency (NITDA)—play major roles in facilitating the government's digital surveillance activities. This seamless collaboration between security agencies and telecom regulators reek of a deliberate coordination of state mechanisms to engender a climate of repression. Telecommunication regulatory agencies can block access and regulate the internet through several technical protocols. The common methods include:[148]

Domain Name Server (DNS) Tampering: This method involves deregistering the domain name hosting a site, making it invisible so that intending users cannot access it.

IP Blocking: The authorities through this process blacklist the IP address of a site they wish to block. This interrupts attempts to access any site and connection cut through a surveillance process.

144 Titiola Oludimu, Techpoint, Lagos state's new surveillance system amplifies the need for a unified database (2017), Accessed via Lagos state's new surveillance system amplifies the need for a unified database Techpoint Africa

145 Jonathan Rozen, Committee to Protect Journalists, How Nigeria's police used telecom surveillance to lure and arrest journalists Jonathan Rozen, Committee to Protect Journalists, Nigerian Military Targeted Journalists' Phones, Computers With "Forensic Search" for Sources, October 22, 2019; Accessed via https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/

146 Nkanga, P. (2018, July 1). (2018, July 1). SPECIAL REPORT: How Buhari's govt detained Nigerian journalist for two years without trial. Premium Times. https://www.premiumtimesng.com/news/headlines/274467-special-report-how-buharis-govt-detained-nigerian-journalist-for-two-years-without-trial.html

147 Terman, R. Internet Censorship (Part 2): The Technology of Information Control. Townsend Center for Humanities, University of California, Berkeley. https://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control

Transparent HTTP Proxy: This is a server that intercepts connection between end users and the internet without any modification to request.

Outright ban of social media platforms: The Nigerian government banned citizens from using Twitter in June 2021. The targets of these methods include:

-Protesters

The #EndSARS and #RevolutionNow movements began on Twitter before cascading offline. The recent ban on Twitter, a popular mobilization platform used by local campaigners to foster civic engagement and challenge political impunity, points to the misapplication of the security paradigm to narrow the online civic space. Just the same way netizens are deploying technological tools and resources to stoke and amplify public fury, governments at all levels are equally capitalizing on the variety of the computerized spywares to accelerate the surveillance of civic actors operating and converging on online communities. Crackdowns on digital-fueled protests and the ensuing offline demonstrations are usually linked to national security concerns or the enforcement of health emergency measures, or premised on the rhetoric of anti-money (AML) laundering and countering financing of terrorism.

-LGBTQ activists and organizations

The location of the offices, safe houses—set up to protect marginalised persons fleeing dangerous situations—and staff of LGBT+ rights organizations have been tracked through social media posts. Consequently, certain LGBT+ rights activists have been harassed, subjected to mob attacks and their properties destroyed. Mere public association with persons who are perceived to be homosexual can lead to this form of harassment. One LGBT+ activist who runs an organisation for sexual and gender minorities in Nigeria's conservative northern region had his shop burnt to the ground.[149] LGBT+ rights organisations have also reported heightened surveillance of their members, including the use of fake emails, email monitoring, website attacks, phishing attacks, and hacking into LGBT+ activists' social media accounts to bully and harass them online. Other tactics used include sending hate mails, posting hateful comments, reporting the posts made by activists to content moderators on social media even when unrelated to LGBTQI+ activism. The hacking and digital monitoring

One of the prominent voices of the ENDSARS movement, Eromosele Adene, was held without charge for over 72 hours. Mr. Adene posted live updates on Twitter as security forces swooped in and arrested him in his Lagos family home. Police found him by tracking Mr. Adene's phone number, which had been displayed on the flyers calling for a renewed protest.

149 Interview with LGBTQ activist, September 1, 2021.

activities are arbitrarily carried out by homophobic individuals and groups including state actors who oppose the promotion of LGBT+ rights in Nigeria and seek to silence and reduce the spread of LGBT activism.

Although homophobic-induced surveillance is not framed around the objective of counterterrorism, it poses credible threat to LGBTQI+ movement and mobilization in Nigeria which mostly rely on the anonymity of social media to conduct their advocacy. But the story is changing rapidly with the combined effect of draconian homophobic legislation and restrictions on social media usage. Social media mobilization is likely to come under more scrutiny in Nigeria with the recent approval of N4,870,350,000 allocation to the National Intelligence Agency to monitor WhatsApp messages, text messages and phone calls. While the government claims that this action is to protect Nigerians from cybercrime and terrorism, the timing of the event which is just few weeks after the banning of Twitter in the country makes it suspicious.[150] Attacks on LGBT+ activists in Nigeria have grown more audacious with the passage of the Same-Sex Marriage (Prohibition) Act 2013, (SSMPA).

Women: female activists, bloggers and campaigners

Cyberbullying and slut-shaming women active on social media is commonplace across Nigeria. An interwiewee, Tawakalit Kareem from Lagos, narrated:

"A young man called me Ashawo - prostitute - on Twitter because I condemned the imposition of separate punishments for boys and girls for the same offences."

Likewise, the courageous activism of Nigeria's foremost activist from the religious conservative northern region of Nigeria, Aisha Yesufu, has continued to attract a barrage of degrading insults especially from the men in her region who believe that Muslim women should only be seen and not heard. During the October 2020 #EndSARS protests against police brutality, Ayisha Yesufu's vociferous campaigns for good governance and social justice earned her the description of a 'bad Muslim' by

150 Iroanusi, Q. (2021, July 12). Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls. Premium Times Nigeria. https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

online trolls. In one tweet, a Muslim man marked her picture in red X, condemning her un-Islamic activism. He wrote on the photo: "Don't be deceived by the hijab-wearing revolutionary. Islam is free from her actions." In another post on Facebook, another troll called her a 'mad whore".

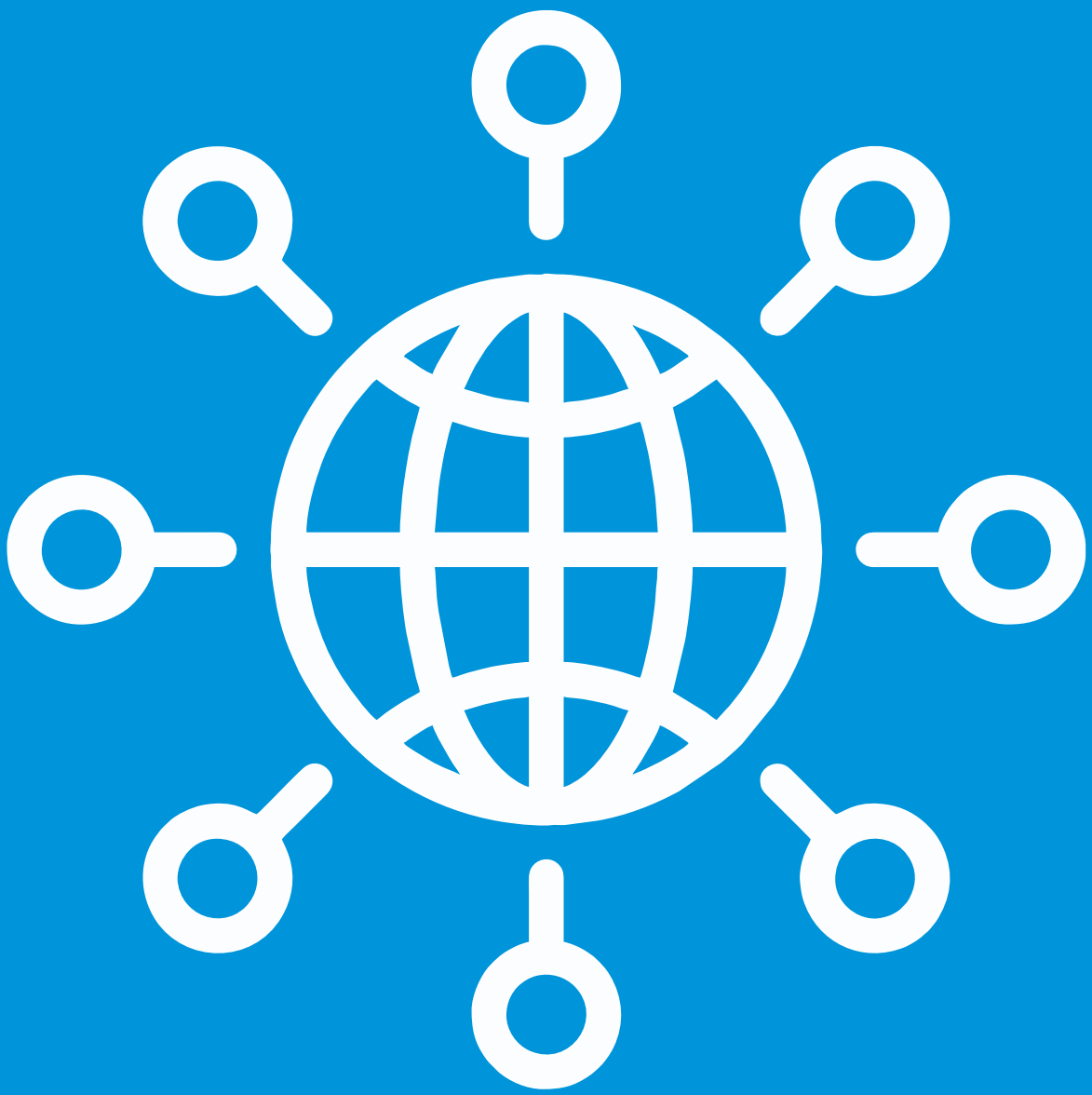
Women and young girls are singled out for slut-shaming on account of their civic activism. Slut-shaming women into silence and tagging them as 'prostitutes' both online and offline is widespread in Nigeria, but female activists remain undeterred. Sarbyen Sheni, from Plateau State, stated: "I use my social media to speak about child marriage, call out and expose injustices against women. I have been harassed but insult doesn't kill anybody." Others have reported sexual harassment, catcalling and a lot of negative comments especially from men. Turning off the Facebook or Twitter notifications is another popular coping mechanism for women determined to keep on using the social media to promote feminism and gender equality.

