AN XRAY OF THE NIGERIA CYBERCRIMES ACT 2015 VIS-À-VIS RIGHT OF PRIVACY IN NIGERIA

Oluwaseun Viyon Ojo, Lagos State University
AN XRAY OF NIGRIA’S CYBERCRIMES ACT 2015 VIS-À-VIS THE RIGHT TO PRIVACY

The National Assembly passed the Cybercrimes (Prevention, Prohibition etc.) Bill after having deliberated on its various provisions. On the eve of the administration of President Goodluck Jonathan, the bill passed by the National Assembly became the Cybercrimes (Prevention, Prohibition etc.) Act 2015 (hereinafter to be referred to as the Act) after having received presidential assent. Thus, it entered into the corpus of laws and legislations in force within the Nigerian legal environment. It must be said that the Act is a laudable development in Nigeria’s legal and commercial jurisprudence as much as it contains new and novel provisions.

As much as the Act contains laudable objectives and intendment to achieve in the ICT, e-commerce and financial sector, it should still be subject to critical appraisal in certain areas observable from a circumspect scrutiny of the Act.

To start with, one of the many objectives of the Act is to confer on the Nigerian Communications Commission (NCC) (the regulatory body with respect to the communications sector) and security agencies the unrestricted powers to intrude into private communications of Nigerians such as telephone calls, email messages and such other electronic exchange of information like short messaging service (SMS) and multimedia applications with a view to enhancing national security, preventing crime and facilitating criminal investigations. It is pertinent to state here that these particular provisions of the Act mandating the Nigerian Communications Commission as the relevant authority to authorise the service provider to keep certain subscriber information and then make disclosure when required indeed raises a whole lot of concerns and issues in respect of the human rights of individuals especially the right to privacy. The questions that would necessarily crop up are whether the emergence of the Act would portend that the private correspondence of all persons would be intruded upon without legal implications. Does it mean that the security agencies will have the licence to interfere with the privacy of an individual in the course of investigations? Does it mean that no private information and details shared by an individual with a social network can remain confidential? Does it portend that no hitherto confidential information is really confidential in the real sense of the word? Does it imply that the right to privacy guaranteed under the Nigerian Constitution 1999 (as amended) could be reasonably derogated from in reasonable circumstances as provided in this Act under consideration? These are the questions that should be considered cursorily by the relevant parties and stakeholders even after the enactment of the Act with such enormous powers placed on the relevant authority and security agencies. This piece shall seek to discuss the following questions in view of the available statutory enactments and judicial authorities both within the Nigerian and United States legal terrain and then use the United States position as a template to assessing critically Nigeria’s Cybercrimes (Prohibition, Prevention etc.) Act.

With utmost importance placed on the right to privacy in this piece, it is apt to state the constitutional position on the privacy of persons. The 1999 Constitution of the Federal Republic of Nigeria (as amended) has sufficient provisions in relation to the privacy of citizens and section 37 thereof states that “the privacy of citizens, their home, correspondence, telephone conversations and information contained therein shall be inviolable and no one shall be interfered with in the exercise of this right except in the interests of national security, public safety, or the law enforcement agencies.”
AN XRAY OF NIGRIA'S CYBERCRIMES ACT 2015 VIS-À-VIS THE RIGHT TO PRIVACY | The Lawyers Chronicle

2/4


9/11/2015

"right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned. The term “right of privacy” is a generic term encompassing various rights recognized to be inherent in concept of ordered liberty, and such prevents governmental interference in intimate personal relationships or activities, freedoms of individuals to make fundamental choices involving himself, his family, and his relationship with others."

As a matter of constitutional expediency and human rights necessity, the privacy of every person is duly guaranteed and any infringement on such right will actually entitle the person to seek legal redress in the court of law.

Now turning to the Act, the Act allows the monitoring of electronic communications by government and empowers it to carry out lawful interception on suspected electronic communications. The Act in question contains some provisions in relation to right to privacy. The Act provides that the service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority (that is the Nigerian Communications Commission) for the regulation of communication services in Nigeria for two years (see section 38(1) of the Act). In addition, the service provider shall, at the request of the relevant authority (as stated above) or any law enforcement agency, preserve, hold or retain any traffic data or release any information required to be kept by the Act (see section 38(2) of the Act). Furthermore, it shall be mandatory upon the service providers to comply with any request made by any authorised officer of any law enforcement agency for the release of information retained or preserved by them (see section 38(3) of the Act). What these provisions therefore allow is for the disclosure of any information shared by a subscriber with the service provider to any law enforcement agency. As soon as the Act imposed the duty on the service provider to release such information, it quickly provided that any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this request shall not be utilised except for legitimate purposes as may be prescribed under the Act, regulation or under any order of the court (see section 38(4) of the Act). It implies that such retained information must only be used for purposes sanctioned by the law and not for any other illegitimate purpose.

Furthermore, where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purpose of a criminal investigation or proceeding, a judge may, on the basis of information on oath; order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data or traffic data associated with specified communications transmitted by means of a computer system (see section 39 of the Act).

