International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 18-02-2023, Accepted: 07-03-2023, Published: 21-03-2023
Volume 5, Issue 1, 2022, Page No. 86-91

Upsurge in cybercrimes in Nigeria. The need for a centralized database

Dr. Kingsley Omote Mrabure
Ph.D, Associate Professor, Department of Public Law, Faculty of Law, Delta State University, Abraka, Nigeria

Abstract
The urgent need to combat the menace and challenges of cybercrimes is based on the fact that Nigeria has been ranked third in global internet crimes. According to the Information Security Society of Nigeria (ISSAN), 25 percent of Nigeria's cybercrimes are unsolved, while Nigerians account for 75 percent of the world's hackers. Customers in Nigeria lost around 6 billion naira to cyber thieves in 2014, according to the EFCC. Between 2000 and 2013, Nigerian banks lost around 159 billion naira to electronic fraud and cybercrime, with substantial implications for the country's economy and cashless policy. These scenarios vividly portray the need to take drastic measures for a functional central or unified or national database as Nigeria is making significant strides in terms of access and usage of information and communication technology (ICT) in combating the upsurge and menace of cybercrimes.

Keywords: curtailing cybercrimes in Nigeria, information and communication technology, lack of centralized data base, impediment, nation's economy

Introduction

The term 'database' is usually used with regard to computers. It is defined as a "large body of information stored in a computer which can process it and from which particular bits of information can be retrieved as required". [1] It operates like an electronic filing system. Governments and private entities maintain central data warehouses or database (big data) that host large amount of personal data. These data warehouses are not physical warehouses that can be seen or perceived. They are usually imaginary and sometimes in a cloud which hosts volumes of data. Central data warehousing brings about economies of scale. It also facilitates data processing and makes data management more efficient and effective. [2]

With computers and the internet, data bases are increasingly fed with personal information for storage purposes. Personal information is an extremely valuable commodity which has been aptly described as the lifeblood and basic currency of the information economy. [3] The importance of personal data in the information society has made the innovation of new ways to facilitate its exploitation an increasingly attractive venture. These innovations have been made easy with the advances in technology, particularly, Information Technology (IT) which has made it very easy to accumulate vast amounts of personal data with very little effort, for example by the mere click of a mouse. [4]

A functional central or national or unified database, though presently non-existent in Nigeria, is needed to combat the menace of cybercrimes contained in the Nigerian Cybercrimes Act [5] such as identity theft, [6] child pornography offences, [7] cyber stalking, [8] cybersquatting, [9] the distribution of racist and xenophobic material [10] to the public through a computer system or network (e.g. Facebook and Twitter) and a host of other offences.

The urgent need to tackle cybercrimes stems from the fact that Nigeria is ranked third_ in worldwide online crimes [11], trailing only the United States of America and the United Kingdom. According to the Information Security Society of Nigeria (ISSAN), 25 percent of cybercrimes in Nigeria go unsolved, and Nigerians account for 75 percent of the world's hackers [12]. Customers in Nigeria lost roughly 6 billion naira to cyber thieves in 2014, according to the EFCC, while NDIC (2015) recorded [13] an 183 percent rise in the use of the e-payment platform in Nigerian banks.

In a related development, the CBN (2015) research revealed [14] that electronic channels were used in 70% of attempted or successful fraud/forgery incidents in Nigeria's banking sector. Between 2000 and 2013, Nigerian banks lost around 159 billion naira to electronic fraud and cybercrime, with substantial implications for the country's economy and cashless policy. Nigeria is making tremendous strides in terms of access and use of information and communication technology [15] (ICT), the following examples vividly show the need to take severe efforts for a functional central or unified database.

In lieu of the above, this paper discusses instances of cybercrimes, institutions with databases in Nigeria, the problems with the operation of different databases in Nigeria, a comparative study, lessons derived therein for effective eradication of cybercrimes in Nigeria and the need to have a national database.

Instances of cybercrimes

Despite holding a diploma in computer technology, Elekwe, [16], a chubby-faced 28-year-old man gained a fortune through the fraud after two years of joblessness. The leader of a fraud ring in a business centre persuaded him to Lagos from Umuahia. From his exploits, he owns three elegant automobiles and two homes.

Security agencies in Ghana arrested four Nigerians suspected of running a "419" scam on the internet to defraud unwary Western investors in July 2001[17]. Prospective investors are believed to have lost several millions of dollars as a result of their actions. Two young lads were recently detained after purchasing two laptops listed on a woman's website under false pretenses [18]. Government officials apprehended them at the moment of delivery.

Mike Amadi was sentenced [19] to 16 years in jail for creating a website that advertised lucrative but fictitious procurement contracts. An undercover agent posing as an Italian businessman caught the him impersonating the EFCC Chairman.

Amaka Anajemba, who was sentenced [20] to 212 years in prison, perpetrated the largest international con of all. She was also sentenced to refund $25.5 million of the $242 million she helped a Brazilian bank steal. In one recent internet scam case [21], a 24-year-old Nigerian woman named Yekini Labaika and a 42-year-old American nurse named Thumbelina Hinshaw were looking for a Muslim boyfriend to marry.The young man claimed to be an American Muslim named Philip Williams who worked for an oil business in Nigeria and promised to marry the victim. He invented dubious methods to defraud the victim of $16,200 and numerous expensive goods. After being found guilty of eight crimes. the fraudster was sentenced to a total of 19½ years in prison. These types of incidents are becoming more common.

Several young guys continue to effectively carry out these illicit crimes, robbing trusted persons and institutions.

Institutions with databases in Nigeria

Public data controllers include government and its numerous department and agencies that process individuals' personal information. The data processing activities of the government that will be discussed here are data collected and used by the Nigerian Communications Commission (NCC), the Independent National Electoral Commission (INEC) and the Nigerian Identity Management Commission (NIMC) and a host of others.

1. Nigerian communications commission (NCC) sim card registration exercise

The NCC in 2010 introduced a compulsory registration scheme for users of the subscribers identity module (SIM) cards in Nigeria. [22] The scheme was adopted so as to create a credible database to ease identification of criminals as a result of concerns from security agencies. [23] Subscribers' personal information such as facial photograph and other biometric data (like fingerprints) were collected. [24] Subscribers were also required to present identification documents such as e-passports, company Identity cards (ID) with tax/pension numbers, student ID cards from recognized institutions and drivers' licenses. The SIM card registration was made compulsory for all subscribers as unregistered SIM cards were to be disconnected from the networks. [25]

2. Independent national electoral commission's (INEC) voters registration exercise and the permanent voter card (PVC)

Based on its mandate as the primary electoral body in Nigeria, INEC collects personal data of individuals. [26] Personal information like voters' names, addresses and biometric data is collected for the purpose of voter's registration and stored in INEC'S database using computers and direct data capturing (DDC) machines. [27]A personal voter's card (PVC) is subsequently issued which contains these details which enable a citizen to vote if his/her personal data matches what is stored in INEC's database.

3. Nigerian identity management commission (NIMC) national identity card scheme

The Nigerian President launched a new e-ID (Electronic Identity) card which doubles as a national ID card and an automated teller machine (ATM) card. [28] The card is to be used for identification and electronic signature (e-signature) purposes. Implementation of the project was to be in phases. [29] The project has been lauded for preventing data from collected by different bodies at the same time as it is a unified biometric database. [30] The project is still on going as it has taken many years to accomplish it.

4. Federal road safety corps (FRSC drivers' license)

In February 1988, the Federal Government established the Federal Road Safety Commission. [31] Its responsibilities include creating and generating driver's licenses for various kinds of vehicle operators, as well as setting the standards that must be met by a driver's license application from time to time. In processing a driver's license, personal information such as names, addresses and biometric data are collected and stored in FRSC's database using computers and direct data capturing (DDC) machine. A driver's license is subsequently issued which contains these details.

5. Nigerian immigration service (international passport)

Since its separation from the Nigerian Police Force (NPF) in 1958, the Nigerian Immigration Service (NIS) has undergone numerous changes. The Immigration department was created by an Act of Parliament on August 1, 1963. [32] In processing an international passport, personal information such as names, addresses and biometric data is collected and stored in NIS's database using computers and direct data capturing (DDC) machine. An international passport is subsequently issued which contains these details.