-Persons with Disabilities

Persons with disabilities now add to the list of civic actors targeted fiercely for their online and offline social justice campaigns in Nigeria. The arrest of Samuel Gabriel Iwatonaiye, a blind saxophonist, dominated news headlines and shocked the Nigerian civil society community in July. He was among the five human rights activists who wore the #BuhariMustGo T-Shirts to the Dunamis International Gospel Centre (Glory Dome), Abuja, arrested and handed over to the Department of State Services (DSS) operatives. Samuel's ill-health in custody was not enough for the state to release until a Federal High Court in Abuja ordered the release of the five activists in late July. Majority of PWDs are sedentary and leverage on social media to speak out, maintain online visibility and interact with a global audience. Consequently, they feel disproportionately impacted by the Twitter ban, and feel cut off from the social media community where they get news and access a lot of vital care and resources for enhancing their social and economic mobility.

CONCLUSION

That state agents use spyware against protesters and the opposition is no longer in doubt. This chapter identified the public and private actors behind the influx of sophisticated spywares and hacking technologies in the country, used to collect information against political opponents, and arbitrarily surveil and intercept communications. In short, what we have done is to provide a detailed account to date of the specific companies supplying surveillance technologies to the Nigerian state for repressing fundamental human rights, highlighting the buyers and beneficiaries of these importation contracts. When the dots between the repressive laws that enable abuses are connected to the mode of contracts awards for the importation of surveillance technologies and down to how these technologies are actually exploited to stifle dissent, all of these point in one direction: the government's promotion of an "authoritarian agenda."



CHAPTER 5

TRANSNATIONAL DRIVERS OF DIGITAL REPRESSION

© *The Guardian Nigeria*

This chapter explores the connections between the international norms on counterterrorism and the surveillance practices and abuses in Nigeria. It examines the role FATF and other international conventions play in normalizing surveillance for counterterrorism purposes, providing evidence of how well-intentioned international norms and laws generate unintended consequences in national contexts. It goes further to unpack how legal standards set by international security organizations like the Financial Action Task Force has specifically generated certain harms. It concludes by extending the searchlight to other transnational drivers that are contributing to digital repression in Nigeria.

It is necessary to scope the entities that are responsible for the formulation of the international rules on terrorism for a good understanding of how their enforcement techniques have influenced Nigerian laws and institutions on terrorism. The international institution whose resolutions are legally binding on countries is the United Nations Security Council.[151] However, since September 11, 2001, there has been a proliferation of new institutions, many with selective memberships whose regulatory scope is increasing and expanding and whose standards (usually in the form of "soft law")[152] are often binding on other states and crystallise into hard law.[153] One such international body whose soft laws on counterterrorism (CT) have strong binding effects on states is the Financial Action Task For (FATF).

151 In addition to the UNSC resolutions, countries are bound by CT treaties which they have signed

152 Fionnuala Ní Aoláin "Promotion and protection of human rights and fundamental freedoms while countering terrorism". Available at https://undocs.org/A/74/335, accessed 26 September 2021. "Soft law" has been defined as those international norms, principles and procedures that are outside the formal sources applied by the International Court of Justice and lack the requisite degree of normative content to create enforceable rights and obligations but are still able to produce certain legal effects. Ibid.

153 Fionnuala Ní Aoláin , Ibid

The FATF (also known as Groupe d'Action Financière (GAFI)) is an international task force of governments that was formed in 1989 following the G7 Summit in Paris in response to the mounting concern over money laundering across the globe.[154] Taken together, FATF's 40+9 recommendations and compliance mechanism amount to a comprehensive set of anti-money laundering and counter-terrorist recommendations. Membership of FATF is selective, and the core of its membership are 30-something of the world's most powerful economies. Non-members of the FATF may, however, join FATF-styled regional bodies (FSRBs) but do not by the virtue of that fact participate in the formulation of FATF standards.

5.1. FATF's Specific Statements and Recommendations on Surveillance

FATF: The Financial Action Task Force (FATF) and the regional body for West Africa, Intergovernmental Action Group Against Money Laundering (GIABA) strongly recommend surveillance by countries as part of their customer due diligence obligations and as tools for tracing and curbing the financing of terrorism. FATF Recommendations require countries, financial institutions and designated non-financial institutions (DNFIs) to collect information about customers and to report suspicious transactions to a government regulator – the financial intelligence unit. FATF Recommendation 10 requires that each country may determine how it imposes specific customer due diligence (CDD) obligations, either through law or enforceable means. As a result of this, governments have gone beyond to require information which do not have bearing with the regulated transaction.

More specifically, Nigeria's bank verification number (BVN), programme exemplifies the country's effort to comply with FATF's Recommendation 10, which makes BVN a compulsory requirement to open and operate bank accounts. According to a press release by GIABA in respect of the 28th GIABA Technical Commission/Plenary Meeting held in Nigeria in 2017, GIABA's Director-General supported Nigeria's plan to freeze "all bank accounts that have not complied with the enhanced Customer Due Diligence (CDD) of registering with the BVN hindering them from carrying out transactions on all banking platforms." When the requirement for CDD is joined to Recommendation 8 discussed above, it becomes clear why citizens, including non-profit organizations (NPOs) have been subjected to aggressive financial surveillance initiatives. Despite the revision of Recommendation 8 few years ago, GIABA specifically singles out NPOs for rigorous surveillance". According to GIABA's Assessment of Counter Terrorist Financing Capacities in West Africa (Burkina Faso, Cote D'ivoire, Mali, Niger, and Nigeria), "the lack of rigorous supervision and surveillance of activities, including the funding of several NPOs in these countries, constitutes further risks of TF.[155] [156]

154 Spaces for Change "Closing Spaces for Democratic Engagement and Civil Society in Nigeria". Available at https://spacesforchange.org/wp-content/uploads/2017/06/Beyond-FATF.-Trends-Risks-and-Restrictive-Regulation-of-Non-Profit-Organisations-in-Nigeria.pdf, accessed 26 September 2021, pp. 22-23.

155 GIABA - Press Release -

156 1132_ENG-Assessment of the CFT Capacities in GIABA MS.pdf p. 53

Although FATF has lately adopted conciliatory positions to recognise and acknowledge certain "unintended consequences" of its Recommendations (including cautionary provisions in its Guidance Notes on Digital Identity), the reality is that it is practically impossible to comply with FATF Recommendations, as well as state obligations under the relevant UNSC resolutions without conducting surveillance over citizens. For example, FATF Recommendation 1 which requires that countries conduct risk assessments cannot conceivably be complied with if a country does not monitor citizen activities. Similarly, FATF Recommendation 29 (Financial Intelligence Units) requires that:

> Countries should establish a financial intelligence unit (FIU) that serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and terrorist financing, and for the dissemination of the results of that analysis. The FIU should be able to obtain additional information from reporting entities, and should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.

