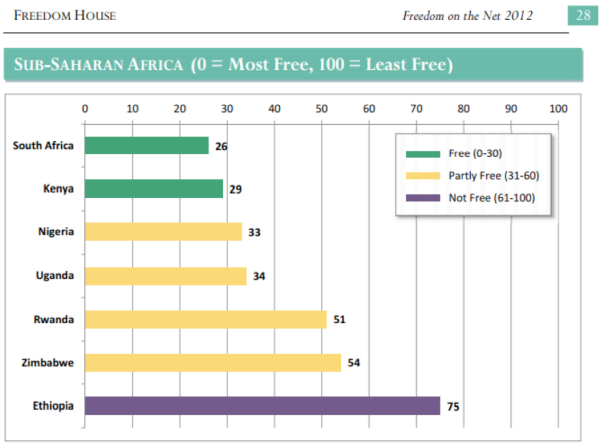
PIN Policy Brief No. 1

Nigeria: Making A Case For Enduring Internet Freedom

National Security and Internet Freedom

Internet Freedom is at risk in Nigeria, and there is a need to understand the surrounding issues within the context of citizen rights as established by the constitution of the Federal Republic of Nigeria.

Since Nigeria's return to democratic rule in 1999, the state of press and Internet freedoms in the country has swung from a pendulum, ranging from disinterest to sporadic clampdowns on press. In all of these, the Internet was mostly left alone, ostensibly because it had not become a major concern. Nigeria has been rated *Partly Free* over the last two years in the annual *Freedom On The Net* report, with slight improvement in 2012, compared to 2011. Fellow African countries, Kenya and South Africa, achieved the *Free* rating in 2012. Kenya actually crossed from *Partly Free* in 2011 to *Free* in the 2012 *Freedom on the Net* report.



The rise of the Internet on the back of mobile revolution has given voice to a new class of Nigerian citizens that are vocal and increasingly interested in public policy. The overall intention was to engage the government, and it was only a matter of time before active citizen presence on social and electronic media would begin to have real life impact.

Starting from the first day, 2012 was a tipping point for Nigerian citizen engagement of public policy, a trend that has strong roots in social media. The Occupy Nigeria movement of January 2012, for instance, started out as a hashtag on Twitter that found its way offline in a matter of hours, and eventually became a massive nationwide protest that would last two weeks.

The growing clamour of informed citizens who have taken to the Internet to demand accountability from the government has finally come to the ears of the country's leaders. However, recent trends suggest that in response, the Federal Government might be resorting to extreme measures to subvert the free activity of Nigerian citizens online.

On July 26, 2012, while speaking at a media retreat, the President of the Senate of the Federal Republic of Nigeria, who is ranked after only the President and Vice President, called for a clampdown on the use of social media in Nigeria. The House of Assembly of Oyo State in South-West Nigeria also made a similar call, following rumours about the state governor's wife. Bayelsa State, in Nigeria's Niger Delta area, embarked on a campaign to ban rumours.

On April 25, 2013, a Nigerian online newspaper, Premium Times, reported that the Nigerian government had signed a $40 million contract with Israel-based Elbit Systems to monitor Internet communication in Nigeria. Provisions in Nigeria's 2013 budget proposal setting aside $61.9 million for a "Wise Intelligence Network Harvest Analyzer System", among others, also confirm government's intention to commence Internet monitoring and surveillance.

In a related development, Nigeria was shown to be among the latest set of countries to have joined the league of 36 nations that have active Finfisher Command and Control servers. Finfisher, as described by the distributing company, has only one purpose – to help governments with *Information Technology intrusion and remote monitoring solutions*, including spying on the private Internet activity of their citizens.

Recently, the Nigerian Communications Commission also released the draft *Lawful Interception of Communications Regulations*. The draft has been met with stern criticism from civil society and Nigerian ICT journalists who have also described it as an attempt to retroactively jury-rig a regulatory framework around surveillance activity via secondary legislation, which is not subject to the scrutiny of the National Assembly.

The problem is not so much about monitoring as much as it is about such surveillance not being conducted within within pre-defined legal frameworks that are fair and reasonable to citizens, even when done in the name of keeping same citizens safe from terrorism and other vices. The absence of data privacy and lawful interception laws raises issues of the possibility of grave abuse by trigger-happy officials still steeped in military-era thinking.

While it could be argued that the Nigerian government is doing all of these against a backdrop of increasing security concerns, it is also important to avoid possible abuse, considering the context of Nigeria's maturing democracy. It is the primary responsibility of government to provide security, but with it comes an equally important duty to ensure that the rights of its citizens are not trampled.

PIN Policy Brief No. 1

Paradigm Initiative NIGERIA

Scenarios and Causes for Concern

The long-term consequences of the Nigerian government's current course of action could be severe and far-reaching, and it is possible that the policymakers do not fully comprehend the future implications of granting security operatives unchecked and unlawful powers of surveillance and access to private data.

Civil society organisations and journalists that already make government uncomfortable would be the first victims of the resulting Internet gestapo. After them, the increasingly vocal opposition, citizens who wish to freely express their opinion, and any perceived "enemy" of the administration, could lose their fundamental rights in the name of keeping Nigeria safe. Such a society cannot be said to be free or democratic.

The alternative, and preferred, scenario would involve the Nigerian government reversing its current course of action. This would be consistent with the promise of government to improve the nation's economy and quality of livelihoods by encouraging the expansion of affordable and high-quality broadband services. A connected citizenry that enjoys constitutionally guaranteed freedom could add better value through digital participation.

The Way Forward

Providing security for its citizens is the government's duty and prerogative, but protection by emasculation defeats the purpose. Internet surveillance within clearly established legal boundaries, that respect the fundamental privacy rights of Nigerians, is not abhorrent by itself. However, a balance has to be found between that duty to protect and a responsibility to ensure that fundamental rights are upheld. Nigeria must put appropriate laws and checks in place first. That is the least any government owes citizens whose rights it swore to protect.

Upon this premise, the advised course of action for the government would be to work toward the passing of *Data Privacy* and *Lawful Interception* laws that:

1. Prescribe the fundamental privacy rights of citizens and define the legal framework around surveillance.
2. Accord data privacy more priority than it currently has now. This is all the more urgent considering the numerous government and private institutions that hold sensitive citizen data. These include the National Identity Management Commission, Independent National Electoral Commission, Nigerian Communications Commission, Federal Inland Revenue Service, Nigerian Immigration Service, Federal Road Safety Corps, and banks.
3. Clearly outline provisions for interception in pursuit of a safer country without sacrificing the freedom of citizens or their constitutional right to communicate freely, including on the Internet.
4. Provide sufficient safeguards against abuse and opportunities for redress where infringement occurs.

In addition, it is in the interest of all concerned that the Internet surveillance and monitoring contract be annulled. The citizenry must also be sensitised, by relevant institutions, about the (direct and indirect) implications of unchecked government access to the private data of citizens. Enduring Internet Freedom is in Nigeria's best interest. (May 29, 2013)

Prepared by **Bankole Oluwafemi** and **'Gbenga Sesan**

For further information, please contact **Godson Ogumka**, ICT Policy Officer, Paradigm Initiative Nigeria: **info@pinigeria.org**
Website: **www.pinigeria.org** | Twitter: **@pinigeria**