Data are collected from Nigerians and non-Nigerian Immigrants at the borders and the ports of the country. Data details include information on the profile of the traveller to Nigeria such as, the origin of his/her journey, the purpose of visit, and the length of stay in Nigeria, the mode of transportation. For the emigrant, information is sought on the profile, mode of transportation and the destination. Data are collected on immigration and emigration forms on a daily basis.

Private data controllers

The activities of private data controllers to a large extent are usually regulated by specific governmental bodies assigned by statute to do so.

1. Banking sector: BVN and KYC schemes

Banks and other financial institutions, through their numerous activities, accumulate large amount of personal data. Quite recently, the Central Bank of Nigeria (CBN), in collaboration with the Bankers Committee, launched the Bank Verification Number (BVN) project a key component of the know-your-customers (KYC) policy of the banks. [33] This project aims to curb fraud in the financial sector. [34] Hence, all bank customers must be issued a unique identity (BVN) which can be verified across the banking industry. The exercise involves the collection of personal data, including photographs and other biometric data. This is a compulsory exercise which must be carried out by banks and there are substantial penalties for a bank that fails to comply. [35] Banks in Nigeria also carry out KYC functions

at regular intervals. KYC is a process used by banks to identify and get more acquainted with their customers. Personal data of customers are therefore updated regularly through this process.

Problems with the operation of different databases in Nigeria

According to Awodokun, [36] the problem for a centralized or unified database persists because data is collected and stored everywhere, making it difficult to glean information across multiple government parastatals databases that house these data. He adds [37] further that the reason for this ambiguity is an obvious one because when different government agencies and parastatals have their own IT systems with no shared synchronization, the result is monotony and inaccuracies. He concludes by stating [38] that with the data sitting in different silos, it is hard to derive analytical insights or information for social-economic purposes since we are only seeing a part of the picture with every single database. As it is obvious that the government cannot trust or rely on the data collected so far, it is not surprising that government has to invest much needed human and capital resources on new data project or schemes. The government is spending billions of naira on several data collection and registration exercises, which stakeholders say amounts to redundancy and waste of human and financial resources.

On his part, Olusola opines [39] that the cost of these exercises is increasing because Nigeria suffers from a science-technology deficit, where adoption of technology is done from different sources and no collaborative thought is given to the national outcome. The establishing of a centralized database (sometimes abbreviated CDB) is the key towards the harmonization of different databases in Nigeria. The office of the National Security Officer should champion this cause towards reducing the incidences of cybercrimes.

The CDB is a database that is stored, accessed, and maintained in one place. A central computer or database system, such as a desktop or server CPU, or a mainframe computer, is frequently used in this location.

An organization or institution would most likely use a centralized database. Users connect to a centralized database via a computer network that allows them to access the central CPU. All of the data on the CDB is accessible from a variety of different locations.

The speed and potency of modern information technology, on the other hand, makes computer crime detection and investigation more difficult [40]. Communications networks, for example, now span the world, and a modest personal computer can link to sites in different hemispheres or continents with ease. Despite the foregoing, the need for a national data base is still justified for the reasons indicated below.

This aids in the maintenance of data as accurate and consistent as possible and improves data reliability; generally better data security as the single data storage location implies only one possible place from which the database can be attacked and sets of data can be stolen or tampered with; better data preservation than other types of databases due to often-included fault-tolerant setup; easier for end-users to use due to the simplicity of having a single datum storage location; There exist institutions with databases in Nigeria such as Federal Road Safety Corps, Nigerian Immigration Service, Independent National Electoral Commission, Nigerian Communication Commission and others. Despite the numerous databases being maintained [41] by various government agencies, information is not shared amongst them, thereby militating the fight against cybercrimes. Arguably, could it just be to add figures to their yearly annual budget?

However, there exist no national or centralized or unified databases which ought to be coordinated by the office of the National Security Adviser (NSA) as provided under the CBA. This could serve as a means of monitoring perpetrators of cybercrimes by checking into their personal data and tracing their movement and apprehending them. A careful perusal of some provisions of the CBA attests to this.