The above reproduced provisions of the Act allows for the retention of subscriber information, interception of electronic communications and then disclosure of such to the government or law enforcement agencies. It must however be stated here with regards to the right to privacy that section 38(5) of the Act provides that anyone exercising any function under this section shall have due regard to the individual’s right to privacy under the Constitution of the Federal Republic of Nigeria and shall take appropriate measures to safeguard the confidentiality of the data retained, processed, or retrieved for the purpose of law enforcement. This provision as reproduced above is a pointer to the fact that the right of privacy of individuals is still considered important by the Act. However, the permission given the service providers to unusually retrieve and disclose any confidential information shared by the subscriber with them is still a breach of confidentiality and privacy of correspondence, telephone conversations and telegraphic communications enjoyed by the individual under the Constitution. As a matter of fact, most of these service providers usually have privacy policies which usually govern the relationship between them. Disclosure of such information will no doubt amount to a breach on the privacy policy and confidentiality agreement.

However, the above argument should not be construed as creating the grounds for the removal of these provisions that purportedly affect the privacy of individuals. What will be proposed, at this juncture, is the fact that there is need for a proper balance to be struck between the rights of persons to be protected from undue interference with their private communications and the interest of the government to protect people from grossly offensive communication and forestall perceived breach of security and criminal activities. The right of privacy of persons is a sacrosanct right entrenched in the 1999 Constitution. However, it is subject to the constitutional restriction and reasonable derogation clause contained in section 45 of the 1999 Constitution (as amended). As a result, section 45 of the 1999 constitution states that:

"Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society

1. a) in the interest of defence, public safety, public order, public morality or public health; or
2. b) for the purpose of protecting the rights and freedoms of other persons.”

The implication of the above provision to the guarantee of the right of privacy of persons is that it can be derogated from or restricted upon in the interest of the public and for the purpose of protecting the rights and freedoms of others. However, it must be pointed out here that such restriction or derogation must be reasonable and justifiable in any democratic society. Flowing from these, the following questions become relevant; are the provisions of the Act affecting right of privacy reasonably justifiable in a democratic society? Are the various provisions of the Act relating to the punitive measures reasonable in the light of a democratic society? Such provisions could arguably be considered reasonable considering the fact that the disclosure will only be required by the law enforcement agencies for the purpose of protecting public interest, public safety, promoting national security and facilitating criminal investigations.

However, it can still be argued that such provisions in the Act could be considered reasonable and

Dictionary, 6th Edition, 1990 at p.1195 defines the right to privacy as:

"..."
justifiable considering the fact that the disclosure will only be required by the law enforcement agencies for the purpose of protecting public interest, public safety, promoting national security and facilitating criminal investigations as envisaged by the Constitution under the reasonable derogation clause. The argument may seem plausible. But the need for it must be balanced with the guarantee of the privacy of persons and public opinion. It is instructive to consider what the Supreme Court of the United States ruled when a matter on this issue came up for determination. Thus, in United States v. Jones, 565 US, 1332 Supreme Court 945 (2012), the joint Federal Bureau of Investigation (FBI) and Metropolitan Police Department task force in 2004 began investigating Antoine Jones for narcotics violations. During the course of the investigations, a Global Positioning System (GPS) device was installed on Jones’ Jeep Grand Cherokee without a valid warrant. The device tracked his movements constantly for four weeks. The FBI arrested Jones in late 2005. He was arraigned before the court, convicted on the basis of the GPS tracker’s discovery and sentenced to life in prison. The case was appealed to the United States Court of Appeal for the district of Columbia Circuit and the conviction was overturned on the fact of the violation of the Fourth Amendment’s unreasonable search and seizure clause by the use of the GPS tracker. Thus, the Supreme Court of the United States in a 9-0 decision found that the government installation of a GPS system in a vehicle constituted a search under the Fourth Amendment and therefore requires a warrant and compliance with the terms of the warrant. Thus, the court ruled to reverse the conviction. What can be gleaned from the above decision is that the Supreme Court was against unreasonable and unwarranted investigation of person’s private affairs without compliance with the due process set by law. Similarly, in the case of Sorrell v. IMS Health Inc. 131 S.Ct. 2653 (2011), the Supreme Court debunked the argument of Vermont that the Prescription Confidentiality Law, which required that records containing a doctor’s prescribing practices not be sold or used for marketing purposes unless the doctor consented, was necessary to protect medical privacy and achieve improved public health care.

In view of the above argument, it is suggested that the fact that the Act allows for lawful interception on electronic communications and disclosure of confidential records does not open the room for the service provider and other persons to unduly breach and disregard the sacrosanct provisions of the Constitution relating to the right of privacy. Right of privacy is and remains a fundamental right of an individual under the 1999 Constitution of the Federal Republic of Nigeria. The confidential nature of the data and information shared with the service provider must still be upheld and safeguarded against any third party, unlawful intruder and meddlesome interloper save for instances of grave security threat and potential breach of the interest of defence and public safety where they would need to comply with the mandatory obligations imposed by the Act.

Ojo Oluwaseun Viyon

Ojo Oluwaseun Viyon is a graduate of law from Lagos State University (LASU), Lagos, Nigeria.

Author: tlc

302 articles / Browse all articles

RELATED ARTICLES »

AN ASSESSMENT OF NIGERIA’S CYBERCRIMES (PROHIBITION, PREVENTION ETC) ACT 2015

THE INTERNET, FREE SPEECH AND NATIONAL LAWS

ELECTRONIC SERVICE OF COURT PROCESSES IN AFRICA: HOW RELEVANT IS FACEBOOK, YAHOO AND GMAIL?

POST A COMMENT

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment
