ADDRESSING LEGAL ISSUES IN THE USAGE OF BIOMETRIC DATA IN NIGERIA: A COMPARATIVE REVIEW OF THE BIOMETRIC INFORMATION PROTECTION ACT OF THE UNITED STATES

Daniel S. Padonu[6]

ABSTRACT

Biometric data is frequently used to uniquely identify an individual. However, recent studies show that biometric data acquired for identification purposes when processed reveals sensitive information about data subjects rendering them vulnerable and infringing on their privacy rights. It is therefore argued that data protection framework in Nigeria is blatantly insufficient to effectively protect the vulnerabilities brought on data subjects by reason of the processing of their data. The perspective is founded on a careful examination of Nigeria's current legal framework vis-a-vis the privacy, security, human rights, ethics and socio-cultural implications associated with the processing of biometric data of data subjects. Through deliberate comparison with the Illinois' Biometric Information Act of the United States, this paper identifies challenges which impedes the protection of biometric data and proffers solutions.

Keywords: Data, Biometric Technology, Privacy, Data Protection

[6] Daniel Padonu is a final year law undergraduate of Lagos State University. He can be reached at: padonudaniel03@gmail.com

INTRODUCTION

Data has become one of the most significant assets for both individuals and corporations in the current digital era. The 21st century, marked by rapid technological innovations/advancements and widespread internet usage, have made data collecting, processing, and storage less daunting. These technological advancements, particularly the usage of biometric systems and technology, have become an incredible tool in obtaining individual's personal data for the seamless performance of activities ranging from the personal use of smart devices to the performance of commercial transactions among private or legal entities, conduct of government surveillances, implementation of security measures, conduct of civil activities such as elections among numerous others.[7] These set of personal data obtained via the use of biometric systems are regarded as **"biometric data"**. The interpretation section[8] of the *Nigerian Data Protection Act 2023*[9] explains biometric data as "*any personal data resulting from specific technical processing relating to their physical, psychological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retina scanning, voice recognition, DNA analysis*." According to a recent survey on consumer perception of biometrics, *82%* of individuals who have access to devices equipped with fingerprint sensors utilizes them.[10]

With the proliferation in the usage of biometric technology in general course of dealings, the unequitable vulnerabilities on data subjects' security and privacy of their biometric information raises weighty concerns. The *Article 29 Working Group*[11] discovered that sensitive information such as health status, disease susceptibility, and racial or ethnic origin are contained in biometric

---

[7] Samuel Uzoigwe, "Biometric Technology in Nigeria: Examining Data Privacy Concerns", <https://aanoip.org/biometric-technology-in-nigeria-examining-data-privacy-concerns/> accessed 27 February 2024.

[8] Section 65 of the ACT.

[9] The Nigeria Data Protection Act 2023 ("NDPA") is Nigeria's first major federal legislative instrument governing personal data processing and protection. The NDPA, along with its regulatory framework in Nigeria, provides a comprehensive approach to personal data protection. To a significant extent, the NDPA parallels the European Union ("EU") General Data Protection Regulation ("GDPR"), but adds a few new legal concepts.

[10] Alžběta Krausová, Hananel Hazan, Ján Matejka, "Biometric Data Vulnerabilities: Privacy Implications", <https://www.researchgate.net/publication/328392791> accessed 27 February 2024.

[11] Working Party on the Protection of Individuals with regard to the Processing of Personal Data (Article 29 Working Group) was an independent European Union advisory body on data protection and privacy. It was composed of the European Commission, the European Data Protection Supervisor, and a delegate from each EU Member State's data protection body.

data[12] as it is considered the most personal information a person possesses because it is an unalterable link to their identity.

Consequently, there is a need to harmonize the legal, ethical, and technical frameworks in order to guarantee the privacy of people's biometric data and minimize inherent risks. This article aims to elucidate on the legal concerns arising from the processing of biometric data while exploring means to ensure adequate protection.