Due to the activism of NPOs including Spaces for Change on this issue, other major international CT norm-forming organisations such as the Egmont Group[157] and the FATF[158] are beginning to recognise how their standards and recommendations are either being misused or misapplied at the national level to limit civil society. FATF recently launched a workstream on unintended consequences resulting from the incorrect implementation of the its standards including the dispositions of countries to use such standards to unduly target NPOs through non-implementation of FATF's risk-based approach; and the curtailment of human rights.[159]

5.2. UNSC Resolutions on Surveillance

UNSC resolutions empower states to conduct physical surveillance on persons. For example, Nigeria can justify its surveillance programme on the basis of Resolution2(c) of UNSC Resolution 1373 which mandates states to "take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information."The monitoring of communication channels of citizens, including wiretaps, social media surveillance, and mail interceptions by governments can be justified by states under resolution 3(a) of the same UNSC which calls on states to "find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist group."

No doubt, these provisions by UNSC and FATF are intended to curb terrorist activities, but they have given governments the impetus to hide under the guise of compliance to divert efforts towards attacking individual freedoms. Both FATF and UNSC recognise the dangerous effects of

157 The Egmont Group "EG Chair's Statement on Allegations of FIUs Misusing Their Powers to Combat ML and TF." Available at https://egmontgroup.org/en/content/egmont-group-chair%E2%80%99s-statement, accessed 26 September 2021

158 FATF "Mitigating the Unintended Consequences of the FATF Standards." Available at https://www.fatf-gafi.org/publications/financialinclusionandnpoissues/documents/unintended-consequences-project.html, accessed 26 September 2021

159 Ibid.

their requirements on civic freedoms. In the FATF Guidance Note on Digital ID such as BVN, FATF mandated that "digital ID systems must be underpinned by policies, laws and regulations that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability"[160] and recommended that states make laws and regulations on data protection and privacy which should also include oversight from an independent oversight body (e.g. a national privacy commission) with appropriate powers to protect subjects against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or legitimate purpose.

In sharp contrast to the UNSC's recommendations, the bulk of existing laws that expand access to information and digital technologies are cast in a regulatory mould rather than as a medium to preserve human data and digital rights. The Nigerian Data Protection Regulation (NDPR), touted as the country's glowing policy elixir for data privacy, has been bugged by low compliance. Improved compliance with NDPR will not only consolidate the constitutional guarantees of privacy, but also bolster confidentiality and responsible use of personal data. More tellingly, an independent judiciary is indispensable in an era of unrelenting physical and digital attacks in order to tame executive and legislative arbitrariness, criminalize and punish intrusive surveillance and fairly arbitrate in the event of collision between people power with the state's hegemonic power.

5.3.Influence of International CT Norms on the Nigerian civic space

For the most part, international CT standards pay lip service to the tenets of human rights. Mere reference to, and the use of standard phrases like "in compliance with international law,[161] including human rights, humanitarian and refugee law" do not translate into any positive obligation for states. The FATF Recommendations contain only three mentions of human rights in the Interpretative Notes which are all framed along the lines of the afore-referenced phrase.[162] Security Council resolutions regulating CT and prevention and countering of violent extremism are all characterized by lack of or insufficient engagement with civil society actors regarding the legal, political, social and cultural impacts of such resolutions; so much that the first resolution to contain a reference to civil society in its operative part is Resolution 2178 of 2014.[163]

The absence of prescriptive standards on upholding human rights while countering terrorism is not the only human rights concern with international CT standards. A study of the FATF Recommendations (now updated in 2021) reveals subtle provisions urging governments to take steps which would inevitably translate to infringement of rights. An infamous example is the initial language of Recommendation 8 which stated that "NPOs possess characteristics that make them particularly attractive to terrorists or vulnerable to misuse for terrorist financing" and called on countries to "review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism." Although Recommendation 8 has been rephrased,[164] Section 35 of the Terrorism Prohibition Act (TPA) is a clear footprint of Recommendation 8 within the Nigerian legal system. The TPA allows the government agency responsible for registration of organisations to refuse to register, or to deregister any charity

160 Page 89
Ibid., p. 9
161 It could be argued that since it is not a human rights document, it needs only reference existing obligations. However, this
162 argument would miss the point. The onus is on a person who is prescribing standards with potential effects on human rights to take initiatives for the preservation of human rights while complying with the standards.
163 Fionnuala Ní Aoláin "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders." Available at https://undocs.org/pdf?symbol=en/A/HRC/40/52, accessed 26 September 2021, p. 6
164 The current iteration of Recommendation 8 prescribes a risk-based approach of regulating NPOs requiring states to assess the TF risks to which NPOs are exposed and then apply commensurate measures aimed at countering the identified risks.

"based on security or criminal intelligence reports, where there are reasonable grounds to believe that an applicant for registration as a registered charity has made, is making or is likely to make available any resources, directly or indirectly, to a terrorist group".[165] In keeping with FATF's elevation of security over human rights (in this case the presumption of innocence), the TPA places the obligation on the charity to file an action in court to reverse the decision within 60 days after which the charity is foreclosed from challenging the decision. Glaringly, charities were the only organisations singled out for this kind of measures in the TPA. This provision has already been wielded by the government.

The international CT narrative has also provided security agencies like the State Security Services (SSS) with undefined powers to proceed against citizens even where there is no perceivable act of terrorism or security threats. In absence of definitional certainty regarding what constitutes terrorism, states are enabled to flexibly determine what falls within the purview of countering or preventing terrorism and violent extremism. As evidence in numerous chapters demonstrate, this permission is often overstretched to include virtually anything so designated as terrorism by state agents. This has two implications: first, it makes an objective delimitation of the state's security powers more difficult. Secondly, it expands the list of persons that can be harassed by state agents under the guise of national security. The endless list of targets and the consequences of overbearing governmental power have already been detailed above.

The Office of the National Security Adviser (ONSA) and the agencies within that office, particularly the State Security Service (SSS), are powerful tools within the control of the Presidency. In its position as the implementer of CT initiatives within Nigeria, the SSS has taken drastic actions against or affecting the civic space under the guise of CT. Now also known as the Department of State Services (DSS),[166] the agency has in time past been associated with repressive actions in the name of national security during the military era but has continued in this culture during the present civilian dispensation armed with Section 45 of the Constitution and its role as the CT centre for Nigeria. Examples of the brazen tactics popularly used by the SSS to enforce crackdowns in the name of counterterrorism include:

a. arrests (including pre-emptive arrests) of opposition figures and ordinary citizens even for comments made on social media on grounds ranging from inciting of statements, cyberstalking, sedition;
b. categorizing emancipation movements within the country as terrorism and violent extremism and treating members of such movements as extremists and terrorists;
c. invitation of persons including journalists for questioning[167]; and
d. prosecuting citizens on charges of terrorism and acts of violence.
e. Sending messages to citizens charged with threatening undertones.