Despite the establishment of a fund, known as the National Cyber Security Fund provided under section 44 CBA with funds accruing from electronic transactions by businesses, grant-in-aid and assistance from donors, bilateral and multilateral agencies; all other sums accruing to the fund by way of gifts, endowments, bequest or other voluntary contributions by persons and organizations; monies as may be appropriated for the fund by the National Assembly; and all other monies or assets that may, from time to time accrue to the fund, the office of the NSA is yet to establish and maintain as provided under section 41 CBA, a National Computer Emergency Response Team (CERT), Coordination Centre responsible for managing cyber incidences in Nigeria; and a National Computer Forensic Laboratory and also to coordinate utilization of the facility by all law enforcement, security and intelligence agencies and establish appropriate platforms for Public Private Partnership (PPP).

The office of the NSA needs to take proactive steps to comply with the provisions of section 41 stated above. It must take the lead in the fight against cybercrime, as stipulated in section 41, which states that the National Security Adviser's office shall be the coordinating body for all security, intelligence, law enforcement, and military services in Nigeria in order to prevent and combat cybercrime; ensure the formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria.

As laudable and encompassing the above provisions of the CBA are, the office of the NSA is yet to actively coordinate and collaborate with public institutions and private bodies with databases respectively. The office of the NSA should deploy the necessary funds provided under section 44 CBA in establishing a central or national database; establishment of a National Computer Emergency Response Team (CERT) and a National Computer Forensic Laboratory so that it can make the extant provisions of the law practicable.

Further, under section 43 CBA, it is provided that the Cybercrime Advisory Council shall establish a programme to award grants to institutions of higher education to establish Cyber Security Research Centres to support the development of new cyber security defences, techniques and processes in the real-world environment; and promote graduate traineeships in cyber security and computer and network security research and development.

The above provisions of the CBA, though commendable and insightful are yet to see the light of the day in the fight against cybercrimes in Nigeria as these provisions are passive. The Cybercrime Advisory Council should earnestly

also make use of and intensify the use of surveillance technology. Security challenges today have made governments increase their investments in surveillance technologies that have the capabilities of capturing and analyzing digital footprints. [42] This is in order to combat contemporary criminal activities such as cyber terrorism. [43] This does not, however, mean that private entities are not involved in accumulating personal data using surveillance technologies. It is very rare today to enter a grocery store, bookshop, or bank without one form of surveillance device or another. Employers also monitor their employees using these technologies.

There are different types of surveillance; which include physical surveillance, psychological surveillance and data surveillance. [44] There are various types of surveillance technologies that can be deployed for this purpose. The most prevalent surveillance tool nowadays is the closed circuit television (CCTV). [45] Originally, video camera technology was a mild system of collection of personal data. This is because the product of their monitoring was to a larger extent, based on human interpretation. [46] Digital technology has now changed video surveillance. It is a tool of intelligence not just to record, but also to analyze data, independent of human inputs, based on specified rules of the programmer. [47]

Many countries are therefore increasing and improving their surveillance programmes for security purposes. [48] Nigeria should be part of this trend. Surveillance technologies are also usually combined with the internet to produce a very powerful tool of accumulation and storage of personal information. This is carried out using some of the internet monitoring devices and invasive devices such as Fin Fisher [49] which enables governments and private persons to be able to monitor users' activities on the internet.

Comparative study

The United States

The Federal Bureau of Investigation (FBI) sponsored the creation of a forward-thinking agency to aggressively fight cybercrime even before it was recognized as a substantial criminal and national security problem. In 1997, the National Cyber-Forensics and Training Alliance (NCFTA) was founded [50].It has become a global model for bringing law enforcement, private sector, and academia together to develop and exchange resources, strategic information, and threat intelligence in order to identify and stop potential cyber threats and mitigate existing ones. The NCFTA has developed since its inception [51] to keep up with the ever-changing cybercrime scenario.

