GUARDIANS OF THE DIGITAL REALM: MAPPING KEY STAKEHOLDERS IN DATA PRIVACY AND DIGITAL CREDIT UNIVERSE

Oluwabunmi A. Falebita[1] and Oluwafemi P. Famakinde[2]

[1]Innovation and Technology Policy Department
[2]Social Policy Department, Nigeria Institute of Social and Economic Research (NISER), Ibadan, Nigeria

ABSTRACT

In Nigeria's rapidly evolving digital economy, data privacy and digital credits emerge as critical areas demanding robust stakeholder engagement and strategic oversight. This study examines the intricate web of key stakeholders in digital data privacy and digital credit sectors, their interrelations, responsibilities, and impacts. These stakeholders include governmental regulatory bodies, financial technology firms (fintechs), consumers and international organizations. Through a systematic literature review, the study navigates the complexities of these relationships, particularly in the wake of Nigeria's Data Protection Act and the burgeoning digital credit market. Data is synthesized from policy documents, digital credit transaction trends, and organizational repositories to underscore the growing significance of stakeholder actions and interactions. The findings illuminate the current landscape and forecast the trajectory of digital data governance and credit practices, emphasizing the necessity for a harmonious and secure digital economy that serves all stakeholders equitably.

KEYWORDS

Data Privacy, Data Protection, Digital Credits, Stakeholders

1. INTRODUCTION

Digital transformation has ushered in an era where digital credits and data privacy are pivotal to a country's economic and social fabric (Lottu *et al.,* 2023). The convergence of technology and finance has revolutionized credit systems worldwide, with Nigeria being no exception. As Nigeria strides into the digital age, its trajectory is markedly influenced by the increasing significance of data privacy and the burgeoning sector of digital credit (Kperogi, 2019). This transformation has introduced new opportunities and challenges, particularly in the realms of data privacy and digital credits.

As digital lending platforms proliferate, the management and protection of personal data have become critical issues. These elements are not merely technological advancements but are pivotal in shaping the economic and social tapestry of the nation (Anand & Brass, 2021). The digital revolution has compelled a reassessment of traditional privacy norms and credit systems, leading to a sophisticated and complex landscape where multiple actors wield influence (Ladagu, 2021). The proliferation of digital credits has transformed the financial landscape, offering unprecedented convenience and access to credits for individuals globally. Digital credits offered by lending firms have risen as a substitute for offering short-term loans through mobile apps and websites, some of which are specifically optimized for mobile use (Francis et al, 2017; Robinson et al., 2023). While the convenience and accessibility of digital credit services are undeniable, the

collection and utilization of vast amounts of sensitive personal and financial data raise important questions about data privacy and security. In an era where personal and financial information is stored digitally, the risk of unauthorized access, data breaches, and misuse of sensitive data is significant. Inadequate data protection measures and cybersecurity vulnerabilities can jeopardize an individual's privacy and financial security (Sule, Zennaro, and Thomas, 2021).

These challenges necessitate robust safeguards, policies, and regulations to mitigate the potential threats to data security and individual privacy ensuring that digital credit remains a viable and secure option for all. According to Yang et al. (2015), the inadequacies in data protection regulations have made it increasingly challenging for customers to assert their rights in e-commerce. The regulatory uncertainty surrounding mobile payments has led to heightened concerns among customers regarding their privacy and finances (Eke et al., 2022; Nwafor, 2022). The rapid growth of digital lending platforms, also necessitates the security and responsible handling of personal and financial data, due to the likelihood of data breaches and digital privacy violations. As these services grow in popularity, they raise fundamental questions about digital privacy and policy, bringing to the fore the importance of data privacy practices and policies (Iheanachor et al., 2023).

Data privacy refers to the protection of personal data from unauthorized access, use, and disclosure by governments, companies, or individuals. According to Greenleaf (2018), the concept of data privacy started to gain prominence in the mid-20th century. Furthermore, the concept of data privacy can be described as the safeguarding of the collection, processing, and utilization of personal information, particularly in response to the rapid advancements in technology (Umeh, 2022). Data privacy practices and policies are fundamental in safeguarding consumers from the potential misuse of their personal information. One of the significant challenges confronting data privacy globally is the need for a consistent and comprehensive regulatory structure (Rustad & Koenig, 2019). Other challenges include the impact of new technologies and platforms on data gathering and processing. To enshrine data privacy several policies and regulations have emerged including the European Union's General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA) in 2023 (NDPC, 2023). The advent of the internet and smartphones play a pivotal role in enhancing the value, accessibility, and abundance of digital data. The increased connection of various items and mobile devices to the internet provides an impetus for the exponential growth of digital data. The volume of data generated thus underscores the necessity for the protection, handling and usage of this type of data leading to the concept of digital data privacy.

