International Journal of Academic Accounting, Finance & Management Research(IJAAFMR)
ISSN: 2643-976X
Vol. 5 Issue 3, March - 2021, Pages: 10-16

Data Sharing And National Security In Nigeria: Interrogating The Practice Of Multi-Agency Collation Of Similar Data

[1]OMOTOSHO Pius Arowolo and [2]Prof. EWUIM, Ngozi Christiana (PhD.)

[1]Department of Public Administration, Nnamdi Azikiwe University, Awka Anambra State, Nigeria
pius_omotosho@yahoo.com
[2]Department of Public Administration, Nnamdi Azikiwe University, Awka Anambra State, Nigeria.
n.ewuim@unizik.edu.ng

Abstract: *The study is an empirical inquiry on data sharing and national security in Nigeria, an interrogation of the practice of multi-agency collation of similar data. The objectives of the study are to establish the relationship between multiple biometric capturing and accuracy of biometric information in Nigeria and to ascertain the effect of inter-agency data sharing on crime prevention, investigation and control in Nigeria.in view of the specific objectives of the study, two research questions and hypotheses were formulated and tested for the study. Data for the study was obtained through primary and secondary sources. With a total population of 355 respondents, a sample of 188 was obtained using Taro Yamani Formula. Data obtained from the respondents was presented in table and analyzed using frequency counts and mean scores and the hypotheses were tested using Pearson correlation at 0.05 level of significance. Findings from the study revealed that there is no significant positive relationship between multiple biometric capturing and accuracy of biometric information in Nigeria and that inter-agency data sharing has an effect on crime prevention, investigation and control in Nigeria. On the basis of the findings, the researchers recommended, among others that the Nigerian government should set modalities in place to begin to harmonize existing data and to extend the reach and coverage of the citizens in order to create a robust database for effective policy planning, security and provision of social services.*

Keywords: Biometric Data, National Security

INTRODUCTION

On Sunday the second day of February, 2020, a suspected terrorist attempted to bomb the Kaduna state branch of a first generation Pentecostal church in Nigeria. The incident, aside from the obvious threat it poses to the security and safety of the hundreds of worshippers that were present at the time of the incident, raises serious questions about the poor state of Nigeria's demographic data management. The Nigerian Police Force, through the Kaduna State Police Public Relations Officer, DSP Yakubu Sabo, gave the name of the suspect as Nathaniel Samuel, but the Kaduna State Chairman of the Christian Association of Nigeria (CAN), Rev. John Hayab disagreed with the identity of the alleged suicide bomber as given by the police. According to Hayab, the suspect had earlier identified himself as Mohammed Sani when he was apprehended by the church security officials.

Joining in the controversy, a former Minister for Aviation and a popular critic of the Muhammadu Buhari administration, Femi Fani Kayode, corroborated the views of the CAN Chairman, claiming on his twitter handle that the suspect is actually Mohammed Nasiru Sani. In the same vein, the Muslim Rights Concern (MURIC) – a well-known Civil Society Organization for Muslims – released a statement through its Director – Prof. Ishaq Akintola – to buttress the fact that by the identity of the suspect, it becomes obvious that terrorism is not the exclusive preserve of a particular religion as wrongly speculated.

There has been back and forth comments, insinuations and controversies, especially on the social media as to the identity and religious inclinations of the suspect. The religious belief of the suspect is not our major concern in this study but the fact that there is actually no effective system of identifying individuals especially for the purposes of investigation, crime prevention and control. In advanced societies, such controversies as to the true identity of the suspect will be needless because in less than five minutes, all his details will be obtained from a central database, instead of relying on what the suspect said at different times during his arrest and interrogation.

The above scenario is made possible by the fact that in the western world biometric information of the citizens are shared between various government agencies. If one violates traffic rules, for instance, the person is booked and the ticket sent to his or her home address or even email. If one commits a crime and the Closed Circuit Television (CCTV) footage is captured, the individual's biometric and other information is captured from a central source for the purposes of arrest and prosecution.

Sadly, the situation in Nigeria has been that government institutions work in isolation, each with its own database often not digitized and that cannot be merged with others. These databases typically contain data entry mistakes as well as duplicate and dead entries causing substantial mis-targeting of beneficiaries and constituting a huge challenge to national security. In the light of

the above situation, it becomes imperative to interrogate the practice of multi-agency collation of similar data in this study as it focuses on data sharing and national security in Nigeria.