EMBRACE OF BIOMETRIC SYSTEM/TECHNOLOGY IN NIGERIA

Due to inadequate identity management systems, several forms of fraud were largely addressed in Nigeria with the advent of biometric identification. *A priori*, the country's poor identity management system allowed unscrupulous individuals to easily manipulate the system by creating bogus individual profiles for various objectives. Fake passports and driver's licenses, inactive bank accounts plundered by dishonest bank personnel, fraudsters diverting earnings to shareholders, and other widespread issues were all part of the problem. Notable and yet embarrassing is the escape of Diepreye Alamieyeseigha, a Nigerian state governor, who returned to his home village a folk hero after apparently escaping the UK's prison in a female dress and on a forged passport after being indicted of €1.8million charge.[13] Hence, the need for a proper identity system for its citizens which would enhance access to social services and also aid in curbing crime. This paper aims to examine how different organizations in Nigeria are employing biometric technology and how same is advancing both national development and security.

a. Commercial Banks

There is a strong need for increased security for access to sensitive or personal information in the banking system due to the rising number of compromising incidents on traditional security systems (passwords and PINS). Recent advancements in real-time security procedures have led to the implementation of BVN and the analysis of human traits using biometric technology as an improved method of identification and authentication.[14] The Central Bank of Nigeria (CBN)

---

[12] Ibid (n 2).

[13] The Guardian, "Nigerian state governor dresses up to escape £1.8m charges in UK", <https://www.theguardian.com/world/2005/nov/23/hearafrica05.development> accessed 27 February 2024.

[14] Ehiagwina Frederick, Afolabi L.O, "MANAGING INSECURITY WITH BIOMETRIC ENGINEERING: AN OVERVIEW OF THE NIGERIAN EXPERIENCE",

adopted the Bank Verification Number (BVN) in February 2014, which was one of the first biometric measures employed.[15] It entails utilizing biometric technologies to register consumers in the banking system. This is accomplished by collecting and storing each customer's distinct physical characteristics, like their fingerprints and facial features. After then, this collected data is used for multiple transactions to accurately identify the customer. It will not be feasible to open and maintain a personal bank account in Nigeria without the BVN.[16] The project's goal is to use biometric data to identify and validate every person who has an account at any Nigerian bank, and then to use that data to authenticate customers' identities during transactions.

b. Nigerian Communication Commission (NCC)

The Nigerian Communications Commission (NCC) used a fingerprint reader and facial biometric capture device to roll out a biometric SIM card registration system across the nation. In order to generate an accurate user database for tracking SIM card usage, prevent fraud, and discourage criminals from selling pre-activated SIM cards, the implemented biometric identification system requires civilians to register their biometric credentials for SIM card registration. This has made it easier for telecom providers and the NCC to trace and monitor mobile activity by enabling the creation of a centralized database containing over 140 million SIM card user fingerprint biometric templates.[17] The primary goal of Nigeria's biometric-backed sim registration program is to help law enforcement agencies enhance their security protocols by minimizing robberies, kidnappings, cybercrime, and acts of terrorism.

c. National Identity Management Commission (NIMC)

The National Identity Management Commission (NIMC) is the body in charge of gathering citizen data. Their tasks include assigning unique serial keys with eleven (11) digits that serve as the citizen's identification number (also known as the NIN) and updating the current identity database. NIN is generated for individual records using a multimodal biometric recognition method that involves gathering ten fingerprints, head-to-neck facial and signature information,

---

<https://www.researchgate.net/publication/292367915_MANAGING_INSECURITY_WITH_BIOMETRIC_ENGINEERING_AN_OVERVIEW_OF_THE_NIGERIAN_EXPERIENCE> accessed 28 February 2024.

[15] Central Bank of Nigeria (2019), 'Payment System: Bank Verification Number (BVN)', <https://www.cbn.gov.ng/Paymentsystem/BVN.asp> accessed 28 February 2024.

[16] Ibid (n 2)

[17] Case Study on Biometric SIM Card Registration System in Nigeria, <https://www.m2sys.com/blog/case-study-on-fingerprint-biometric-based-sim-card-registration-system/> accessed 28 February 2024.

and demographic data.[18] All Nigerian citizens and legal residents are required to enrol for the NIN, which necessitates the NIMC gathering and processing biometric data from citizens.

The NIN can be used to get a variety of services, including government social services such as loan applications, voter registration, the issuance and renewal of international passports, and bank account opening and reactivations. Most recently, the Joint Admissions and Matriculation Board (JAMB), which is in charge of administering admission exams and placing students in Nigerian higher institutions, made having a National Identification Number (NIN) a prerequisite for candidates wishing to register for the 2021 examination. This provision was designed to combat checkmate examination misconduct. Also in December 2020, the Federal Government of Nigeria ordered that all Nigerians link their National Identification Numbers (NINs) to their SIM cards or risk losing the ability to possess and operate the numbers given to such SIM cards.[19]

LEGAL ISSUES ASSOCIATED WITH THE USE OF BIOMETRIC TECHNOLOGY

The widespread adoption of sophisticated technologies such as biometric technology for the collection, storage and processing of confidential information raises concerns about the protection and security of individuals' data which underscores the very essence of privacy rights guaranteed not only in domestic legislations, but recognized internationally under various international instruments and treaties.[20] Without doubt, incredible advancements in electronic data processing systems and devices have enabled governments and large corporations to construct large data banks in order to better and expand the collection, processing, and interchange of personal data, with positive intent. However, this comes at a great cost to individuals' privacy and has raised concerns as to whether the private life of data subjects is, in truth, safeguarded. There are significant privacy arguments that personal data gathered by public and private entities may not be handled properly and wisely, as well as serious privacy issues about the proper protection of individuals' rights.

---

[18] T. F. Sholanke, "Biometrics Application: A Critical Review", Journal of Technology and Systems, ISSN : 2788-6344 (Online), Vol.5, IssueNo.1, pp 22 –39, 2023, <file:///C:/Users/USER/Downloads/1391-Article%20Text-4392-1-10-20230813.pdf> accessed 28 February 2024.

[19] Ibid (n 2).

[20] The Universal Declaration of Human Rights (UDHR), which has now received the status of customary international law, is the foremost international treaty on the protection of human rights worldwide. Article 12 of the Declaration provides for the right to privacy of humans.

Biometric data systems pose a multitude of privacy issues, from fraud and social sorting to identity theft made feasible by unauthorized parties hacking biometric databases and subsequent data breaches.[21] Data subjects become vulnerable when databases are hacked or used for purposes that differ from the basis on which it was collected. If stolen or copied, biometric data can provide access to that person's most sensitive secrets, data, bank accounts, and so forth. In July 2019, a profile data breach was revealed in the United Kingdom. Data from 339 million customers' personal records was taken in a cyberattack that began in 2014 against the Marriott Hotel network database. Passport numbers, credit card details, log-in credentials, and travel itinerary details were among the sensitive information taken. Further information from the Information Commissioner's Office (ICO) showed that over 400,000 consumers' data was compromised due to a data breach that also affected British Airways.[22]

The concerns about access to biometric data emerge when the data controllers blatantly violate the principles of data protection which are embedded in various data protection laws locally and internationally.[23] As universally acknowledged, data protection principles include but not limited to transparency, fairness, integrity and accountability. Compliance with these principles will truncate the occurrence and reoccurrence of data breach on the part of data controllers. However, it has been the incessant habits of data controllers to allows access to multiple governments or private entities for a variety of reasons, such as third-party verification or security activities by security services. Data subjects may not be aware of all the true uses of biometric data or how much it is shared and transferred among corporate entities, making their lives and concerns less private than ideal. The purpose for which biometric data is collected may not be the only purpose for which it is used. Because of the nature of permission, such as the need for more information before giving consent or the serious consequences of withholding consent, data subjects' purported assent—whether express or implied—to the collection and processing of their data may be questioned.

[21] Ibid (n 2)
[22] "Biometric Data & Privacy Laws (GDPR, CCPA/CPRA)", <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data> accessed 28 February 2024.
[23] The OECD Privacy Framework, <https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf> accessed 28 February 2024.

