On the review of the Cybercrime Act 2015

By Dr Jimson Olufuye, 19/11/2023

1.0 Introduction

The UN Human Rights Council (HRC) adopted by consensus a key resolution to promote, protect and foster the enjoyment of human rights on the Internet (UN Doc. A/HRC/20/L.13) on 5 July 2012.The protection of citizens' right is a security concern affirmed by the Universal Declaration of Human Rights, adopted by the United Nations in 1948. Hence, the diverse organisational mechanisms in place to provide this assurance.

In the same vein, per the resolution of July 2012, the need to assure online security (*a.k.a. Cybersecurity*) of citizens cannot be over-emphasized. The implication of the resolutions is that whatever rights (including security) citizens enjoy off-line apply online as well. Cybersecurity is thus a concern to all stakeholders; government, the private sector, the civil society, the technical and the academic communities and the youths in the multi-stakeholder Internet ecosystem.

2.0 The Terrestrial Security

In securing the lives of citizens, the Office of the National Security Adviser (ONSA) oversees the overall terrestrial national security interests of the nation in tune with the UN resolution above through the Armed Forces (the Army, the Airforce and the Navy), the Police, Civil Defence, etc. on behalf of the President and C-in-C.

3.0 The Cyber Security

With respect to the cyber ecosystem, why shouldn't a body also exist to handle the security issues thereof? In this wise, a case is hereby made for the establishment of an agency for Cybersecurity Coordination and Cybercrime Enforcement (A3CE) with the ability to coordinate all the disparate CERTS in Nigeria, protect the Critical National Infrastructure (CNI), conduct cyber research & intelligence (offence/defence), and prosecute cybercrimes, all under the auspices of the ONSA. (If it is just within NSA, nothing will happen as we have witnessed in the past. ONSA is best fit to oversee and not operate.)

The Agency would also be in a position to take responsibility for many regional and international cybersecurity conventions which we have been too slow to acknowledge, review, sign and ratify. Example is the Africa Union Convention on Cybersecurity and Personal Data Protection (a.k.a the Malabo Convention) released in 2014 which never came before any of our National Assembly sessions including the current 10th NASS. 15 Countries have signed the Convention, the number required for it to become binding. But how can Nigeria participate in cross-border cooperation when it has done nothing about this?

Examples of nations with Cybersecurity Agency/Authority

a. Togo: Togo cybersecurity agency - https://www.togofirst.com/en/itc/
b. b. Rwanda: Rwanda cybersecurity Authority - https://cyber.gov.rw/home/
c. Ghana: Ghana cybersecurity Authority - https://www.csa.gov.gh/
d. Europe: European Union Agency for Cybersecurity (ENISA) - https://www.enisa.europa.eu/
e. United States: U.S. Cybersecurity and Infrastructure Security Agency (CISA) - https://www.cisa.gov/

4.0 Drawbacks to the Nigerian Cybercrime Act 2015

The Nigerian Cybercrime Act 2015 is being reviewed because it could not be implemented due to a number of drawbacks.

Some of the drawbacks include:
1. Ineffective implementation mechanism. The Acts has no clearcut functional mechanism to drive the expectations of the Act. An Advisory Council could not have driven the Act because it is simply just an advisory body.
2. Absence of a body corporate to take full operational charge for the implementation of the Act.
3. Conflicting directives on how law enforcement can operate when it come to seizure of devices involved in cybercrime.

5.0 Proposal for Title Change

It is hereby proposed that the title of the Act be changed to the Nigeria Cybersecurity Act 2023 in line with the United Nations Economic Commission for Africa (UNECA) recommendation on a model Cybersecurity Law and the need to emphasize and promote security over and above cybercrime.

It can be recalled that African Heads of States (absent Nigeria) in collaboration with UNECA on 23-24 March, 2022 convened the first African Summit on Cybersecurity in Lome and agreed to a Lome Declaration on Cybersecurity and Fight Against Cybercrime, 2022. The Declaration expressed African Governments' commitment to establish a framework to efficiently fight against cybercrime and promote a culture of cybersecurity, including the creation of **authorities, structures and capacities dedicated to cybersecurity.** The vehicle for the realization of the Lome Declaration is the newly formed African Centre for the Coordination and Research in Cybersecurity (ACCRC) located in Lome, Togo by the instrument of the Memorandum of Understanding signed on 29, July, 2022 by the Government of the Republic of Togo and the United Nations Economic Commission for Africa.

6.0 Area of Amendments in the Act

Apart from the recommendation for an inverted focus from cybercrime to cybersecurity, I wish to propose amends as follows:

1. Section 38(1): "A service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria, for a period of 2 years."

There is a need to amend the title "Records retention and protection of data by service providers" to read "Data preservation and protection of data by service providers" for the following reasons:

i. To maintain consistency of the subject on data rather than records and
ii. The use of preservation rather than retention. Data preservation is requiring Communications Service Providers (CSP) (including Internet Service Providers) to store a particular individual traffic data for a finite period as specified under the appropriate judicial authority. Whereas, data retention is requiring all CSP to retain all of certain types of the traffic data created by all users. Data preservation is recommended because it is less burdensome and costly than retention and less harmful to public confidence.

2. Still on Section 38(1): Reference to "...all traffic data...", be replaced with "...specified traffic data..." to avoid the tendency of any agency responsible for the regulation of communication services in Nigeria to come up with a fiat directive for service providers to keep all traffic data of all subscribers; a situation, which will be grossly uneconomical, expensive and capable of increasing tariff instead of reducing it. There is no issue if based on lawful request by a law enforcement agent, all traffic data of a particular subscriber can be kept for a given period of time.

3. On lawful intercept by law enforcement officer, Section 38(2)(3)(4), it is recommended that the action of the law enforcement officer be backed up by "judicial authorization". This is essential, to avoid any form of abuse of office by any law enforcement officer and to respect the privacy commitment of service providers.

Dr Jimson Olufuye is the Chair of the Advisory Council of AfICTA - Africa ICT Alliance (https://aficta.africa), Principal Consultant at Kontemporary Konsulting Ltd and the UNECA Consultant on Cybersecurity. He recently delivered a UNECA sponsored report indicating a 10% increase in cybersecurity maturity enables between 0.66% and 5.4% increase in GDP per capita in Africa. The same report also showed a 10% increase in Internet Penetration enables between 1% and 8% increase in GDP per capita.