Objective of the study

The broad objective of this study is to investigate the nexus between data sharing and national security in Nigeria; an interrogation of the practice of multi-agency collation of similar data. Specifically, the study seeks to:

1. Establish the relationship between multiple biometric capturing and accuracy of biometric information in Nigeria.
2. Ascertain the effect of inter-agency data sharing on crime prevention, investigation and control in Nigeria.

Research Questions

The study provided answers the following research questions.

1. What is the relationship between multiple biometric capturing and accuracy of biometric information in Nigeria?
2. What are the effects of inter-agency data sharing on crime prevention, investigation and control in Nigeria?

Hypotheses

The following hypotheses were formulated for the study:

1. There is no significant relationship between multiple biometric capturing and accuracy of biometric information in Nigeria.
2. Inter-agency data sharing has no effect on crime prevention, investigation and control in Nigeria.

Conceptual Review: Biometric Technology and National Security

Biometrics according to www.searchsecurity.techtarget.com is the measurement and statistical analysis of people's distinctive bodily and social characteristics. The technology is mainly used for identification and access control, or for identifying individuals who are under surveillance. The rudimentary principle of biometric verification is that every person can be accurately identified by his or her inherent physical or behavioral traits. The term *biometrics* was derived from the Greek words *bio* meaning *life* and *metric* meaning *measure*. Wikipedia online dictionary defines biometrics as the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification based on distinct characteristic features. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

As a technological innovation, biometric systems are composed of automated programs that provide identification of various physiological and behavioral characteristics of a person such as fingerprints, retina, signature, etc. Such systems collect data through sensors, build a biometric impression and store it to verify personal traits and characteristics for identification purpose. Whenever a person passes through a biometric check, the system compares the information obtained from that check with the one already recorded during the registration process. For an identification system to be said to be Biometric, it has to possess some properties and must be able of decipher certain things.

One of these properties is that the system must be able to decipher the uniqueness of the features of individuals. The fact is that every person in the world has his or her own unique features, traits and characteristics, and these can never be duplicated as no two individuals in the world have the same features. Not even a set of identical twins or triplets do. No two thumbprints are the same.

Another property that a biometric system should possess is permanence. All the features of a person must be constant over a period of time. The only thing that can alter any feature is if an accident occurred, e.g., the severance of an arm in an accident. A person with no beard when he was registered under a biometric system, but has now grown one after sometime, however, still has the same features underneath the beard. Another feature is Collectability. This means that all the relevant features of an individual must be collectible and collected and measured in quantitative terms.

A Biometric system must also be seen to be credible by not being susceptible to fraudulent manipulations. Some other performance indicators for a biometric system are efficiency and accuracy. A typical biometric system comprises of some components and processes. These include the following:

- **Sensor:** This is a device that collects or detects data or trait, and converts it into a digital format.
- **Signal Processing Algorithms:** These are quality control performers that manipulate the signals received into a biometric template.
- **Data Storage:** The data gotten from the Biometric registration are stored for preservation. From here, it can be retrieved at any time for comparison with the subject being identified.
- **Matching Algorithm:** This refers to the comparison of a newly formed biometric template with the one or more templates created from the previously stored information in data storage.
- **Decision Process:** Results obtained from the matching algorithms are used to make a decision that is either assisted by a person or automated. It is a system level decision.

Some of the techniques of capturing Biometric identification include the following:

- **Facial Recognition:** This is the Biometric system used for the recognition and identification of the human face in order to allow for distinguishing one person from another. Facial expressions are also considered for facial recognition. The area of the face captured in this case include the forehead, the eyes, the ears, the nose, the lips, chin, neck and a little below the shoulder. Pictures and thermals are used for this purpose.
- **Fingerprint Reading:** Each individual possesses a unique set of fingerprints. No two individuals have the same fingerprints. Fingerprints are recognized by the different patterns of ridges, valleys and minutiae points present on the surface of fingers. These are captured with the help of a sensor for each individual for biometric identification purposes.
- **Iris Recognition:** The Iris of each individual also possesses unique patterns and color. A sensor also captures this for Biometric identification purposes. In some very high security areas in Europe and America, access to some sensitive areas can only be made through Iris Recognition.
- **Voice Recognition:** The vocal tract of an individual is also unique. This is why it is easy to know the voice of someone you know talking without seeing that person. A sensor also captures this and it is used mostly for voice recognition and verification.
- **Hand Geometry Recognition:** This is a Biometric technique in which various features of the hand, such as the width of hand and length of fingers are considered for identifying an individual.
- **Signature Recognition:** Identification of an individual is done by analyzing signatures made by every person.
- **Veins Recognition:** One revolutionary Biometric identification system is the use of different patterns of veins in a human body for identification of that person.
- **DNA Matching:** Another revolutionary biometric identification technique used in identifying a person is on the basis of unique characteristics of the DNA of that person.