DATA PROTECTION FRAMEWORK FOR BIOMETRICS IN NIGERIA

It is noteworthy that there is no single legislation enacted specifically for the protection of biometric data in Nigeria. Rather, an array of regulations that deal with the regulation of the data of its citizens. They are best defined as a patchwork of regulations, as they serve distinct purposes for various industries. However, just the constitution and the Nigerian Data Protection Act 2023, which is presently the most comprehensive legislation on data protection, will be examined.

The *1999 Constitution of the Federal Republic of Nigeria* (as amended) is the most superior legislation in Nigeria and is the grundnorm for all privacy rights in Nigeria. *Section 37 of the 1999 Constitution* enshrines the inalienable privacy rights which repletes that ***"The privacy** of citizens, their homes, correspondence, telephone conversations and telegraphic **communications is hereby guaranteed and protected".*** It is based on this provision that all other privacy rights are structured in Nigeria.

The primary data protection legislation in Nigeria is the *Nigeria Data Protection Act 2023*[24]. June 12, 2023, saw the enactment of the NDPA, which has since taken effect. Before the NDPA, the National Information Technology Development Agency (NITDA) published the Nigerian Data Protection Regulations 2019[25], which served as the de facto data protection regulations.[26] It is still ancillary legislation even though it is enforced. In addition to protecting the fundamental freedoms and rights of data subjects as stipulated by the Nigerian Constitution and data protection practices, the Act offers a thorough and extensive legal framework for the protection of personal information.[27]

Holistically, the NDPA is made up of 66 sections divided into 12 parts and a schedule. These parts provides for the objectives and application of the Act; the establishment of the Commission and its Governing Council; the financing of the Commission; principles and lawful basis governing the processing of personal data; rights of a data subject; data security; cross-border transfer of

[24] Hereinafter referred to as 'NDPA'.
[25] The NDPR
[26] Unveiling some salient features of Nigeria's novel Nigeria Data Protection Act (NDPA) 2023, International Network of Privacy Professionals, <https://inplp.com/latest-news/article/unveiling-some-salient-features-of-nigerias-novel-nigeria-data-protection-act-ndpa-2023/> accessed 2 March 2024.
[27] Data Guidance, "Nigeria - Data Protection Overview", <https://www.dataguidance.com/notes/nigeria-data-protection-overview> accessed 2 March 2024.

personal data; registration of controller/processors and penalties for violations of the Act; enforcement provisions of the Act; legal proceeding on matters covered by the Act; and Miscellaneous provisions.[28] More specifically, the NDPA, unlike the NDPR, makes provision for Biometric Data and recognizes its delicate nature. This indeed is a laudable step taken by the National Assembly in recognizing their obligation to secure and protect the privacy of Nigerians.

Notwithstanding the Act's undeniable contribution to the sector's expansion, there are certain drawbacks. Although the act provides for biometric data in its interpretation section, it does not provide for the implementation of any unique security measures when using biometric data. It just states that data controllers and processors have a "duty of care," but it offers no concrete means of accountability. More so, there has been little or no implementation measures to ensure that data controllers strictly adhere to the provisions of the NDPA as well as provision of stringent penalties for violation of same.

AN APPRAISAL OF THE BIOMETRIC INFORMATION PROTECTION ACT

The United States does not have a comprehensive data privacy regulation that applies to biometric data nationwide, in contrast to many other nations. However, in 2008, Illinois became the first state in the US to enact a regulation specifically for the protection of biometric data.[29] The Biometric Information Protection Act (BIPA) primarily governs the biometric data collection, processing, disclosure, and security of Illinois residents. Because biometric data cannot be easily altered, BIPA distinguishes it from other personally identifiable information. It delineates rigorous guidelines for the acquisition, transformation, retention, or dissemination of "biometric identifiers," which encompass scans of the retina or iris, fingerprints, voiceprints, or hand or facial geometry.[30] In order to conduct business in Illinois, private entities must abide by a number of requirements set forth by BIPA. The law ensures that individuals are in control of their own

---

[28] A REVIEW OF THE NIGERIAN DATA PROTECTION ACT 2023: HIGHLIGHTS AND LIMITATIONS INTRODUCTION, <https://strenandblan.com/2023/07/26/a-review-of-the-nigerian-data-protection-act-2023-highlights-and-limitations-introduction/> accessed 2 March 2024.

