PRESS STATEMENT | December 8, 2021

ACTION GROUP ON FREE CIVIC SPACE

ACTION GROUP ON FREE CIVIC SPACE'S (AGFCS') LATEST REPORTS RAISE ALARM OVER THE USE AND MISUSE OF THE SECURITY RHETORIC TO RESTRICT CIVIC FREEDOMS IN NIGERIA

- **Calls for Urgent Measures to Safeguard Civic Space**

Ladies and Gentlemen of the Press

The Action Group on Free Civic Space (AGFCS) welcomes you to the launch and presentation of its latest joint action research reports: ***The Security Playbook of Digital Authoritarianism in Nigeria*** and, ***Harms from Abroad – The Impact of Global Security Measures on the Civic Space in Nigeria.***

The two reports present the findings of a three-part study which examined how the military and non-military measures—mostly copied from abroad—deployed to combat numerous security threats in the country, including terrorism in the north-east region, create opportunities for the use and abuse of counterterrorism (CT) and security laws to curtail civic freedoms. This is potentially becoming the dominant driver of closing civic space in Nigeria.

The first report, ***The Security Playbook of Digital Authoritarianism in Nigeria***, unveils how huge budgetary allocations, equipment, and technologies originally procured in the name of counterterrorism and curbing insecurity are being diverted to monitor the movement of citizens, track the activities of civic actors online, intercept private communications, and limit the ability of civic actors to organize, associate and assemble freely. The most popular tactics include the interception of private communications, network shutdowns, seizure of mobile phones and computers, use of forensic technology to extract and decode every ounce of data stored within digital devices, obtaining call records of individuals from network providers without a judicial warrant, blocking internet and website access through several technical protocols etc.

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. Although the government has used excuses like countering terrorism, fighting corruption and easing service delivery to justify intensive data collection, research findings prove otherwise. There is evidence that large volumes of personal data, including biometric information stored on multiple centralized databases, have been frequently compromised thereby increasing citizens' exposure to privacy intrusions, targeted advertisements, identity fraud and blackmail. State actors could not have recorded considerable successes in their diversionary and 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. Major suppliers of surveillance technologies to Nigeria include the Israeli-owned company, Circles; the U.S.-based Access Data Group, China's ZTE Corporation. Others include Cellebrite, FTK, Elbit Systems, Romix Technologies, together with Packets Technologies AD, another Israeli company operating out of Bulgaria.

The second report ***Harms from Abroad – The Impact of Global Security Measures on the Civic Space in Nigeria***, supplies evidence showing how the global war against terrorism—

instrumented in several norms set by international institutional mechanisms like the United Nations Security Council, the Financial Action Task Force (FATF) and the UN's Global Counterterrorism Strategy—is providing legal impetus for the Nigerian state to domesticate and implement hard security measures that limit civil society and fundamental freedoms. Because terrorism lacks a clear definition globally, the absence of a universally accepted definition of terrorism has acted as a motivation for governments to drift towards authoritarianism and apply overreaching measures to restrict the democratic rights of civic actors under the guise of preserving national security. The most popular tactics include (1); recharacterizing organised dissent as terrorism (2); proscription of self-determination movements; (3) criminalizing free expression and (4) restrictions on open democracy. Findings further show that governments like Nigeria introduce and enforce these stringent measure measures that shrink civil liberties in order to escape the dire consequences of non-compliance to global security norms and measures.

Incidents tracked on the Closing Spaces Database reveal that civic actors—such as journalists, protesters, LGBTQ activists and organizations, female activists and bloggers, persons with disabilities—are most affected by the state's arbitrary surveillance and misuse of security measures. The disproportionate crackdowns on civic actors are usually premised on national security concerns or the enforcement of health emergency measures, or premised on the rhetoric of anti-money (AML) laundering and countering of terrorist financing. Non-profit organizations operating in the country also pay a heavy price for these heightened security measures. Blanket restrictions, multiple registration controls, onerous reporting requirements, deregistration, forced closures, aggressive financial surveillance add to the list of heavy burdens NPOs are subjected to in the name of counterterrorism.

RECOMMENDATIONS

The AGFCS hereby calls for concerted efforts by the government, international community, private sector, media, and civil society to strike the requisite balance between competing legal interests such as national security, profit maximization and human rights. We recommend the following actions to halt and reform the misuse of digital technologies and security narratives to restrict civil liberties:

- Civil society, members of the public and Nigerian parliament should institute a process to properly define the term ‘‘terrorism’’ in existing anti-terrorism legislation. The definition of terrorism must be sufficiently clear and not exploited to target civil society actors or stifle freedom of expression.
- The Nigerian government can explore the use of legislative measures, import controls and strong sanctions against powerful businesses and individuals that supply and operate spyware technologies that are used to indiscriminately surveil citizens in the country.
- Civil society and concerned citizens can push for a review of all data protection legislation and judicial provisions that empower state agents to arbitrarily surveil persons or obtain personal data of citizens ‘‘without warrant’’ or court order.
- Businesses should seek to protect the rights of clients and customers by developing and adhering to data privacy policies and processes espoused under international and local laws. The United Nations’ (UN) Guiding Principles on Business and Human Rights (2011) provides standards and call to action processes that offer guidance to corporations on how to respect and protect human rights within their sphere of influence.

- International organizations can offer support to the advocacy by local organizations by pushing for stronger legal regimes and stiffer sanctions for suppliers of digital technologies used to indiscriminately surveil the activities of civic actors.

SIGNED BY THE FOLLOWING ORGANISATIONS

1. **INTERACTIVE INITIATIVE FOR SOCIAL IMPACT (DATAPHYTE)**
2. **THE INITIATIVE FOR EQUAL RIGHTS (TIERS)**
3. **SPACES FOR CHANGE | S4C**
4. **JUSTICE RIGHTS INITIATIVE (JRI)**
5. **VISION SPRING INITIATIVES (VSI)**
6. **CENTRE FOR CITIZENS WITH DISABILITIES (CCD)**
7. **WORLD IMPACT DEVELOPMENT FOUNDATION (WIDEF)**
8. **RULE OF LAW AND ACCOUNTABILITY ADVOCACY CENTRE (RULAAC)**
9. **BUILDING BLOCKS FOR PEACE FOUNDATION (BBFORPEACE)**
10. **SB MORGEN INTELLIGENCE (SBM INTELLIGENCE)**
11. **YOUTHS RIGHT AND ENVIRONMENTAL ADVOCACY CENTRE (YEAC)**