The key components of data privacy are the loss of control over personal data and the intrusion of unauthorized parties. Oftentimes, online users have concerns about the unauthorized utilization and disclosure of their information to third parties. Hence, Odusote (2021) identified a rise in the frequency of reported digital data privacy concerns in Nigeria. Individuals reserve the right to provide consent for the gathering of their data by organizations, while such organizations owe it to users to provide detailed measures employed in securing such data from breaches and unauthorized access Alafaa (2022). To be ethically responsible, such organizations are also expected to provide privacy policies that inform users about the type of personal information required, its intended use and the likely parties with whom it could be shared (Falebita & Famakinde, 2024). Organizations such as lenders or digital credit providers often require certain information from the lenders or users of their services, ranging from general to personal data. Such data include Bank Verification Number (BVN) and National Identification Number (NIN), which have been perceived as sensitive by lenders or users of digital credit services in Nigeria as highlighted by Falebita & Famakinde (2024). These users are however significant, representing the most susceptible stakeholders in the realm of digital privacy, they are generally referred to as the “data subjects” (Odusote, 2021; Wang et al., 2021). In addition, other stakeholders exist in the

digital realm to shape the norms and practices of digital data privacy and credit systems. This study therefore seeks to unravel the intricacies of this realm by identifying and analyzing the roles of the key stakeholders in Nigeria's digital data privacy and digital credit ecosystems. This study would also delineate the critical roles of these stakeholders in navigating the challenges and opportunities presented by digital transactions while underscoring a cooperative approach where regulation, innovation, consumer protection, and societal norms align.

2. METHODS

To comprehensively explore the roles of key stakeholders in Nigeria's digital data privacy and credit landscape, this study employed a systematic literature review method. This approach ensures a thorough and unbiased synthesis of existing research, providing a robust foundation for understanding the dynamics within this ecosystem.

2.1. Data Sources and Search Strategy

The literature review was conducted using a range of reputable and reliable sources, including scholarly articles, books, and peer-reviewed journals. The primary databases and platforms utilized for sourcing literature were: Google Scholar, ResearchGate, NCBI, and JSTOR. The initial search was conducted from October 23 to November 10, 2023, with a supplementary search on November 29, 2023, to ensure the inclusion of the most recent publications. The search strategy was designed to identify relevant studies published within the last 7 to 10 years, with a probability of irreplaceable older sources not exceeding 5%. Keywords and search terms included "digital data privacy," "digital credits," "Nigeria," "stakeholder roles," "data governance," and related terms.

2.2. Review Process

Each identified article was subjected to a rigorous review process. Initially, the titles and abstracts were screened to assess their relevance to the study objectives. Full-text reviews were then conducted for studies that met the initial screening criteria. Each article was reviewed by at least two reviewers to ensure accuracy and mitigate bias. A total of three researchers participated in the review process at different stages, contributing to the robustness of the methodology.

2.3. Data Extraction and Synthesis

Data extraction focused on key themes relevant to stakeholder roles in digital data privacy and credit, including regulatory frameworks, lender practices, and borrower experiences. The extracted data were systematically organized and synthesized to identify patterns, gaps, and emerging trends in the literature. For consistency and accuracy in citations, an automatic reference generator was used throughout the review process. This tool facilitated the efficient management of references and ensured adherence to citation standards.

3. FINDINGS

This section summarises the main findings, offering a comprehensive overview of the multifaceted roles of stakeholders within Nigeria's digital landscape. The analysis draws on a rich body of academic research, policy analyses, and case studies to elucidate the impact of these stakeholders on shaping digital data privacy and credit systems. The exploration covers the spatial distribution of digital credit providers in Lagos, Nigeria, providing insights into the geographical concentration and accessibility of these services. Additionally, the study

summarizes the attributes of digital credit providers (DCPs) and their customer bases, offering a detailed picture of the market dynamics in Nigeria's digital credit and data privacy landscape. Furthermore, the analysis includes a depiction of the years of operation of the DCPs to improve understanding of the growth trends within the sector and highlight its stability.

3.1. Stakeholders of Digital Credits in Nigeria

This section delves into the stakeholders of digital credits and their multifaceted roles within Nigeria's digital landscape, providing a detailed examination based on a wealth of academic research, policy analyses, and case studies. Figure 1 shows the interdependent relationships among these stakeholders.