The concept of national security goes beyond merely the protection of the territorial integrity and sovereignty of a state, it includes all those steps that helps in the elimination of all forms of threat to peace, be it internal or external and covers the prevention of criminal activities like terrorism, armed robbery, kidnapping, banditry, etc. The complexities of today's society make it imperative

that both conventional and non-conventional approaches. A critical component of this non-conventional approach is the use of technology in security operations. All over the world, this fact is widely accepted and practiced in varying degrees.

The use of technology to enhance national security in Nigeria is not lost to the government. For instance, in 2015, the Buhari-led federal government imposed a fine of 1.04 trillion naira on MTN Nigeria, one of its leading mobile telecommunication outfits for failure to deactivate 5.2 million subscribers whose SIM cards were either unregistered or incompletely registered after the expiration of the deadline given by the regulatory body expired. The unregistered SIM cards, according to the government poses great threat to national security as it could be used to perpetrate criminal activities like kidnapping, internet fraud among others.

A key aspect of technology for security operations is biometric technology. With respect to the Nigerian government and MTN, the argument is that it will be difficult to identify individuals who engage in criminal activities using those unregistered SIM cards. Sadly, though, Nigeria does not seem to have a central database that links an individual's biometric features with all his other information including bank accounts, vehicles, office address/work history, as well as travel information, crime records, etc.

The visa ban on certain categories of Nigerian immigrants to the United States of America can also be traced to the US government's inability to access critical data about Nigerian travelers. This information exists but is not harmonized and certainly cannot effectively be shared among government agencies, thus, necessitating the conduct of this research to fashion out possible modalities of how they can be properly harnessed for security reasons.

Empirical Review of Literature

Empirical studies abound on how national security can be enhanced and improved upon using technology. For instance, Nwanga, Onwuka Aibinu and Ubadike (2014) whose study titled; leveraging big data in enhancing national security in Nigeria argued that the recent successes recorded by terrorist elements in Nigeria have been attributed to lack of actionable intelligence that would enable preventive action against terrorists. To successfully defeat terrorism in Nigeria, the paper advocates for a collaborative information gathering, analyzing and sharing system among the security agencies in Nigeria through Big Data Center. The framework should consist of Military Agencies from Ministry of Defense, Paramilitary Agencies from Ministry of Interior, Big Data Center, National Communications Commission, Nigerian Communication Satellite Limited (NIGCOMSAT) and Network Operators from Ministry of Information and Communication Technology. The paper concludes that technology will greatly enhance the efforts of security agencies in the fight against terrorism and to secure the life and property of the citizenry.

Also, Adams (2016) investigated the role of information technology in National Security, a case study of Nigeria. Using the simple random sampling technique, the researcher selected a sample of 150 respondents from six different government parastatals namely Federal Ministry of Defense, Federal Ministry of Science and Technology, National Defense College, Defense Headquarters, the Police Force headquarters and National Information Technology Development Agency (NITDA). Data was collected using structured questionnaire. Findings from the study revealed that a great number of the officers in the Nigerian military and other security agencies believe that IT can be of great impact in National Security so therefore there is a great relationship between Information technology and National security.

Finally, in their study on the role of Information and Communication Technology (ICT) in combating corrupt business activities in Nigeria, Ayuba and Aliyu, (2014), sampled 200 respondents to generate data for their study. The analysis of the data was conducted using Descriptive Statistics and chi-square to test the formulated hypotheses which reveal that ICT helps in reducing organizations spending and increases earning, identification of ghost workers and elimination of corrupt practices, as well as enhancing marketing practice and tracking of financial fraudsters and other fraudulent banking services which significantly helped in achieving greater transparency, accountability and effective management as well as reducing opportunities for corruption. Some recommendations were made, among the major recommendations is the need for business organizations (public and private) in Nigeria to ensure adequate provision of ICT infrastructure such as access to computers and capacity to connect to the internet globally and the need to ensure massive involvement of local communities in the ICT derive in the country.