Currently, the organization is dealing with threats from transnational criminal organizations such as spam, botnets, stock manipulation schemes, intellectual property theft, pharmaceutical fraud, telecommunications scams, and other financial fraud schemes that cost companies and consumers billions of dollars. The NCFTA gathers information from hundreds of commercial sector NCFTA members, NCFTA intelligence analysts, Carnegie Mellon University's Computer Emergency Response Team (CERT), and the FBI's Internet Crime Complaint Center.

CIRFU has used its broad knowledge base to play a crucial strategic role in several of the FVI's most critical cyber cases in recent years [52].In order to stay up with the ever-changing world, and the growing menace of cybercrimes, laws have been enacted in succession to curtail the nefarious activities of perpetrators of cybercrimes. The first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 (CFAA). In 1986, Electronic Communications Privacy Act (ECPA) was an amendment to the Federal Wiretap law. In 1996, National Infrastructure Protection Act was enacted. This was followed in 1998 and 1999 by the enactment of Digital Millennium Copyright Act (DMCA) and Cyberspace Electronic Security Act respectively. The Patriot Act was passed in 2001 and Cyber Security Enhancement Act (CSEA) was passed in 2002. The Anti-Phishing Act of 2005 introduced two new felonies to the United States Code. Furthermore, the Obama Administration produced a cyber security study and strategy in 2009, which culminated in the passage of the Cyber Security Act of 2010, which enhanced public-private collaboration on cyber security concerns. In the United States, a number of agencies have been established.

The FBI, the National Infrastructure Protection Center, the National White Collar Crime Center, the Internet Fraud Complaint Center, the Department of Justice's Computer Crime and Intellectual Property Section, the Department of Justice's Computer Hacking and Intellectual Property Unit, and Carnegie-Computer Mellon's Emergency Readiness Team/Coordination Center (CERT/CC), among others, are all working to combat cybercrime.

To aid in the investigation of cybercrime, the FBI has established specific technical units and developed Carnivore, a computer surveillance system that can intercept all packets sent to and from the ISP where it is located.

Lessons for Nigeria

The principal law on cybercrimes in Nigeria which is the CBA is adequate in the fight against incidences of cybercrimes in Nigeria. However, the major hindrance is in implementing the spirit and letters of the law governing cybercrimes. The various bodies that have been assigned certain functions by the CBA are failing woefully in carrying out their ascribed functions as stipulated under the CBA. For instance, coordination and utilization of the facility envisaged by the law such as the establishment, provision, maintenance of a National Computer Emergency Response Team (CERT), the National Cyber Security Fund, a national Computer Forensic Laboratory by all law enforcement, security and Intelligence agencies and establish appropriate platforms for Public Private Partnership (PPP) have not been realized or at most at an abysmal implementation level.

Huge financial funds must be deployed by the office of the NSA to accomplishing the fight against the menace of cybercrimes since it is highly capital intensive. It involves the acquisition of highly modern sophisticated gadgets and equipment. The above shortcomings of the office of the NSA is at variance with the active roles played by the FBI in the United States in combating the alarming ever rising menace or incidences of cybercrimes. Succinctly, the office of the NSA, Cybercrime Advisory Council need to be pro-active in effectively carrying out their prescribed functions under the CBA in the fight against cybercrimes in Nigeria as evident by FBI's roles in this-regards in the United States.

Conclusion

Without prevarication, there is upsurge in the incidences of cybercrimes in Nigeria. Therefore, this evil menace of cybercrimes must be tackled headlong bearing in mind the

enormous responsibilities of the office of the National Security Adviser to establish a unified or national database and coordinate and partner other relevant bodies in curtailing the upsurge and scourge of cybercrimes in Nigeria. The office of the NSA and the Cybercrime Advisory Council must rise up to the challenges by doing the imperatives provided under the CBA. They should take a cue from the resilient, persistent and pro-active roles of the FBI in the United States in the fight against perpetrators of cybercrimes.

