PROTECTING THE PRIVACY OF DATA: SEARCH AND SEIZURE OF COMPUTER DEVICES UNDER THE CYBERCRIME (PROHIBITION, PREVENTION, ETC) ACT 2015*

Abstract

Certain far-reaching powers are sine qua non in facilitating the proper policing of the society. One of such powers is the Police investigative powers of search and seizure. This paper examines how the Nigeria Police have used this power of search and seizure, especially, as allowed under the Cybercrime (Prohibition, Prevention, Etc.) Ac 2015. It answers the question of the propriety of the search and seizure of computer devices in this age of the internet, as well as, the constitutionality thereof, in the light of the provisions of the Cybercrime (Prohibition, Prevention, Etc.) Act 2015. In investigating this paper, such, analytical tools as, meta-analytical style doctrinal comparisons, overt and covert interviews, including resort to both primary and secondary sources of law, were deployed. This paper recognizes that the search and seizure powers are not only crassly abused by the members of the law enforcement community in Nigeria; rather, that computer devices contain so much information in this era, that their data is protected by the constitutional right to privacy. A law enforcement agent only needs to place a person under arrest to enjoy virtually unbridled powers of search, and even the seizure of such computer devices with their critical private data. It concludes that in the present internet age, a computer device-borne personal data is too sensitive to be treated as a mere chattel found on the arrestee. Further, it is the conclusion of the paper that the data contained in a computer device is constitutionally protected under privacy rights; hence, evidence procured in breach thereof, cannot be rendered admissible under Nigerian statutory exception for 'illegally obtained' evidence: it would be 'unconstitutionally obtained' evidence. It thus recommends that the decision on whether to search a person, be vested on the team leaders and or senior police officers (SPO's), and their equivalent in rank, while a computer device itself must not be searched and its content accessed without a warrant. Also recommended is that the computer-borne data cannot be admitted in evidence, if it is obtained either warrantless, or outside the exceptional circumstances accommodated in the constitution itself.

Keywords: Privacy, Computer, Protection, Cybercrime, Seizure, Prevention

1. Introduction

In Nigeria, it is a frequent and notorious practice of the officers of the Nigerian Police to snatch smart phones, iPads, laptops and other computer devices from suspects and even regular wayfarers, alike; these officers usually go on to recklessly browse the personal information contained therein, willy-nilly. Often, the Police do so under the pretext of seeking incriminating information as part of their vaunted 'investigation activity' aimed at preempting or solving the commission of crimes. The undeclared reason, however, is often to check their victim's bank account balance, so as to determine their capacity to 'settle' them (the Police). Public resentment against this notorious practice of virtual armed robbery by, especially, the Nigerian Police Special Armed Robbery Squad (SARS), amongst such other despicable and oppressive practices like prolonged detention, brutality while in detention, and the lending of their powers to the settlement of civil disputes, came to a head with massive nationwide peaceful protests code-named #EndSARS, which drew global attention from the European Union[1], United States of America Government[2], to the United Nations[3], etc. The international community weighed in on the concerns of the #EndSARS protesters; they advised the Nigerian Government to address the concerns of the protesters.

2. Abuse of the Powers of Search and Seizure under the Cybercrime (Prohibition, Prevention, Etc.) Act, 2015

The most current of the powers thus abused by the Police in conducting these whimsical searches and seizures of citizens' computer devices are found under Sections 9 and 144 Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 (C.P.P.A, 2015). Section 9 of the C.P.P.A, 2015, provides thus:

> [1] Where a suspect is arrested by a police officer or a private person, the officer making the arrest or to whom the private person hands over the suspect:
>
> (A) may search the suspect, using such force as may be reasonably necessary for the purpose; and

*By **S.C. IFEMEJE, LLB, BL, LLM, PhD,** Professor and Dean, Faculty of Law, Nnamdi Azikiwe University, Awka, Anambra State, and

***Nwafili Mark OKWUOSA, LLB, BL, LLM, PhD Candidate**, Faculty of Law, Nnamdi Azikiwe University, Awka, House of Solomon & Associates, No. 9 St. John Street, Odoakpu, P.M.B 2967, Onitsha, Anambra State.

[1] 5 United States Code, *Section 552a (c), (d).*

[2] https://www.dw.com>nigeria>un-slam. Last accessed ion 14/7/2021.

[3] ·https://www.state.gov/ongoing-protests-in-nigeria.Last accessed on 29/10/2020

> (B) shall place in safe custody all articles other than necessary wearing apparel found on the suspect.