Methodology

The study was carried out in Ogun State, South West Nigeria and adopted the descriptive survey research method as the research design for the study. Data for the study was obtained through primary and secondary sources and the organizations of focus in this study is the Ogun state command of the Nigerian Police force, the National Identity Management Commission and Selected Mobile Network Providers in Ogun state Nigeria with a total population of 355 respondents, from where a sample of 188 was obtained using Taro Yamani Formula. The data collection instrument for the study was a questionnaire structured on a five-point

Likert scale to elicit information from the respondents. Data obtained from the respondents was presented in table and analyzed using frequency counts and mean scores and the hypotheses were tested using Pearson correlation at 0.05 level of significance.

Data presentation, Analysis and Test of Hypothesis

Data for this study was presented and analyzed according to the research questions and hypotheses formulated for the study. We begin with the first research question.

What is the relationship between multiple biometric capturing and accuracy of biometric information in Nigeria?

Answers to the above research question will be presented in table 1 below and analyzed accordingly.

S/N	QUESTIONS	ΣFx	X	Decision
1	Government agencies require their individual database because information sought are unique and peculiar to the organization and cannot be applied to others.	420	2.9	Disagreed
2	Multiple collation of similar information is a waste of time both for government and its agencies and the citizens supplying the data.	492	3.4	Agreed
3	There is hardly any mechanism for verification of the data provided by a single individual to different Ministries, Departments and Agencies of government.	489	3.4	Agreed
4	Inaccurate biometric data is dangerous to national security.	541	3.8	Agreed
5	People are wont to manipulate their biodata information at different times to suit the particular purpose for which their information is being sought.	520	3.6	Agreed
6	Accurate data aids in crime prevention, investigation and control. .	531	3.7	Agreed

Source: Field Survey, 2020

The table above presents the responses of the respondents to the issues in the first objective of the study. With six statements in the table, respondents agreed to all but one of the assertions. The first statement tries to provide a justification as to why government agencies need to capture the same data at multiple times but the respondents disagreed to the view that government agencies require their individual database because information sought are unique and peculiar to the organization and cannot be applied to others. By implication, data sharing can still address the issues of uniqueness and peculiarity of the nature of the data. The remaining statements received positive reviews as the respondents agreed that multiple collation of similar information is a waste of time both for government and its agencies and the citizens supplying the data. Again, there is hardly any mechanism for verification of the data provided by a single individual to different Ministries, Departments and Agencies of government. With this, there is bound to be distortions and manipulation of information because people are wont to manipulate their biodata information at different times to suit the particular purpose for which their information is being sought. This trend, if allowed to fester is dangerous because inaccurate biometric data is dangerous to national security and accurate data aids in crime prevention, investigation and control.

Test of hypothesis one: There is no significant relationship between multiple biometric capturing and accuracy of biometric information in Nigeria.

Correlations

		Multiplicity of Biometric Data Capturing	Accuracy of biometric information
Multiplicity of Biometric Data Capturing	Pearson Correlation	1	-.328
	Sig. (2-tailed)		.059
	N	142	142
Accuracy of biometric	Pearson Correlation	-.328	1

information	Sig. (2-tailed)	.059	
	N	142	142

In the test of the first hypothesis, the analysis shows that the probability value (0.059) is greater than the alpha value (0.05), the researcher therefore accepts the null hypothesis and concludes that there is no significant positive relationship between multiple biometric capturing and accuracy of biometric information in Nigeria, with a correlation value of -0.328.

Research question two: What are the effects of inter-agency data sharing on crime prevention, investigation and control in Nigeria?

Answers to the above research question will be presented in table 2 below and analyzed accordingly.