165 Section 35(1) of TPA

166 See Premium Times "FACT-CHECK: How Nigeria's secret police, SSS, is violating the law and illegally parading itself as DSS." Available at https://www.premiumtimesng.com/investigationspecial-reports/209343-fact-check-nigerias-secret-police-sss-violating-law-illegally-parading-dss.html, accessed 26 September 2021

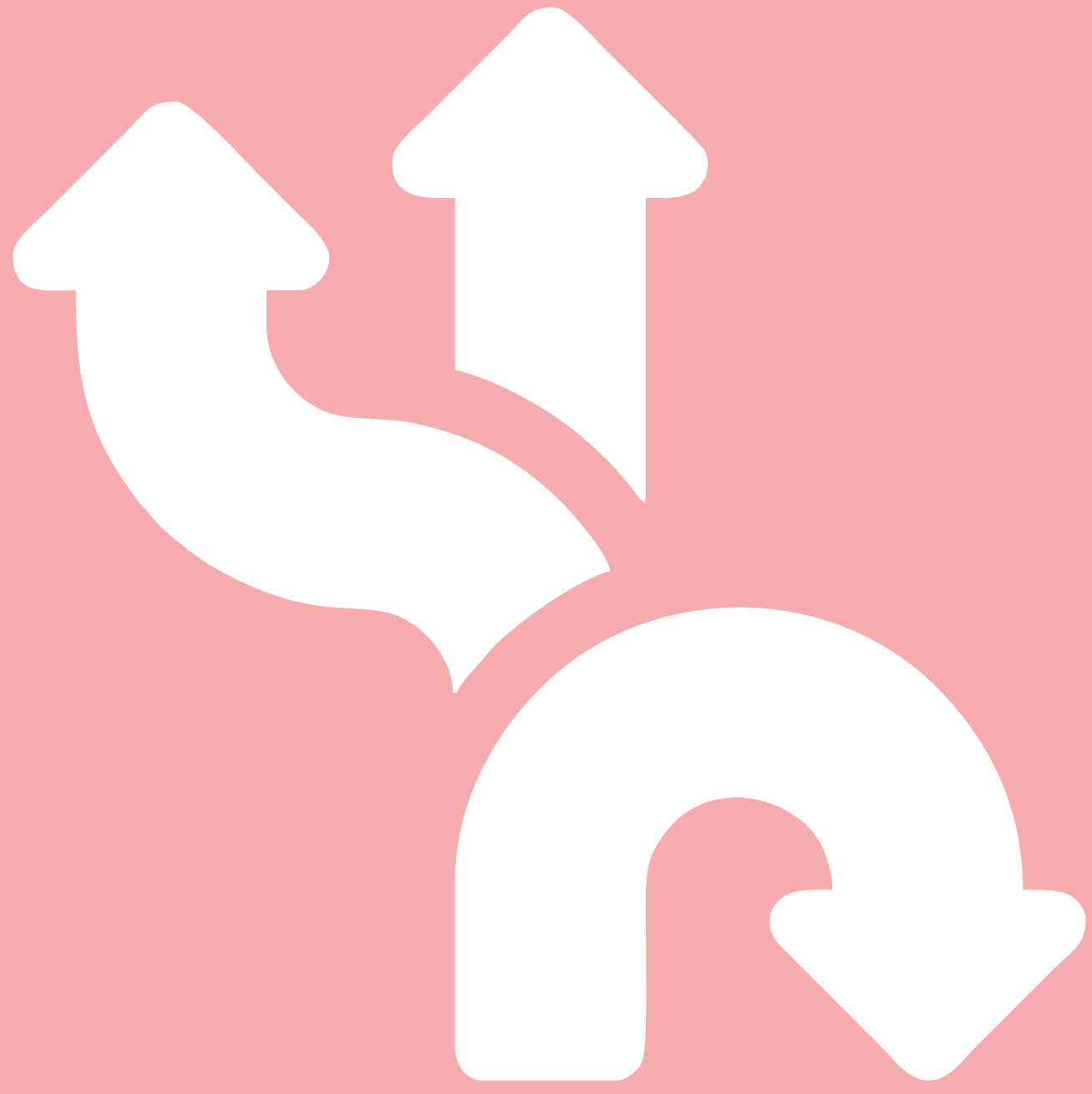
167 For example, the SSS recently invited anchors of Channels TV for questioning over an interview during which their host made statements critical of the government. See Vanguard "DSS grilled Channels TV anchors for hours, asked them to sign undertaking." Available at https://www.vanguardngr.com/2021/08/dss-grills-channels-tv-anchors-for-hours-releases-them/, accessed 26 September 2021

Apart from the numerous incidents of clampdowns, the invocation of international CT norms to rationalise recurrent attempts to introduce restrictive regulations for NPOs is well-documented. It is still not clear why NPOs, a diverse sector both in terms of number, type, structure, and complexity could be bundled together and categorised as vulnerable to terrorist abuse. This error needs to be corrected as the mere revision of Recommendation 8 has proven to be insufficient. Compared to all other sectors of the Nigerian economy, there is hardly any characteristic of NPOs that makes them inherently vulnerable for abuse over and above other kinds of organisations requiring targeted regulation.[168] It appears that FATF's Recommendation 8 primarily targets certain kinds of NPOs particularly operating in high-risk zones, whose objectives include receiving and distributing donated resources. The broad scope of Recommendation 8 has provided states the legal impetus to extend the application of international CT norms to groups outside the purview of FATF Standards such that NPOs engaging the government on politics, transparency and rights activism often get caught in the web of onerous CT measures.

CONCLUSION

Countering terrorism has increasingly become an omnibus shield for covering up numerous atrocities and illegalities perpetrated by the state against its citizens. Under the pretext of countering terrorism and insecurity, governments at the state and federal levels have procured and amassed surveillance technologies and hacking tools to monitor the movements, financial transactions, internet activities and phone conversations of people they consider opposition or activists. Other ulterior motives for the heightened surveillance initiatives include election manipulation, spying and clampdown on a variety of civic actors demanding accountability and asking uncomfortable questions. Critics, especially those operating online, have borne the brunt of these surveillance initiatives and the ensuing repression. The uniformity of the tactics deployed from state to state, and by the central government, reinforces fears that state authorities are copying from an unscrupulous playbook of repression disguised as security. Particularly undergirding this inference is the huge disconnect between mere critical commentary on social media and the terrorism charges characteristically slammed on the authors. Overstretching existing laws in a manner that casts the net so wide to catch all possible offenders of serious and not-so-serious misdemeanours further substantiates the claims of abuse of the legal system or the manipulation of the judicial system to silence voices of dissent.

168 Spaces for Change "Unpacking the Official Construction of Risks and Vulnerabilities for the Third Sector in Nigeria. " Available at https://spacesforchange.org/wp-content/uploads/2019/03/FULL-REPORT.-UNPACKING-THE-OFFICIAL-CONSTRUCTION-OF-RISKS-AND-VULNERABILITIES-FOR-THE-THIRD-SECTOR-IN-NIGERIA_compressed.pdf, accessed 26 September 2021, pp. 43-49



CHAPTER SIX

ROADMAP FOR CHANGE

© *Nairametrics*

What are the ways to counter the government's repressive agenda and the underlying motivations for enhancing its authoritarian mindset? What legal fixes need to be made in order to push back against directives that enhance digital repression? Are there opportunities for reforming, disrupting the influence of international counterterrorism norms at the national, regional and international levels? How can civil society advocates and organizations leverage on existing mechanisms or create new ones to push back against digital repression?

The opportunities to disrupt, to reform and, over long-term, transform the misuse of technology to suppress dissent hinge on a holistic five-pronged approach involving different stakeholders and calibrated to strike a balance between the competing agendas of the government, the private sector, civil society, and the media. This approach not only requires tackling the structural vulnerabilities that are unduly exploited in the data access policies, practice, and procedures governing the data protection and surveillance ecosystem, but also encompasses dismantling the constraints limiting the full implementation of these regimes. Some of these constraints manifest in the form of cracks in the monitoring and enforcement of data protection laws, inadequate checks and balances on government/corporate surveillance activities and non-adherence to data-specific data protection regulations. This section suggests five major actors that can take bolder action to keep surveillance programmes on track.

6.1. The Government: What the Government Can Do

Regulation, Legislation and Sanction: A plethora of legal provisions dispersed in a maze of legal and policy frameworks empowers regulatory bodies—such as National Identity Management Commission (NIMC), National Information Technology Development Agency (NITDA), Federal Ministry of Communications and Digital Economy (FMoCDE), Nigerian Communications Commission (NCC)—to use regulation, legislation and sanction to exercise oversight over surveillance operations in Nigeria. For instance, the Implementation Framework of the Nigeria Data Protection Regulation (NDPR) Act issued in January 2019 sets out guidelines for data subjects, private businesses and government agencies. The NITDA is empowered to ensure compliance with these guidelines. Scaling up compliance is one way the government can make regulated entities, corporate bodies and security agents take information security and data privacy very seriously.

The Nigerian Data Protection Regulation (NDPR) imports the sentiments codified in the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014 and European Union General Data Protection Regulation (EU GDPR). Not only that, the NDPR has been subordinated to these international protocols especially "where the NDPR and this Framework do not provide for a data protection principle or process." That means that law enforcement agents will recourse to these international protocols where there is a lacuna is the national legal framework. To match words with action, strengthening enforcement mechanisms are necessary to ensure corporations, state departments and security agents put in place adequate controls for accessing biometric databases and for safely transmitting personal and sensitive data across networks.