Section 144 of the C.P.P.A, 2015, provides thus:

> [1] Where a court or Justice of the Peace is satisfied by information on oath and in writing that there is reasonable ground for believing that there is in any building, ship, carriage, receptacle, motor vehicle, aircraft or place:
> (A) anything upon or in respect of which any offence has been or is suspected to have been committed; or
> (B) anything which there is reasonable ground for believing will afford evidence as to the commission of an offence; or
> (C) anything which there is reasonable ground for believing is intended to be used for the purpose of committing an offence, the court or Justice of the Peace may at any time issue a warrant, called a search warrant, authorizing an officer of the court, member of the police force, or other person named to act in accordance with subsection (2) of this section.

It is clear that while under Section 9, C.P.P.A, 2015, the person to be searched is someone who has been placed under arrest by the police, or arrested by a private person and handed over to the police. Under Section 144, C.P.P.A, 2015, the person is not under arrest, but the search must be consequent on a duly issued search warrant. Clearly, none of those sections justifies the Nigeria police officers' notorious practice of searching the person of wayfarers, snatching their portable computer devices and accessing the oft very confidential data stored therein. This is so because these street and highway searches are hardly conducted on suspects *placed under arrest,* or are they backed with any *search warrants* procured in respect of those individuals whom the police always just run into on the road, minutes before the searches. Indeed, these searches are mostly targeted at young persons, particularly, those dressed in the exuberant manners favoured by the very young and opulent, otherwise referred to as 'Yahoo Boys.'[4]In the very Nigerian public officers' manner of speaking without thinking through their dismissive denial of responsibility, the Nigerian Police authorities have often declared in the press that such searches are illegal. Of course, such declarations are little more than sheer grandstanding, as the obnoxious and abusive practice has continued unabated, and publicly, too. What is more, such searches are not necessarily entirely illegal, without more; this much is clear from the letters of Sections 9 and 144 of the C.P.P.A, 2015, reproduced above.

It is submitted that even if the men of the Nigerian police were to comply with the provisions of Section 9, C.P.P.A, 2015, i.e., searching only the people that they placed under arrest, it would still amount to a violation of privacy rights of suspects. It is submitted that to empower the police to capriciously do so merely because they elected to place one under arrest, (which arrest may be terminated, after all, the moment the police are done with violating the data privacy of detainee's computer device in the guise of a search), is to authorize a violation of citizens', otherwise, constitutionally guaranteed rights to privacy and the dignity of the human person, without remedy. For the avoidance of doubts, in providing for privacy rights over the citizens' 'correspondence, telephone conversations and telegraphic communications'[5], the Constitution clearly assured the privacy of the data stored in citizens' computer devices. This is so because most computer devices are now correspondence devices, as well. The only exceptions[6] permitted by the Constitution over the observance of this right to privacy are: (a) In the interest of defence, public safety, public order, public morality or public health; or (b) For the purposes of protecting the rights and the freedom of other persons.

It would be begging the question to emphasize that none of those constitutional exceptions/ grounds operate on the minds of the men of the Nigeria police when they decide to frisk members of the public, *a fortiori*, staying within the bounds of those constitutional exceptions. Assuming but not conceding that the police actually contemplate those bases, whose decision should it be to resort to those exceptions? Should it be the

[4]This is a street lingo originally used to refer to (mostly young) persons who used the internet to perpetrate various forms of financial fraud (advance fee fraud, love scam, etc.). The vice came into its own in the early days of the internet, when 'Yahoo' held the present place of 'Google', as the dominant search engine; hence, the term 'Yahoo Boys'. This expression has since been expended from its original connotation to accommodate opulent and loud young persons, whose sources of affluence is now believed to include even kidnapping for ransom, ritual killings, etc.; generally, young persons who live luxuriously on ill-gotten funds.

[5] Section 37, 1999 Constitution of the Federal Republic of Nigeria (as amended).

[6] Section 46 (1) [a] and [b], 1999 Constitution of the Federal Republic of Nigeria (as amended).

call of any gun- toting policeman, to determine when he would set aside the observance of a basic constitutional right? Indeed, is a computer device more than a mere chattel found on an arrestee?