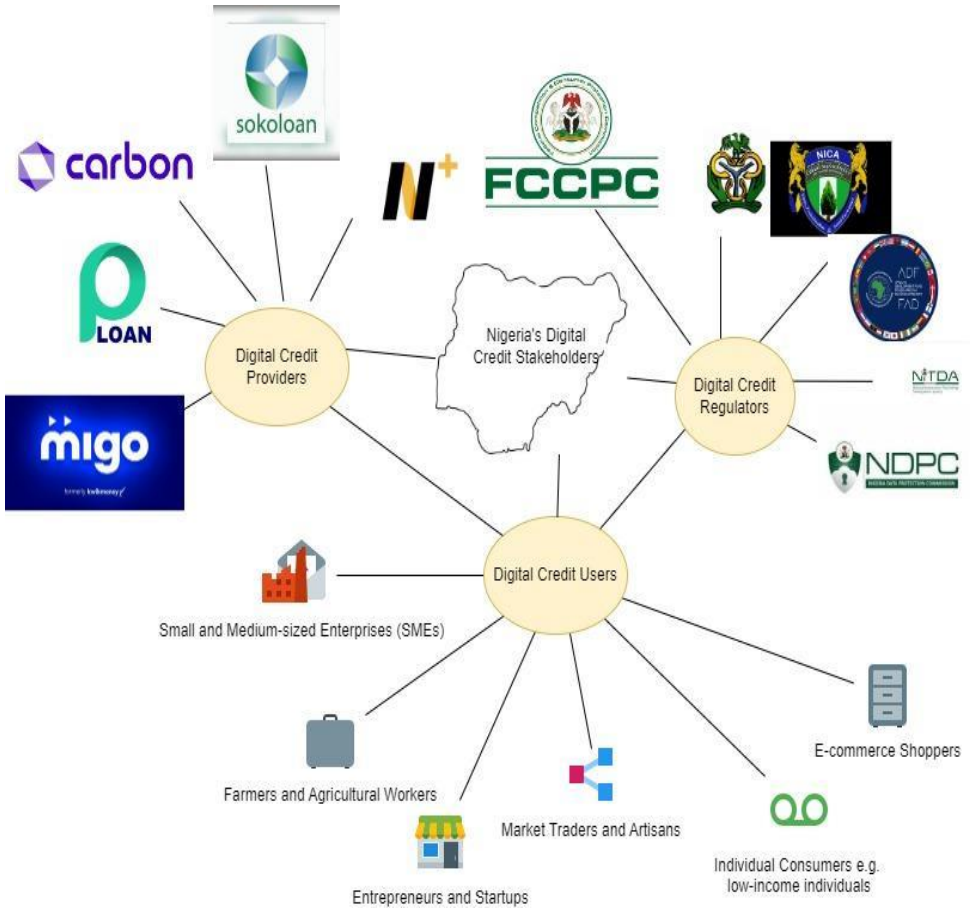

Figure 1: Map of Key Stakeholders of digital credits in Nigeria (Author's Concept)

The stakeholders in Figure 1 include regulators, providers, and users, each playing a distinct yet interconnected role in this evolving ecosystem. Regulators are primarily responsible for establishing and enforcing policies towards data protection and secure digital transactions. Their frameworks and guidelines are crucial in maintaining the integrity of the digital credit system and protecting consumer information. Providers, both traditional financial institutions and emerging fintech companies, are the architects of digital credit offerings. They leverage technological advancements to provide innovative credit solutions, which necessitates the collection and processing of personal data. The practices and policies of these providers are critical in ensuring data privacy and security, directly affecting the trust and participation of consumers in the digital credit market. Consumers (digital credit users) are the end-users who engage with digital credit

services, providing personal data in exchange for financial access. Their role is pivotal in shaping the credit landscape, as they often influence lender practices through their feedback and demand for higher data protection standards.

The interactions among these stakeholders shape the digital credit landscape, highlighting the need for collaborative efforts to foster a secure and efficient ecosystem. This analysis underscores each stakeholder's role and the dynamics of their interactions in enhancing the sustainable growth of digital credit services in Nigeria.

3.2. Organizational Demographics of Some Digital Credit Providers in Nigeria

Considering prevalence, the demographics and spatial distribution of some digital credit providers (DCPs) are presented. The spatial distribution (see *Figure 2*) shows that the majority of these DCPs are clustered in the Eti-Osa Local Government Area (LGA) of Lagos State, while others are dispersed across other LGAs in the State.