More tellingly, the term, national security is undefined, vague and broad hence the need to clearly define and specify legitimate circumstances that may warrant a breach of data protection laws. Legislative clarity on the definition of terrorism is more effective when it is backed by a judicial review or repeal of the numerous legal provisions empowering agents of the executive arm of the government to surveil, "without warrant" or court order. The reviews are necessary to tame arbitrary official behaviour by importing strong safeguards and stringent data privacy processes. Abuse of surveillance technologies also thrives in an atmosphere of inadequate or weak sanctions regimes that can help to deter abuse. For instance, the consequence for blocking peaceful protesters' bank accounts should transcend unblocking or unfreezing the accounts, but also, deterrence measures and sanctions on responsible agencies.

Import and Export Controls: With national security and foreign policy considerations in mind, Nigeria can use import controls as a strategy to limit the influx of sophisticated spyware technologies into the country. Nigeria already enforces import controls on several contraband goods detailed in the import prohibition list such as frozen poultry, pork/beef, sugar, noodles, bagged cement, rice etc.—to prevent the penetration and domination of foreign commodities that are sufficiently produced locally. Adding surveillance and hacking technologies to the list of contraband goods will not only ensure that adequate controls undergird imports, but also push back on powerful countries invested in protecting the commercial interests of their indigenous businesses abroad irrespective of certain ethical shortcomings.

Governments can also use legislative measures to achieve the ends of import controls. Current laws governing the digital spaces mainly concern themselves with the application and use of technology. It might be more effective to cut off uncontrolled supply by criminalising the buying and selling of invasive technologies. That way, powerful business interests in the multi-billion-dollar market, mostly of United States, China and Israeli origins, will be subjected to the impulses of legislation or regulation.

Nigeria can borrow best practices from the United States of America's Commerce Department which issued a new set of rules imposing export controls on items used in surveillance of private citizens and other malicious cyber activities. The rules aim to check the misuse of technology to abuse human rights or conduct other malicious cyber-attacks, and ensure that U.S. companies are not fueling authoritarian practices.[169] The rule titled, information security control,[170] came into effect in January 2021, and is targeted at exports of spywares like Pegasus which had earlier been reported in December 2020 to be used by countries like Nigeria to spy on its citizens.[171]

In 2017, the British government sanctioned the sale of spy equipment capable of intercepting, tracking, and monitoring emails, mobile phones, and messaging services like WhatsApp – to Honduras, shortly before a recently disputed election.[172] Israel set up a commission to review allegations that NSO Group's Pegasus spyware was misused by its customers to target journalists and human rights activists will examine whether rules on Israel's export of cyberweapons such as Pegasus should be tightened.[173] All these are examples of how other governments are using import and export controls, including sanctioning regimes to promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies.

6.2. How the Private Sector can Help

Consistent with Art. 2.6; 4.1(3) NDPR 2019, increased commitment to sensitization, capacity-building and awareness-creation can act as strong springboards for enhancing compliance with applicable data protection laws especially from corporations. Areas where capacity-building investments are critical include the Audit Template for NDPR Compliance' and the 'Sample Privacy Policy Template', provided in NITDA's Implementation Framework document, which clarify and demand transparency in the use of cookies, data processing and the guarantees for consumer data protection. Also, penalties must be attached to unethical practices, such as the Cambridge Analytica case, where artificial intelligence and invasive cookies plugged into people's data interpret people's personal preferences and political leanings.

Businesses already have obligations to protect human rights under international law. The Guiding Principles on Business and Human Rights[174] drafted by the UN Secretary-General's Special Representative for Business and Human Rights, John Ruggie places a responsibility on businesses to respect human rights and provide access to remedies. Article 12 requires businesses to also "respect the human rights of individuals belonging to specific groups or populations that require particular attention, where they may have adverse human rights

170 Federal Register, Information Security Controls: Cybersecurity Items, https://www.federalregister.gov/documents/2021/10/21/2021-22774/information-security-controls-cybersecurity-items

171 Aljazeera, Nigerian intelligence bought tool to spy on citizens: Report, https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report

172 War Resisters International, British government sanctioned sale of spy equipment to Honduras, https://wri-irg.org/en/story/2018/british-government-sanctioned-sale-spy-equipment-honduras

173 The Guardian, Israel to examine whether spyware export rules should be tightened, https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus

174 Hereinafter GPs or Principles.

impacts on them." Businesses cannot effectively respect human rights and the rights of persons that may be disproportionately impacted by their operations unless they have certain data privacy policies and processes in place. Departing from the current trend of complying with regulations as a survival strategy, businesses can incorporate effective data-governance strategies into their corporate social responsibility policies and practices.

6.3. Civil Society and Citizen-based Initiatives

Active citizens are using their access to the internet to raise their voices against the ills in the society. Since the Twitter ban, Nigerians have massively and proactively downloaded anti-censorship software like VPNs in order to survive internet shutdowns and effectively evade censorship. These sorts of measures may be the most effective steps that Nigerians can take until more holistic legislative and normative changes occur.

Organized civil society organizations (CSOs) can lead reforms in three ways: Accountability, Advocacy, and Access. NGOs can demand accountability for non-compliance to NDPR data protection templates using existing accountability monitoring and ranking tools such as Surveillance/Data Privacy Index, Closing Spaces Database, Press Freedom Index, and so on. These mechanisms can be adapted or scaled up to monitor, incident and measure levels of infringements on digital rights, data privacy, and related civil liberties by state and non-state actors. Analysis of monthly/quarterly results provides CSOs with evidence needed to hold government agencies and security forces, Telcos, Financial Institutions, FinTechs and other key players in the digital and civic space to account.

NGOs can demand enforcement of the penalties on a non-compliant company - private and public. Furthermore, advocacy needs to focus on building capacity of diverse stakeholders and facilitating dialogue between them. Trainings are needed to deepen understanding of privacy rights and the enforcement of global best practices. In this regard, civil society-led advocacy has successfully influenced Facebook, Twitter, and WhatsApp to spot misinformation and sanction disinformation. As a result, content moderation platforms like WhatsApp have restricted the number of times one can share a message, and to flag a message as 'forwarded many times'. Also parody and anonymous manipulations have been exposed, while the use of Twitter and Facebook blue ticks can now be used to verify the original account of an influencer.

Pushing for legislative and judicial reviews of repressive laws is imperative. Statutes conferring overreaching powers on states to surveil and derogate from human rights include Section 45 of the 1999 Constitution, the Nigerian Communication Act 2003, Sections 4-9, the National Identity Management Commission Act 2007 (Section 26) and the Criminal Code Act 1995, especially sections 50-53 on sedition, and sections 373-376 on Defamation of Character etc. Legislative reviews are necessary to make national surveillance regimes compatible with international human rights norms and global best practices. As the success of the civil society-led pushback on the Social Media Bill demonstrates, legislative advocacy is critical, and is usually effective when preceded by evidence-backed advocacy. Groups like Social and Economic Rights Accountability Project (SERAP) have frequently approached local and regional courts to challenge legal provisions with restrictive contents.

CSOs can also leverage the ongoing constitutional review process to push for legislative amendments, especially the expansion of privacy rights in S. 37 as well as the state's derogation powers in S. 45. Above all, it is important for CSOs to include grassroots organizations in these advocacy initiatives to empower citizens across urban and rural divides to prepare themselves for the onslaught of digital repression.

6.4. The Media

Collaborations between media organizations and tech companies need to be fully explored to increase the preservation of the digital rights and tech spaces. Collaborations of this nature have enabled investigative platforms such as Africa Check and Premium Times Center for Investigative Journalism (PTCIJ) to emerge. Existing databases and ranking tools can be scaled up to democratize access to information, education, and communication (IEC) resources to promote best practices and deepening public understanding of digital rights protected under national and international legal frameworks. Examples of existing trackers include Closingspaces.org and the Press attack Tracker of the PTCIJ. These are tools used in monitoring violations, reporting incidents of clampdowns on the civic space, archiving evidence of inappropriate practices by state actors, and naming and shaming perpetrators.

The capacity of the media to better report digital rights violations, data protection mechanisms, data privacy concerns, and digital surveillance, needs further strengthening. Learning and open-source tools developed in collaboration with civic tech organisations are important tools that can bolster innovation, investigation, and capacity building in the media sector.

6.5. International organizations

Evidence from the outcomes of corporate accountability advocacy campaigns against the irresponsible activities of oil companies in Nigeria's Niger Delta region provides some inspiration for leveraging on the collaborations with international organizations and partners to push back on the state's abuse of the counterterrorism architecture and invasive technologies to stifle dissent. For instance, it has been notoriously difficult to hold powerful oil corporations operating in Nigeria accountable. Some of the successful settlements involving oil giants are usually negotiated outside the shores of Nigeria through collaborative campaigns between local and international organizations. As has been successfully done in a number of environmental justice litigation campaigns, they can initiate legal action on the parent companies supplying these technologies to Nigeria in the home states of the indicted transnational corporations. Nigerian suppliers mainly come from the United States and Israel.

International organizations can also support and amplify the advocacy by local organizations pushing for stronger legal regimes, stiffer sanctioning goals and penal arrangements designed to subdue the activities of suppliers of spying and hackware technologies.

BIBLIOGRAPHY

Abubakar Ahmadu Maishanu

· , Premium Times: Why we shut down telecommunications networks in Zamfara – Governor, September 6, 2021, Accessed via https://www.premiumtimesng.com/regional/nwest/483366-why-we-shut-down-telecommunications-networks-in-zamfara-governor.html\

· Action Group on Free Civic Space, #EndSARS: POLICE BRUTALITY, PROTESTS AND SHRINKING CIVIC SPACE IN NIGERIA, 2021, Accessed via https://closingspaces.org/endsars-police-brutality-protests-and-shrinking-civic-space-in-nigeria/

· Adejumo, K. Premiunm Times Nigeria (2020, January 16): Police Interrogate PREMIUM TIMES' Journalist Over Report Exposing Islamic Cleric Who Raped 16-Year-Old.https://www.premiumtimesng.com/news/more-news/372729-police-interrogate-premium-times-journalist-over-report-exposing-islamic-cleric-who-raped-16-year-old.html

· Adeyemi Adepetun, The Guardian: Despite security concerns, FG again extends NIN-SIM link deadline by three months, 26 July 2021; accessed via https://guardian.ng/news/despite-security-concerns-fg-again-extends-nin-sim-link-deadline-by-three-months/

· Alabi, Sodiq, Paradigm Initiative: (2017, November 17). President Buhari's Secret War on Free Speech. Paradigm Initiative. See https://paradigmhq.org/president-buharis-secret-war-on-free-speech/.

· Ameh Comrade Godwin, Daily Post :(2018, December 20). Journalist remanded in prison over report against Kebbi Government. Daily Post. https://dailypost.ng/2018/12/20/journalist-remanded-prison-report-kebbi-govt/

· Asadu Chinedu, The Cable (2018, March 13): The police on Tuesday arrested Abdullahi Krishi, House of Representatives correspondent of Daily Trust. TheCable. https://www.thecable.ng/just-police-arrest-daily-trust-reporter-national-assembly

· Bakare Majeed, Premium Times: Groups reject bill seeking to empower NBC to regulate DSTV, Startimes' tariffs, Accessed via https://www.premiumtimesng.com/news/top-news/468179-groups-reject-bill-seeking-to-empower-nbc-to-regulate-dstv-startimes-tariffs.html

· BBC News "Abba Kyari: The Nigerian super sleuth wanted in the US." Available at https://www.bbc.com/news/world-africa-58079504, accessed 26 September 2021

· Biometric Update, Nigeria's move to link digital identity numbers to SIM cards sparks lawsuit, February 2, 2021: Accessed via https://www.biometricupdate.com/202102/nigerias-move-to-link-digital-identity-numbers-to-sim-cards-sparks-lawsuit

Chinedu Asadu, The Cable Nigeria: DSS confirms raid on Igboho's house, declares him wanted, July 1, 2021; Accessed via https://www.thecable.ng/breaking-dss-launches-manhunt-for-sunday-igboho-after-recovering-arms-ammunition-from-his-house

· Emma Okonji This Day (December 16, 2020): "FG Directs SIM Card be Linked to National Identity Number" Accessed February 20. 2021 via https://www.thisdaylive.com/index.php/2020/12/16/fg-directs-sim-card-be-linked-to-national-identity-number/

· Emmanuel Paul, Techpoint, Hackers have access to data from Nigerian and Kenyan universities, June 1, 2020; Accessed via https://techpoint.africa/2020/06/01/nigerian-kenyan-universities-hacked/

· Emma Woolacott, Forbes: Ad Industry Accused of 'Massive' Privacy Breach, Accessed via https://www.forbes.com/sites/emmawoollacott/2019/01/28/ad-industry-accused-of-massive-privacy-breach/?sh=73c6bc076822

· Evelyn Okakwu, Premium Times, Buhari under fire for comment on rule of law, national security, August 28, 2021, https://www.premiumtimesng.com/news/headlines/281576-buhari-under-fire-for-comment-on-rule-of-law-national-security.html

· FATF "Mitigating the Unintended Consequences of the FATF Standards." Available at https://www.fatfgafi.org/publications/financialinclusionandnpoissues/documents/unintended-consequences-project.html , accessed 26 September 2021

· Federal Government of Nigeria gazette: (2019c). Lawful interception of communications regulations. 106(12), 105-118. Available at https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/839-lawful-interception-of-comunications-regulations-1/file

· Financial Nigeria, Nigeria risks lower score on biometric data practices, February 2021; Accessed via http://www.financialnigeria.com/nigeria-risks-lower-score-on-biometric-data-practices-feature-403.html

· Fionnuala Ní Aoláin "Promotion and protection of human rights and fundamental freedoms while countering terrorism". Available at https://undocs.org/A/74/335, accessed 26 September 2021, p. 3

· Fionnuala Ní Aoláin, United Nations: "Impact of measures to address terrorism and violent extremism on civic space and the rights of civil society actors and human rights defenders." Available at https://undocs.org/pdf?symbol=en/A/HRC/40/52 , accessed 26 September 2021, p. 6

· Foundation for Investigative Journalism, EXCLUSIVE: Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall (2021) Accessed via https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

GIABA press release- https://www.giaba.org/press/release.html

· China Aid Data: https://china.aiddata.org/projects/30450/

· CIVICUS, People Power Under Attack, December 2019: Please see https://civicus.contentfiles.net/media/assets/file/GlobalReport2019.pdf

· Closing Spaces Database: Tracking Civic Space Incidents in Nigeria: 2015-July, 2021 https://closingspaces.org/tracking-civic-space-incidents-in-nigeria-2015-july-2021/

· Closing Spaces Database: Businessman Jailed For Allegedly Calling Adamawa Governor 'Father Of All Thieves', Accessed via https://closingspaces.org/incident/businessman-jailed-for-allegedly-calling-adamawa-governor-father-of-all-thieves/

· Committee to Protect Journalists, (2016, May 23): Nigerian journalists detained for investigating alleged water theft. https://cpj.org/2016/05/nigerian-journalists-detained-for-investigating-wa/

· Committee to Protect Journalists: Nigerian journalist jailed for refusing to reveal source, August 2018, Accessed via https://cpj.org/2018/08/nigerian-journalist-jailed-for-refusing-to-reveal/

· Comparitech, Biometric data: 96 countries ranked by how they're collecting it and what they're doing with it, January 2021, https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/

· Counter-Terrorism Centre Strategic Report 2018: Available at https://ctc.gov.ng/wp-content/uploads/2020/03/REVIEW-OF-ACT-Inner-2019.pdf, accessed 26 September 2021

· Ebuzor, C. Premium Times: (2018, August 14). Premium Times journalist detained over a story. Pulse Nigeria. Accessed via https://www.pulse.ng/news/local/samuel-ogundipe-premium-times-journalist-detained-over-a-story/xbesbp0

· Editor, Premium Times: Kaduna to shut down telcos over insecurity, 29th September 2021, Accessed via https://guardian.ng/news/kaduna-to-shut-down-telcos-over-insecurity/