References

1. IJ Lloyd Information Technology Law (Oxford University Press: 390 quoting Concise Oxford Dictionary, 2014.
2. Bergkamp L. 'The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy', Computer Law Security Report,2002:18(1):32.
3. Robison N, *et al.* 'Review of the European Data Protection Directive' (Technical report) Rand Corporation, 2009, 12. available <http://www.rand.org/pubs/technical/_reportsTR710.html> accessed 6 October 2022, The authors adopted the word 'currency' of the internet economy' from OECD Ministerial Meeting on the Future of the Internet Economy'<http:www.oecd.org/document/8/0.3343.en2649_34487_40863240_1_1_1_1.000.html>accessed 7 January 2023.
4. Kuner C. 'An International Legal Framework for Data Protection: Issues and Prospects', Computer Law and Security Review,2009:25(4):308.
5. The Cybercrimes Act became Law in 2015. It shall simply be referred to as "CBA" in the context of this article.
6. Section 22 CBA imposes punishment of imprisonment for a term of 10 years or a fine of not less than ₦7 million or to both fine and imprisonment.
7. Section 23 CBA provides for punishments of imprisonment for a term of 10 years or a fine of not less than ₦20 million or to both fine and imprisonment, depending on the nature of the offence and the act carried out by the accused persons. Offences include, amongst others: producing, procuring, distributing, and possession of child pornography.
8. Section 24CBA.
9. Section 25 CBA. This is registering or using an Internet domain name with bad faith intent to profit from the goodwill of a trade mark belonging to someone else, or to profit by selling to its rightful owner. Individuals who engage in this are liable on conviction to imprisonment for a term of not less than 2 years or a fine of not less than ₦5 million or to both fine and imprisonment.
10. Section 6 CBA.
11. Nigeria Losses ₦127b Annually to Cyber Crime available at http://dailypost.ng/2017/03/08/nigeria-losses-n127b-annually-cyber-crime-buhari%E2%80%8E/ accessed March 4 2023.
12. *Ibid*
13. *Ibid*
14. *Ibid*
15. Odufuwa F. 'What is Happening in ICTs in Nigeria. A Supply and Demand Side Analysis of the ICT Sector' (2012). See also Owasanoye B, Akanle O, 'ICTs, Freedom of Information and Privacy Rights in Nigeria, A Legal Analysis', East African Journal of Peace and Human Rights,2010:16(1):99-123.
16. Ibikunle F, Odunayo E. Approach to Cyber Security Issues in Nigeria: Challenges and Solution <oaji.net/articles/2014/1014-1404316951.pdf> accessed March 5 2023.
17. *Ibid*
18. *Ibid*
19. *Ibid*
20. *Ibid*
21. It was reported on Sunday Punch newspaper of July 16, 2006.
22. Obute PC. 'ICT Laws in Nigeria: Planning and Regulating a Societal Journey into the Future', Potchefstroom Electronic Law Journal, 2014, 438.
23. See Nigerian Communications Commission (NCC) SIMRegistration<http://ww.ncc.gov.ng/index.php?option=comcontent&view=article&id-122&Itewid=113> accessed 9 January 2023.
24. Izuogu CE. 'Data Protection and other Implications in the ongoing SIM Card Registration Process' <http:papers.ssrn.com/sol3papers.cfm?abstractid=1597665> accessed 3 November 2022.
25. NCC (n. 23 above).
26. Section 153 (1); 3rd schedule part 1, Constitution of Federal Republic of Nigeria 1999 as amended. See also 'About INEC' <http://www.inecnigeria.org/?page_id=14> accessed 25 October 2022.
27. DDC machines are devices used to collect personal data of voters in the registration process. The main information it collects are photographs and fingerprints of voters. A DDC is used to prevent multiple voter registration and to remove ghost voters by looking for duplicates of the fingerprints recorded in the registration process. See Human Rights Watch (HRW) 'The Role of the Independent National Electoral Commission (INEC)' <http:..www.hrw./org/legacy/backgrouder/africa/nigeria0407/5.htm>accessed 23 December 2022.
28. Olagunju T. 'Mr President and the National Assembly:Data Protection for Nigerians First'<http://saharareporters.com/2014/09/02/mr-president-and-natioanl=assembly-data-protection-nigerians-first>accessed 7 November 2022.
29. About 13 million Nigerians were to be issued the card in the first phase and an estimated 100 million for the second phase.
30. Oguntimehin J. 'Implications of Nigeria's National ID card' <http://www.iafrikan.com/2014/09/30/nigeria-national-id-card/#sthash.aDBRkrnA.dpuf>accessed 8 January 2022.
31. Through Decree No.45 of the 1988 as amended by Decree 35 of 1992 referred to in the statute books as the FRSC Act cap 141 Laws of the Federation of Nigeria (LFN), passed by the National Assembly as Federal Road Safety Corps (establishment) Act 2007.
32. Cap 171, Laws of the Federation Nigeria.
33. Udo B. 'CBN Sets New Deadline for Bank Customer's Verification' PremiumTimes<http://www.premiumtimesng.com/business/169879-cbn-sets-new-deadline-for-bank-

customers-verification.html>accessed 4 December 2022.

34. Central Bank of Nigeria Introduces Bank Verification Number (BVN)' http://nairabrains.com/2014/10/central-bank-of-Nigeria-introduces-bank-verification-number-bvn/accessed 27 February 2023.
35. For example, suspension of services on a customer's account. The CBN has also directed banks to honour transactions from ₦100 million and above, only from customers with BVN from March 2015. The directive is contained in the CBN's 'Circular on the acceleration of bank verification number (BVN) project,' <http:www.cenbank.org/OUT/2014/BPSD/CIRCULAR%20on%20ACCELERATION%20ON%20BVN2.pdfaccessed 3 January 2023.
36. G Awodokun, 'A Simple Solution to Nigeria's Unified DatabaseProblem'<http://techpoint.ng/2018/03/14unified-database-nigeria/>accessed 18 November 2022.
37. *Ibid.*
38. *Ibid.*
39. How Nigeria Wastes Billions on Data Capturing<http://guardia.ngtechnology/how-nigeria-wastes-billions-on-dat-capturing>accessed 18 January 2022. The President, Association of Telecommunications Companies of Nigeria (ATCON), Olusola Teniola, in an interview with The Guardian, noted that the multiple exercises indicate a lack of a data template required to capture the different types of information sought by each agency and company in the case of BVN and SIM registrations.
40. Ibikunle, Odunayo supra n.16.
41. Awosanya Y. 'Unified Database-Nigeria Worse not Getting Rose'<https://techpoint.ng/2015/03/03/unified-database-nigeria-worse-not-getting-rose/>accessed 5 October 2022.
42. Craig T. ME Ludloff Privacy and bigdata O'Reilly: Sebastopol, 2011, 7.
43. *Ibid.*
44. See A Westin Information Technology in a Democracy. Lloyd (n.1 above)
45. *Ibid.*
46. Lessig L. Code 2.0, Basic Book New York,2006, 207.
47. *Ibid*.eg, the CCTV camera installed in major streets in London captures vehicles number plates and is able to link the number plate with the owner of the vehicle. Another example is the facial recognition cameras used for law enforcement purposes.
48. The UK, for example, has more 14 million surveillance cameras installed in different locations which mean approximately 1 for every 4 inhabitants. See Lloyd (n.1 above). In the US, surveillance technologies are also heavily relied upon for law enforcement purposes. See Craig and Ludloff (n.42 above). The use of surveillance technology is also growing in African countries. Recently, the Nigerian government signed an agreement with a Chinese telecommunication firm – ZTE – to install about 2000 solar powered CCTVs within the Federal Capital, Abuja and Lagos. Abuja and Lagos were selected to host the pilot projects aimed at closely monitoring and uncovering possible threats to public security through the CCTV cameras. 'Abuja: Where are the CCTV cameras?' available at http://www.thisdaylive.com/articles/abuja-where-are-the-cctv-cameras-/141195/>accessed 1 January 2023.
49. This is a sophisticated spying software which can remotely monitor webmail and social networks in real time and collect encrypted data and communications of unsuspecting targets. It is mostly used by law enforcement agencies. It has been said that it is being abused by governments around the world.
50. Cyber Crime, available at https://www.fbi.gov/investigate/cyber>accessed 19 October 2022.
51. *Ibid.*
52. *Ibid*