In the United States of America, in a profound advancement of the digital right of citizens, the Supreme Court, in a unanimous decision, rejected the conviction of the appellant, which was secured on the basis of evidence obtained via a cell phone seized in a traffic stop, in *Riley v. California*.[7] In the *Riley case*, a certain David Leon Riley, as a gang member, used his car as getaway car after his gang members carried out a drive by shooting on 2/8/09. Thereafter, on 22/8/09, he was pulled over by the police, while driving another car. The police discovered that he was actually driving on a suspended driver's license, a situation that, by police policy, carries the repercussion of the impoundment of the vehicle that he was driving. Again, to avoid liability against the police to a future claim, it was imperative that the police searched the car in order to take inventory of the content of the car as at the time of the impoundment, as well as, to discover the presence of any contraband. In the course of the search, the police discovered two guns, and then arrested Riley for possession of firearms. Upon the arrest, Riley was searched, and the cell phone found in his pocket taken custody of. An analysis of the videos, photographs and signs on his cell phone by a police unit specializing in Gang modus, subsequently tied Riley, not merely to gang membership, but also to the drive by shooting earlier that August, 2009, as a result of the ballistics tests on the guns. Another set of charges were also brought against Riley, including shooting at an occupied vehicle, attempted murder, and assault with a semi-automatic firearm. Riley's objection to the admissibility of the evidence of his gang membership, on the ground that same was secured in negation of his electronic data privacy right, was overruled. The jury convicted him on all of the three counts, handing him a sentence of 15 years to life in prison. Subsequently, on appeals up to the Supreme Court, the issue for determination was, whether the evidence admitted at the trial from Riley's cell phone discovered through a search that violated his *Fourth Amendment*[8] right to be free from unreasonable searches, was admissible in proving the charges found on those pieces of evidence. In a unanimous judgment with the lead opinion written by Chief Justice John G. Roberts Jnr. of the United States Supreme Court, recognized the warrantless search exception to the rule against unreasonable search of an arrestee, which exception exists to protect the arresting officer safety and preserve evidence; it however, held that neither is in issue in the search of digital data. Digital data, the court held, cannot pose a threat to the safety of an arresting officer, while police officers have the ability to preserve evidence as they await a warrant, by connecting the phone from the network and placing it in a 'Faraday Bag'[9]. The court qualified cell phones as minicomputers filled with massive amounts of private information, which distinguished them from the traditional items that can be seized from an arrestee's person, like a wallet. Further, the court held that data accessible via the phone but stored using 'cloud computing' is not even 'on the arrestee's person'. The court, though, (not unlike the exemptions under the 1999 Constitution) allowed that warrantless searches of cell phones might be permitted in an emergency: when the government's interests are so compelling that a search would be reasonable. In summary, the court held that police officers must obtain a warrant before searching the phone of a subject of police investigation. If they do not, the search is illegal - it would amount to a violation of the *Fourth Amendment to the U.S Constitution,* the court concluded.

Though even in the United States of America, the laws allowed an arresting officer to search the cell phone of a suspect on the ground that same was in the area into which he might reach, because of the possibility of a hidden weapon or the destruction of evidence, in the *Riley case*, the court rationalized that modern cell phones are not just another technological convenience; that with all they contain and all they may reveal, they hold for many Americans the privacies of life. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought, the court concluded. The judgment in the *Riley case* does not preclude the police's right

[7] 573 U.S. 373 (2014).

[8]Thus *Fourth Amendment*: *(Amendment IV) to the United States Constitution (U.S.C)* of *1789*, which is part of the *Bill of Rights* (Fundamental Rights) provides thus: The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The Bill of Rights is a set of the first ten amendments introduced to the United States Constitution. These amendments made in 1789 were aimed at adding specific guarantees of personal freedoms and rights, clear limitations on the power of the government in judicial and other proceedings, as well as, explicit declarations that all powers not expressly granted to the United States Congress shall be deemed to be reserved and vest in the States and the People. The ideas codified in these amendments were essentially borrowed from the *Virginia Declaration of Rights* (1776), the *English Bill of Rights* (1689), and the *Magna Carta* (1215).

[9]This is a pouch designed to protect its content (cell phones, etc.) from location tracking, hacking, and damage due to external electromagnetic field (EMF) by blocking all outgoing and incoming EMF signals, including GPS, Cell Phone, Wi fi and Bluetooth.

of seizure, but no search of such a seized phone must be carried out without a warrant first sought and obtained. Interestingly, not only has the Supreme Court of Nigeria settled it as a trite part of the Nigerian jurisprudence, that even an illegally obtained evidence cannot be denied admissibility merely because of the manner it was obtained[10] rather, it was eventually codified under the Evidence Act, in the 2011 amendment[11], and affirmed in decided cases[12], since the 2011 amendment.

The above state of the Nigerian jurisprudence may have been permissible before the minicomputers became such a part of our world; however, not anymore. In the present internet age/ era, the warrantless accessing of a computer device borne – personal data, it is certainly no more proper to be thrown into the omnibus basket of 'illegally obtained evidence'. In tandem with the sound reasoning of the lords of the United States' Supreme Court 'Modern cell phones are not just another technological convenience…. With all they contain and all they may reveal, they hold for many Americans, the privacies of life,' [13] the cell phone and its content fall into the basic right protected under the constitutional guarantee for personal privacy.