· Editor, The Guardian (2021, January 26): Clampdown on Peoples Gazette as telcos block access to news website. The Guardian. https://guardian.ng/news/clampdown-on-peoples-gazette-as-telcos-block-access-to-news-website/

Emmanuel Elebeke, Vanguard News: Disconnect all SIMS not connected to NIN by Dec 30, FG orders telcos (December 15, 2020) Accessed via https://www.vanguardngr.com/2020/12/fg-orders-telcos-to-disconnect-all-sims-not-connected-to-nin-by-dec-30/

· Henry Ojelu, Vangaurd: Lawyers divided over superiority of FOI to Official Secret Act, September 6, 2018, https://www.vanguardngr.com/2018/09/lawyers-divided-over-superiority-of-foi-to-official-secret-act/

· Idris Uwaisu, DW.COM, street Debate: how How #ArewaMeToo shed light on sexual abuse in Nigeria, published 07.10.2019: https://www.dw.com/en/street-debate-how-arewametoo-shed-light-on-sexual-abuse-in-nigeria/a-50705429

· Ihuoma Alo, HumAngle: 1,031 Killed, 390 Abducted In 205 Incidents Across 34 States In Nigeria – Report; https://humanglemedia.com/1031-killed-390-abducted-in-205-incidents-across-34-states-in-nigeria-report/

· John Charles, Punch Nigeria: (2018, March 13). Presidency bars PUNCH, others from covering Buhari's Benue, https://punchng.com/presidency-bars-punch-others-from-covering-buharis-benue-visit/

· Jonathan Rozen, Committee to Protect Journalists, How Nigeria's police used telecom surveillance to lure and arrest journalists

· Jonathan Rozen, Committee to Protect Journalists, Nigerian Milsitary Targeted Journalists' Phones, Computers With "Forensic Search" for Sources, October 22, 2019; Accessed via https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/

· Larry Madowo, BBC, Is Facebook undermining democracy in Africa? (2019) https://www.bbc.com/news/world-africa-48349671

· Marczak, B. Scott-Railton, J. Rao, S. Anstis, S. Deibert, R. (2020, December 1). Running in circles: Uncovering the Clients of cyberespionage firm circles. The Citizen Lab. https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

· Mathew T.Page, Fake Civil Society: The Rise of Pro-Government NGOs in Nigeria, Carnegie Endowment for International Peace, (2021) Accessed via https://carnegieendowment.org/2021/07/28/fake-civil-society-rise-of-pro-government-ngos-in-nigeria-pub-85041

· Masari, The Cable: Over 150 groups of bandits operate in the forests, September 21, 2021, Accessed via https://www.thecable.ng/there-are-over-150-groups-of-bandits-in-the-forests-says-masari

· Media Rights Agenda(MRA). (2005, July 29): Airport security officers prevent newspaper editor from travelling. Ifex. https://ifex.org/airport-security-officers-prevent-newspaper-editor-from-travelling/.

· Media Rights Agenda (MRA). Nigeria: armed men attack TV crew, vandalise vehicles and broadcast equipment. IFEX. https://ifex.org/nigeria-armed-men-attack-tv-crew-vandalise-vehicles-and-broadcast-equipment/

· Nairametrics "#EndSARS: CBN says funds in frozen accounts may be linked to terrorist activities." Available at https://nairametrics.com/2020/11/11/endsars-cbn-says-funds-in-frozen-accounts-may-be-linked-to-terrorist-activities/, accessed 26 September 2021

· National Communication Commission: Guidelines for the provision of internet service. https://www.ncc.gov.ng/accessible/documents/62-guidelines-for-the-provision-of-internet-service/file

· News24. (2017, September 23): Nigerian journalist detained over report on flood camp protest.
· News24. https://www.news24.com/news24/Africa/News/nigerian-journalist-detained-over-report-on-flood-camp-protest-20170923

· Nigerian Communications Commission: Challenges of Technology Penetration in an Infrastructure Deficit Economy (Nigeria Perspective), 2021: Accessed via https://www.ncc.gov.ng/documents/976-challenges-of-technology-penetration-in-an-infrastructure-deficit-economy-nigeria-perspective/file

· Nigerian Communications Commission Statistics and Reports (Industry Statistics): 2021 (ibid). See https://www.ncc.gov.ng/statistics-reports/industry-overview#gsm-2

· Nigeria Governors' Forum, Governors: MTN partner to use data to halt spread of COVID-19, https://nggovernorsforum.org/index.php/homepage/73-featured-news/1564-governors-mtn-partner-to-use-data-to-halt-spread-of-covid-19

· Nimi Prinewill, Peoples gazettent (2021, January 30): AUDIO: Governor Umahi threatens to kill Peoples Gazette reporters over Ebonyi corruption story. Peoples Gazette. https://gazettengr.com/audio-governor-umahi-threatens-to-kill-peoples-gazette-reporters-over-ebonyi-corruption-story/?utm_source=ReviveOldPost&utm_medium=social&utm_campaign=ReviveOldPost

· NITDA amendment Bill: https://drive.google.com/file/d/1fOTMidYbICS10aIwWpjdDdgyCBhGUNM7/view

Nkanga, P. (2018, July 1). (2018, July 1). SPECIAL REPORT: How Buhari's govt detained Nigerian journalist for two years without trial. Premium Times. https://www.premiumtimesng.com/news/headlines/274467-special-report-how-buharis-govt-detained-nigerian-journalist-for-two-years-without-trial.html

· Ogala, E. Premium Times (2015, April 5): How PREMIUM TIMES survived massive cyber attacks during presidential election coverage. Premium Times. https://docs.google.com/document/d/11CrFKOiRnsOAIuTDkFuJT9lOekFOnbR_Nj1LrhqaRW0/edit

· Ojoye Taiwo, Punch Nigeria (2019, January 8): Military invasion of Daily Trust, indefensible. Punch; https://punchng.com/military-invasion-of-daily-trust-indefensible/

· Olugbenga Adanikin, ICIR, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy, February 2019, 2019 Election: How APC may have benefited from NCC, INEC breach of voters' privacy - International Centre for Investigative Reporting (icirnigeria.org)

· Oluwakemi Adelagun, Premium Times:Police disperse Yoruba nation agitators; July 3, 2021, Accessed via www.premiumtimesng.com/regional/ssouth-west/471408-police-disperse--yoruba-nation-agitators.html.
· accessed 27 July, 2021

· Oluwafemi Osho and Solomon A. Adepoju, Cybercafés in Nigeria: Curse to the Internet?(2016)Accessed via http://ceur-ws.org/Vol-1830/Paper84.pdf

· Privacy International, Biometrics Collection Under the Pretext of Counter-Terrorism, 2021: Accessed via https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism

· Premium times of Nigeria, National Commission for the Prohibition of Hate Speeches Bill 2019: https://media.premiumtimesng.com/wp-content/files/2019/11/ational-Commission-of-Prohibition-of-Hate-Speeches-Bill-2019-1.pdf

· Premium Times. (2022, October 26). #EndSARS: SERAP fumes as NBC fines Channels, AIT, Arise TV. Premium Times. https://www.premiumtimesng.com/news/more-news/423160-endsars-serap-fumes-as-nbc-fines-channels-ait-arise-tv.html

· Premium Times. (2016, October 21). Kaduna to spend N2.55 billion on drones, surveillance equipment in 2017. Premium Times, Available at https://www.premiumtimesng.com/regional/nwest/213304-kaduna-spend-n2-55-billion-drones-surveillance-equipment-2017.html

· Ode Uduu and Charles Mba, Dataphyte, Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians, Accessed via Lawful Interception: NASS Approves N7.46 bn for DIA to Intercept Voice Calls and Internet communications of Nigerians | Dataphyte

· Ogala Emmanuel, Premium Times, INVESTIGATION: How Jonathan govt. paid companies linked to Doyin Okupe to hack 'unfriendly' websites, January 18, 2016; Accessed via https://www.premiumtimesng.com/investigationspecial-reports/196964-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websitesinvestigation-how-jonathan-govt-paid-companies-linked-to-doyin-okupe-to-hack-unfriendly-websites-2.html

· Ogundipe, S., Premium Times (2018, March 4): SSS wants detained Nigerian journalist to disclose sources
· before release. Premium Times.
https://www.premiumtimesng.com/news/headlines/260695-sss-wants-detained-nigerian-journalist-disclose-sources-release.html

