'Gbenga Sesan | Paradigm Initiative Nigeria | **Case Study for Meeting on an Initiative for an African Declaration on Internet Rights** | February 11, 2014 | **@gbengasesan**

Security vs Freedom

Update on Internet **Freedom** and Communication **Privacy** in **Nigeria**

Military History and Clampdowns

On January 15, 1966, Nigeria's 6-year old post-colonial democracy was truncated by a military coup. What would be the country's first phase of military rule lasted until October 1, 1979, when General Olusegun Obasanjo handed over to a democratically elected Shehu Shagari. On the last day of 1983, General Muhammadu Buhari resumed the second phase of military dictatorship that survived until May 29, 1999. The years of military rule saw huge oppression of citizens and massive clampdown on the media and civil society.

Civil society leaders fled to exile. Media institutions that chose to report the news as it happened faced threats, attacks and even death. Every dissenting voice was billed for squashing until various events led to the re-emergence of democracy in Nigeria. In the same year that the military handed over the leadership of Nigeria and the nation joined other nations across the world to practice democracy, a Constitution (for the Federal Republic) with provisions for citizen rights returned as a supreme instrument.

Among other provisions, Section 37 of the Constitution of the Federal Republic of Nigeria (1999) makes a very strong case for citizens' rights to privacy: "*The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.*" Though Nigeria returned to democratic rule, this provision has not been perfectly respected. In fact, military-style provisions like "Official Secrets" and "Sedition" were popular until a Freedom of Information law was finally approved in 2011.

Threats to Privacy and Freedom

For a long time, Nigeria has seen various degrees of unrest around various regions of the country: South East's *Movement for the Actualization of the Sovereign State of Biafra* (MASSOB), South West's *Odu'a People's Congress* (OPC), militants in Nigeria's oil-rich Niger Delta area and the North East's *Jama'atu Ahlisunnah Lidda'awati Wal-Jihad*, popularly known as Boko Haram. Following a bomb blast at the venue where the 50th independence anniversary of Nigeria should have held, in October 2010, and other terrorist activities, the Nigerian State began activities that were borderline illegal as far as the privacy and freedom of citizens are concerned.

In 2013, the telecommunications regulator, Nigerian Communications Commission, introduced *Draft Lawful Interception of Communications Regulations*, which sought to achieve, through secondary legislation, what a Lawful Interception Bill was slow to achieve. There are now six bills in the National Assembly addressing subjects such as Lawful Interception and more.

Considering the constitutional provision that protects the privacy of telecom users, various groups kicked against the act. Groups asked the Government to do the right thing by subjecting any such regulation to the rigour of legislative processes. At about the same time, an online newspaper, Premium Times, revealed that the federal Government had awarded a secret contract to Elbit Systems – to monitor Internet communication in Nigeria. The contract implementation has since commenced. In May 2013, an online technology newspaper, Technology Times, also revealed that DigiVox, a company that specializes in lawful interception services, listed the Nigerian State Security Service and all private telecommunications operators in Nigeria - MTN, Airtel, Etisalat, Glo – as its clients.

Paradigm Initiative Nigeria's (Ongoing) Intervention

With support from the Citizen Lab/Munk School for Global Affair's CyberStewards Program and Internews' Global Internet Policy Project, Paradigm Initiative Nigeria (PIN) strengthened its focus on ICT Policy in Nigeria in the first quarter of 2013. This put the organization in a good position to fill an existing vacuum in advocacy for Internet Freedom in Nigeria.

Beginning with a Freedom of Information request that was not responded to after the mandatory seven (7) days, PIN commenced a targeted advocacy effort that has now evolved into the application for an "order of mandamus" through a Federal High Court in Abuja. PIN also continues to consult widely and has written 2 Policy Briefs on the subject.

Case Study Questions

1. What reason has your government (or another government that you know) given for similar clampdown or breach on citizen privacy?
2. Is surveillance a bigger problem in an online world than the offline one? If so, why?
3. What limits should apply to freedom of information, in order to protect other rights such as privacy and security?
4. What can we do to better protect privacy online?