[29] Is Biometric Information Protected by Privacy Laws?, Bloomberg Law, <https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/> accessed 2 March 2024.

[30] Fredric Bellamy, "Looking To The Future of Biometric Data Privacy Laws", <https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/> accessed 2 March 2024.

biometric data and prohibits private companies from collecting it unless they (a) inform the person in writing of what data is being collected or stored. (e.g. fingerprint is stored when using TouchID to log into bank account app on phone) (b) inform the person in writing of the specific purpose and length of time the for which the data will be collected, stored and used. (e.g. fingerprint is stored for ease of logging into app and only for a duration of six months) (c) obtain the person's written consent. (e.g. user signs their name before sharing their fingerprint).[31]

The Act is considered the most comprehensive, stringent and litigated biometric privacy law in the United States and is the only one that creates a private right of action. To that end, over 400 BIPA class action lawsuits have been filed in the past five years. The majority of BIPA claims stem from issues related to work, including time clocks, corporate computer access, building security, safes and lockboxes, dual authentication, and facial temperature scanning. Several BIPA lawsuits centre on point-of-sale systems, lunch-paying students, and social media photo scanning features like Facebook's Tag Suggestions.[32]

RECOMMENDATIONS

An intrinsic examination of legal and ethical frameworks created to protect biometric data and the frequent impediment to the effective protection of biometric data provides insights in striking a fair balance between supporting technological innovations and protecting the privacy rights of individuals. In a bid to reconcile technological advancement with legal framework, it is advised that the government should strike a proportionate measure to protect the biometric data of Nigerians specifically, considering the wide spread embrace and employment of biometric technology in Nigeria. Due to the delicate nature of biometric data, a specific legislation synonymous to the BIPA should be enacted and it should stipulate severe penalties for violating citizens' rights to data privacy.

Furthermore, the complex landscape of data protection, especially with regard to biometric data, requires cooperation between academic institutions, governmental bodies, and private sector businesses. The public sector provides the regulatory framework required to protect individual

[31] Section 15 of the Act.

[32] Maryam Rad, Tim Smit, Riley Brant, "Biometric Data: Privacy, Cybersecurity & Insurance Considerations", <https://assets.ctfassets.net/zr7mmeciv2ps/TZqEHSpZlenhS2WSClt87/648a2c8d99ccdb2eb5b942de31071b7c/20201001_WP_Biometric_Data.pdf> accessed 2 March 2024.

rights and maintain public trust, the private sector provides practical implementation, and academia contributes research and analysis expertise to provide insights into emerging technological trends and potential vulnerabilities. By fostering collaborations between academia, industry, and regulatory bodies, a comprehensive framework can be expanded to anticipate, prevent, and rectify potential vulnerabilities, thereby establishing a solid foundation for biometric data protection that conforms to ethical standards and regulatory mandates.

In addition, incorporating a rigorous informed consent procedure is critical. This point of view highlights the importance of striking a careful balance between technical advancement and individual rights, recognizing that collecting, storing, and exploiting biometric data requires individual's informed and express consent. From a legislative standpoint, this includes developing regulatory frameworks that require full disclosure of data usage purposes and associated risks, as well as establishing techniques that allow individuals to exercise control over their data. This point of view highlights the government's responsibility to ensure that informed-consent procedures are rigorously executed and matched with ethical standards, taking into account the nuances of biometric data collecting and processing. To further fully discourage data controllers from violating the law, an efficient regulatory agency that will enforce strict adherence to the regulations should be established. In the case that these laws are disregarded, a severe penalty should be stipulated.

CONCLUSION

In conclusion, data privacy has grown to be a major worry for people, companies, and the government in an era of quickly advancing technology, especially with regard to biometric data. Therefore, it is impossible to overstate the significance of data security and privacy. Over the years, a number of actions have been done to safeguard it. States must, however, exert unrelenting effort to guarantee the implementation of strict measures that would ensure the complete protection of personal data, including biometric data.