S/N	QUESTIONS	ΣFx	X	Decision
7	Government agencies using shared database exposes such information to manipulation and abuse.	355	2.5	Disagreed
8	Information sharing in the banking sector has improved not just service delivery, but customers' satisfaction.	557	3.9	Agreed
9	Information sharing by government agencies can help to improve public service delivery.	468	3.2	Agreed
10	Shared information leads to shared responsibility and better effectiveness.	467	3.2	Agreed
11	Security agencies, in the investigation of crime harvest data from telecommunication companies and banks, thus lending credence to the importance of inter-agency information sharing in the polity.	567	3.9	Agreed
12	Inter-agency information sharing fast tracks the dispensation of justice through speedy investigation and trials.	449	3.1	Agreed

Source: Field Survey, 2020

The issues of how data sharing among government agencies can enhance crime prevention and control is the focus of the second specific objective of this study as well as the second research question and hypothesis. Here, the respondents also agreed to all but one of the statements in table 2. The idea that government agencies using shared database exposes such information to manipulation and abuse was disagreed to by the respondent as they agreed to the fact that in the banking sector, information sharing has improved not just service delivery, but customers' satisfaction and that information sharing by government agencies can help to improve public service delivery. Respondents are also of the view that security agencies, in the investigation of crime harvest data from telecommunication companies and banks, thus lending credence to the importance of inter-agency information sharing in the polity. By implication the responses of the respondents show that in this ICT age, information sharing is necessary for national security.

Test of hypothesis two: Inter-agency data sharing has no effect on crime prevention, investigation and control in Nigeria.

Correlations

		Inter-agency data sharing	Crime prevention, investigation and control
Inter-agency data sharing	Pearson Correlation	1	.781
	Sig. (2-tailed)		.036
	N	142	142
Crime prevention,	Pearson Correlation	.781	1

investigation and control	Sig. (2-tailed)	.036	
	N	142	142

In the test of the second hypothesis, the analysis shows that the probability value (0.036) is less than the alpha value (0.05), the researchers therefore reject the null hypothesis and conclude that inter-agency data sharing has an effect on crime prevention, investigation and control in Nigeria, with a correlation value of 0.781.

Conclusion and Recommendations

The study has been an empirical inquiry on data sharing and national security in Nigeria, an interrogation of the practice of multi-agency collation of similar data. In drawing this academic exercise to a close, it becomes pertinent to state that Nigeria's experience on data management have not been a good one. Even our population figure is questionable because all the demographic features that goes with population studies are based on estimates. The current sanction from the United States government is supposed to provide the needed impetus to overhaul our data management system for better performance and to enhance national security. To achieve this, the following recommendations are necessary.

1. The Nigerian government should set modalities in place to begin to harmonize existing data and to extend the reach and coverage of the citizens in order to create a robust database for effective policy planning, security and provision of social services.

2. Appropriate legislative and policy framework should be put in place to criminalize all forms of fraudulent biodata falsification by individuals and groups. Also, stringent measures should be put in place to discourage all forms of fraudulent alteration of sensitive biodata information like date of birth, names etc.

REFERENCES

Abang, M. (2015). *Nigeria may Harmonise Biometric Data*. IT-Telecom Digest (online Newspaper) of Tuesday, 13 October, available online at https://ittelecomdigest.com/nigeria-may-harmonise-biometric-data

Adamolekun, L. (2009). *Public Administration: Nigeria and Comparative Perspective*. London: Longman

Adams, O. (2016). The role of Information Technology in National Security: A Case Study of Nigeria. *Global Journal of Computer Science and Technology*. 16 (3): 6 – 14.

Adekanye, A. (2006). 'Information and Communication Technology.' In Asaju, D. (ed.) *Readings in General Studies*. Lagos: Lagos State University Press.

Asika, N. (2006), *Research methodology in the behavioural sciences*, Lagos: Longman Nigeria.

Ayuba, B. & Aliyu, I. (2014). 'The Role of Information Communication Technology (ICT) in Combating Corrupt Business Activities in Nigeria.' *IOSR Journal of Business and Management*. 3 (16): 07 - 14.

Francis, N. & Ojo, A. (2015). 'Challenges and Prospects of Implementing E-Governance in Nigeria.' In *2nd Covenant University Conference on E-Governance in Nigeria (CUCEN 2015)* June 10-12, 2015, Covenant University Canaanland, Ota Ogun State, Nigeria.

Nwanga, M., Onwuka, E., Aibinu, A., and Ubadike, O. (2014). Leveraging big data in enhancing national security in Nigeria. *International Journal of Knowledge, Innovation and Entrepreneurship*. 2 (2): 66—80

Ogedebe, P. and Babatunde, P. (2012). The role of Information Technology in combating security challenges in Nigeria. *Academic Research International*. 2 (1): 124 – 130. Available online at www.journals.savap.org.pk