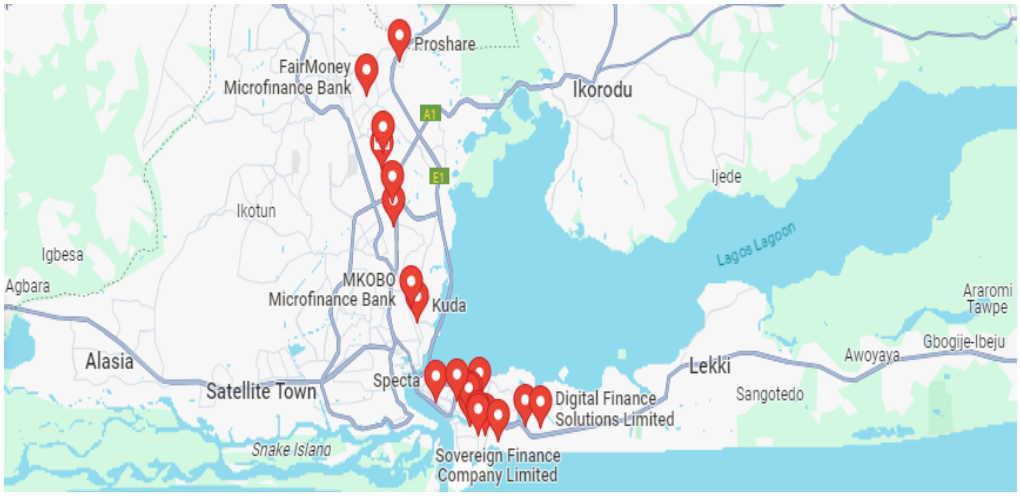

Figure 2: Spatial Distribution of Some Digital Credit Providers in Lagos, Nigeria.

Furthermore, certain attributes of these DCPs are presented, such as the minimum amount loanable to customers (users), the years of operation and the customer base of these DCPs. Findings in *Figure 3* reveal that the minimum amount loanable for half of the DCPs is five thousand Naira, while for the other half, it is ten thousand Naira. Thus, the minimum amount that DCPs can lend to users ranges between five and ten thousand Naira.

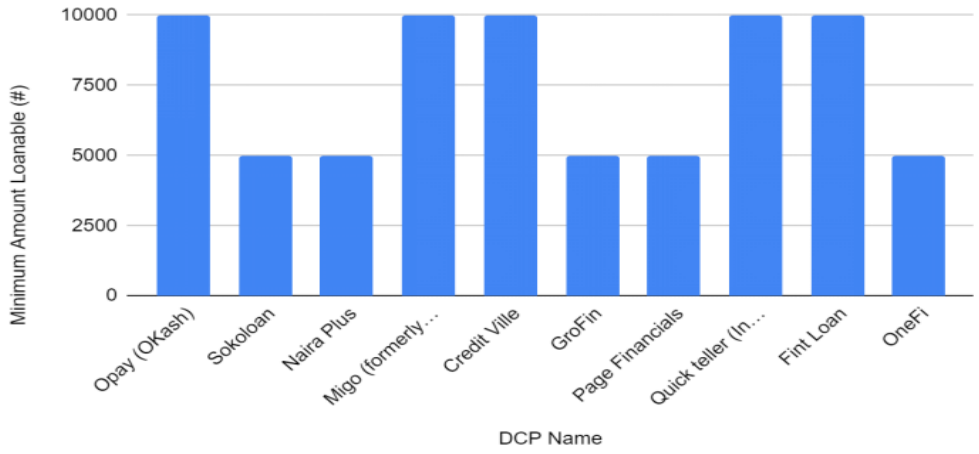

Figure 3: Minimum Amount Loanable to Customers.

Another attribute of DCPs in terms of their years of operation is depicted in *Figure 4*. This figure shows that Migo (formerly Kwik Money) has the longest years of operation over seven years, followed by Opay (OKash) with over five years of operation, while Quick Teller (Interswitch) and GroFin both have over four years of operation. Sokoloan, Credit Ville, Page Financials, Fint Loan, and OneFi all have over three years of operation and the DCP with the least years of operation is Naira Plus with over two years.