In the light of the foregoing, it is not enough to leave, to bundle unconstitutionality with mere illegality, in determining the question of the admissibility of evidence obtained in violation of certain rights, or through the perpetration of some prohibited acts. Of course, outside those constitutionally provided exceptions, the court has no discretion to exercise in admitting a piece of evidence obtained in the violation of a constitutional provision. In Nigeria, the right to privacy is a constitutional right, and it deserves all the special protection that that connotes. Such a minicomputer-borne personal data, if accessed without warrant, in Nigeria, would be 'unconstitutionally' obtained; not just 'illegally' obtained. Put differently, an exception to a constitutional right cannot be provided for or justified by either the parliament or the court in the actual or supposed interpretation of any mere act of parliament; only the Constitution can provide an exception to or a reprieve from compliance with the constitution. That is the essence of the supremacy of the Constitution.

The advent of the internet and the advances in recent years led to the storage of all sorts of extra-ordinary information on the phone. This carries a concomitant need to protect, not the smart phone, but the sensitive contents of a smart phone. In practice, even in the United States of America, it would seem to this scholar that the power to seize without more, when placed side by side with the lack of the power to search the seized phone, without warrant, would mean nothing unless the user's phone is locked with a passcode or encrypted. The user, therefore, carries a duty to lock and keep his phone with a passcode/ password, so that the Police may not be able to access the private data contained therein without the owner's cooperation; howsoever obtained. Incidentally, given the brash and reckless approach of the Nigerian police to this question of accessing the confidential data in the cell phone of a citizen, it would not make any difference that such cell phone is secured with passcode/ password, or whatever other personal identification passcode, because they practically compel the owner (*viet armies*) to unlock the phone by himself.

The 2015 enactment, of the Cybercrimes (Prohibition, Prevention, Etc) Act 2015 heralded Nigeria's entry into the community of nations with Internet violation-specific legislations. The legislation is a commendable gesture, as far as rousing from the slumber of the reality of the imminent and current threats in the information age, after some other nations of the world began to contend with such threats since the late 1960's. However, as per content, the C.P.P.A proved to be quite deficient in some critical respects; unreasonable searches of the individual and his property are one of such deficiencies. The unreasonable or abusive searches of the person of the individual and/ or his property are frowned at by our laws, and so for good reasons; hence, the insistence/ requirement for a search warrant, which is usually issued by a disinterested third party. Of course, once armed with a search warrant an agent of the state may legally carry out a search. The naughty issues, however, as earlier alluded to, are:

(A) Whether the state agent would break the code of an encrypted data;

(B) Whether the subject of the search could be compelled to de-encrypt his encrypted data that the state agent is unable to crack, in the light of his right not to be compelled to give up self-incriminating information; and

(C) Whether or not such encrypted information could be used by the agent of the state, once accessed, would depend on the latitude of the search warrant.

[10] *Sadau v. The State* (1968) 1 ANLR, 124; *Torti v. Ukpabi* (1984) 1 SCNLR, 214.

[11] Sections 14 and 15 thereof.

[12] *Okafor v. State* (2014) LPELR - 24477 (CA); *Abubakar & Anor. v. INEC & Ors.* (2019) LPELR - 48488 (CA).

[13] *Riley v. California (supra).*

Even these issues, we shall answer here without any further deliberation, especially, in the light of what we have thus far espoused hereinabove. With a warrant duly issued, the state can do all of the above; provided that no warrant issued to access the data in a computer device would qualify as having been 'duly issued', unless the grounds justifying the issuance are traced to the exceptions under Section 46 (1), 1999 Constitution.

3. Conclusion and Recommendations

The C.P.P.A, 2015, no doubt, empowers the police to search people they have placed under arrest, and even seize some of their chattel. However, there is nothing in the C.P.P.A, 2015, that either authorizes or excuses the notorious past time of the men of the Nigerian police, in seizing and whimsically browsing the computer devices of the people they regularly stop and search on the highways. The excuse of searching these computer devices as part of the vaunted investigation activities does not avail the police either, because such devices, in the present internet age, cache such sensitive and confidential data, that the contents are protected by constitutional guarantee for the right to privacy; hence, it requires a warrant to be accessed and searched. Any evidence extracted from a computer device, which search and extraction are carried out without a search warrant, would not be admissible in a court trial, and the Evidence Act provisions and judicial precedents, permitting the admissibility of relevant but illegally procured evidence, would not inure to such evidence procured through a warrantless search of a computer device. The reason is that there is a difference between an 'illegally procured', and an 'unconstitutionally procured' evidence. Finally, the open cheque granted to all every policeman to decide when to search a person, is susceptible to abuse. It is recommended that the courts realize that a computer device is not a mere chattel which could be capriciously seized from a suspect and the data stored therein lightly accessed, and also distinguish between an illegally procured evidence, which may be admissible in evidence, and an unconstitutionally procured evidence, which shall not be admissible in evidence, unless the breach that attained the procurement, except the breach falls within the constitutional exceptions. Also recommended is the amendment of the C.P.P.A, 2015, to place the discretion as to whether or not a suspect should be searched, in the exclusive preserve of Senior Police Officers (SPO's).