· Professor Douglas C. Schmidt, Google Data Collection, 2018; Accessed via https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf

· Proshare, EFCC to register cybercafes, others; Accessed via https://www.proshareng.com/news/Investors-NewsBeat/EFCC-to-register-cybercafes,-others/1424

· Protection From Internet Falsehoods: Manipulations and Other Related Matters Bill, 2019; https://placbillstrack.org/upload/SB132.pdf

· Queen Esther Iroanusi, Premium Times (2021, July 12). Nigerian govt moves to control media, allocates N4.8bn to monitor WhatsApp, phone calls. Premium Times Nigeria. https://www.premiumtimesng.com/news/headlines/473147-as-nigeria-moves-to-control-media-nia-gets-n4-8bn-to-monitor-whatsapp-phone-calls.html

· QuartzAfrica, Facebook and Instagram made missteps on Nigeria's EndSARS protest while Twitter boosted it, https://qz.com/africa/1922372/facebook-hurt-nigerias-endsars-protest-while-twitter-boosted-it/

· Ridwan Oloyede, Surveillance Law in Africa: a review of six countries: Nigeria Country Report, published by the Institute for Development Studies, Accessed via https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Nigeria%20Country%20Report.pdf?sequence=7&isAllowed=y

· Rozen Jonathan, Committee to Protect Journalist: (2020, February 13). How Nigeria's police used telecom surveillance to lure and arrest journalists. https://cpj.org/2020/02/nigeria-police-telecom-surveillance-lure-arrest-journalists/

Sahara reporters, Newyork: See also Sahara Reporters. (2020, September 7). Aisha Buhari Attacks Daily Trust Artist, Bulama, Over Cartoon on Daughter's Lavish Wedding. Sahara Reporters. http://saharareporters.com/2020/09/07/aisha-buhari-attacks-daily-trust-artist-bulama-over-cartoon-daughter%E2%80%99s-lavish-wedding

· Sahara Reporters. (2019, March 2). EXCLUSIVE: NBC Shuts Down Jos Radio Station After 'Order From Presidency'. Sahara Reporters. http://saharareporters.com/2019/03/02/exclusive-nbc-shuts-down-jos-radio-station-after-order-presidency

· Samuel Ogundipe, Premium Times: "FACT-CHECK How Nigeria's secret police, SSS, is violating the law and illegally parading itself as DSS." Available at https://www.premiumtimesng.com/investigationspecial-reports/209343-fact-check-nigerias-secret-police-sss-violating-law-illegally-parading-dss.html, accessed 26 September 2021

· Simon Kemp, DATAREPORTAL: Digital 2021: Nigeria, Published 11 February 2021, Accessed via Https://Datareportal.Com/Reports/Digital-2021-Nigeria

· Spaces for Change "Closing Spaces for Democratic Engagement and Civil Society in Nigeria": Available at https://spacesforchange.org/wp-content/uploads/2017/06/Beyond-FATF.-Trends-Risks-and-Restrictive-Regulation-of-Non-Profit-Organisations-in-Nigeria.pdf, accessed 26 September 2021

· SPACES FOR CHANGE, Factsheet: Everything You Need To Know About The Hate Speech Bill, https://closingspaces.org/factsheet-everything-you-need-to-know-about-the-hate-speech-bill/

· Spaces for Change "Closing Spaces for Democratic Engagement and Civil Society in Nigeria". Available at https://spacesforchange.org/wp-content/uploads/2017/06/Beyond-FATF.-Trends-Risks-and-Restrictive-Regulation-of-Non-Profit-Organisations-in-Nigeria.pdf, accessed 26 September 2021, p. 17. For a more complete and updated chronology of attempts to legislate restrictive laws and regulations, see www.closingspaces.org

· Spaces for Change "Closing Spaces for Democratic Engagement and Civil Society in Nigeria". Available at https://spacesforchange.org/wp-content/uploads/2017/06/Beyond-FATF.-Trends-Risks-and-Restrictive-Regulation-of-Non-Profit-Organisations-in-Nigeria.pdf, accessed 26 September 2021, pp. 22-23.

· Spaces for Change "Unpacking the Official Construction of Risks and Vulnerabilities for the Third Sector in Nigeria." Available at https://spacesforchange.org/wp-content/uploads/2019/03/FULL-REPORT.-UNPACKING-THE-OFFICIAL-CONSTRUCTION-OF-RISKS-AND-VULNERABILITIES-FOR-THE-THIRD-SECTOR-IN-NIGERIA_compressed.pdf, accessed 26 September 2021, pp. 43-49

· Temitayo Jaiyeola, The Punch; NCC Warns Nigerians of Iranian Hackers' Possible Attacks (16 November 2021), Accessed via https://punchng.com/ncc-warns-nigerians-of-iranian-hackers-possible-attacks/

· Terman, R. Internet Censorship (Part 2): The Technology of Information Control. Townsend Center for Humanities, University of California, Berkeley. https://townsendcenter.berkeley.edu/blog/internet-censorship-part-2-technology-information-control

· The Bridge News. (2018, July 15):Armed policemen take over Ekiti Radio, TV stations. The Bridge News. https://www.thebridgenewsng.com/2018/07/15/armed-policemen-take-over-ekiti-radio-tv-stations/

· Titiola Oludimu, Techpoint, Lagos state's new surveillance system amplifies the need for a unified database (2017), Accessed via Lagos state's new surveillance system amplifies the need for a unified database Techpoint Africa

· Tope Adebayo, Techpoint: Navigating data privacy issues in targeted online advertising, https://techpoint.africa/2020/07/22/data-privacy-online-advertising/

· TV360: 70 Days in Custody; The Case of Emperor Ogbonna, https://www.youtube.com/watch?v=-7AIhPYzCOY&feature=youtu.be

· United Nations Human Rights Council, A/HRC/29/32: "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye" May 22, 2015, para. 60.

· University of Toronto's Citizen Lab, Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles, December 1, 2020

· Vanguard Nigeria: Igboho: FG, Beninese lawyers battles over extradition in court www.vanguardngr.com/2021/07/igboho-fg-beninese-lawyers-battle-over-extradition-in-court/amp. accessed 29 July, 2021

· Vanguard Nigeria: #EndSARS: Northern Governors sue for peace, condemn violence, October 23, 2020; Accessed via https://www.vanguardngr.com/2020/10/endsars-northern-governors-sue-for-peace-condemn-violence/

· Victor Ekwealor, Sahara Reporters Targeted In A Website Hack Techpoint Africa, January 11, 2017

· Victoria Ibezim-Ohaeri, Confronting Closing Civic Spaces in Nigeria: SUR 26, v.14 n.26, 129 - 140, 2017

· Victoria Ibezim-Ohaeri, Navigating Civic Space in a Time of COVID-19: Reflections from Nigeria, SPACES FOR CHANGE, 2021, Accessed via https://closingspaces.org/navigating-civic-space-in-a-time-of-covid-19-reflections-from-nigeria/

· Victoria Ibezim-Ohaeri, Zikora Ibeh, SPACES FOR CHANGE, Briefer: Civic Space During the Second Wave of Corona Virus, https://closingspaces.org/briefer-civic-space-during-the-second-wave-of-corona-virus/

· Victoria Ibezim-Ohaeri, Galvanizing Collective Action to Protect Nigeria's Civic Space, published by Shehu Musa Yar Adua Foundation, 2021, https://yaraduafoundation.org/files/Galvanizing%20Collective%20Action.pdf

· Yusuf Akinpelu and one other, Premium Times: Another report states that the freezing order was for 90 days – Premium Times "#EndSARS campaigner threatens to sue CBN for unlawful freezing of account." Available at https://www.premiumtimesng.com/news/top-news/441925-endsars-campaigner-threatens-to-sue-cbn-for-unlawful-freezing-of-account.html, accessed 26 September 2021

ACTION GROUP ON FREE CIVIC SPACE

ACTION GROUP ON FREE CIVIC SPACE SECRETARIAT:

SPACES FOR CHANGE | S4C
35B AJAKAIYE STREET, ONIPETESI ESTATE, MANGORO, IKEJA, LAGOS, NIGERIA
Email: info@closingspaces.org
Telephone: +234 703 620 2074 | +234 909 453 9638
Website: https://closingspaces.org/group-activities/