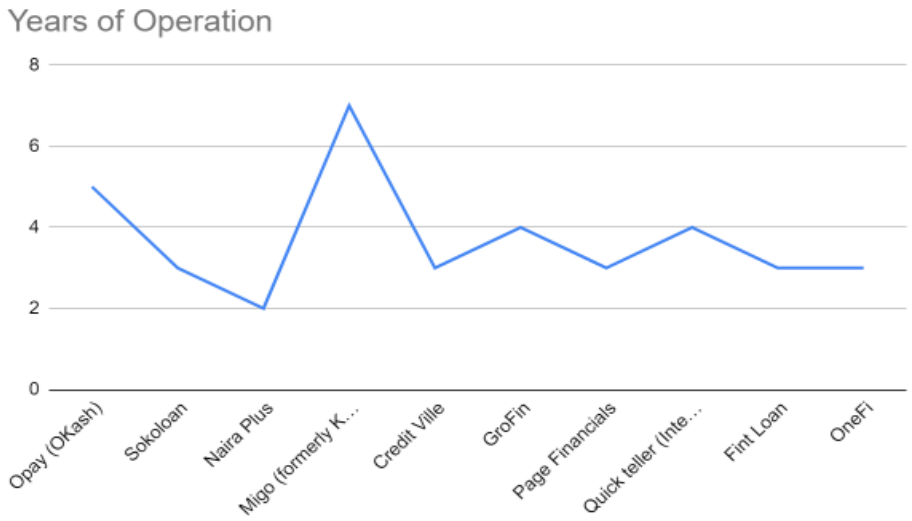

Figure 4: Years of operation of Digital Credit Providers

Lastly, the DCPs were also described based on their customer base, that is the number of customers they have. *Figure 5* shows that both Opay (Okash) and Quick Teller (Interswitch) have the highest customer base of 19.8% (100,000 people). They are followed by five DCPs - Sokoloan, GroFin, Page Financials, Fint Loan and OneFi- with a customer base of 9.9% (50,000 people). Naira Plus has a 5.0% (25, 000 people) customer base and has been in existence for the least number of years. Credit Ville has a customer base of 4.0% (20,000 people) and lastly, Migo (formerly Kwik Money) has the lowest customer base of 2.0% (10,000 people) despite being in existence for the longest period.

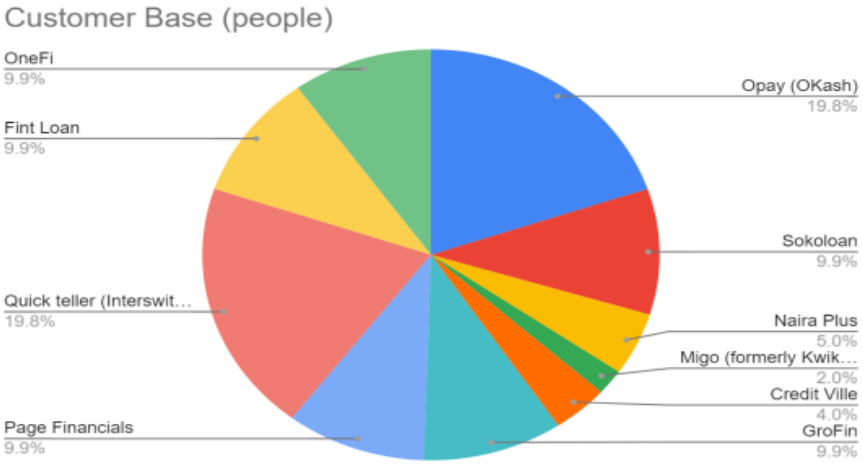

Figure 5: The Customer Base of Digital Credit Providers

3.3. National Stakeholders of Data Privacy in Nigeria

The stakeholder map in *Figure 6* illustrates the key national agencies involved in the governance of data privacy within Nigeria's digital credit ecosystem. Each agency plays a distinct role, contributing to the overall framework of data protection.

The National Development Planning Commission (NDPC) leads in the enforcement of data privacy laws and regulations in Nigeria by ensuring compliance with the NDPA. It oversees lawful, fair, and transparent processing of personal data and impacts how entities handle citizen data. The National Information Technology Development Agency (NITDA) is another agency that is pivotal in developing and regulating information technology policies for economic development. Also, the Nigerian Communications Commission (NCC) as a stakeholder, regulates the telecommunications sector by ensuring that communication service providers adhere to data privacy standards, thereby protecting consumers' personal information in digital transactions.

In addition, the Economic and Financial Crimes Commission (EFCC) focuses on combating financial crimes, investigating and prosecuting data breaches and fraud in the digital credit sector while enforcing data privacy laws to prevent financial misconduct. The National Identity Management Commission (NIMC) manages the national identity database and issues the National Identification Numbers (NINs), which are essential for verifying identities in digital credit transactions, thereby enhancing data security and privacy. Lastly, the Federal Competition and Consumer Protection Commission (FCCPC) protects consumer rights by ensuring that digital credit providers operate transparently and fairly to safeguard consumer data and address grievances related to data misuse. All these stakeholders are interconnected, working collectively to ensure robust data privacy governance within Nigeria's digital credit landscape. Their collaborative efforts are essential for fostering a secure and trustworthy environment for digital financial services (Soetan et al., 2021).

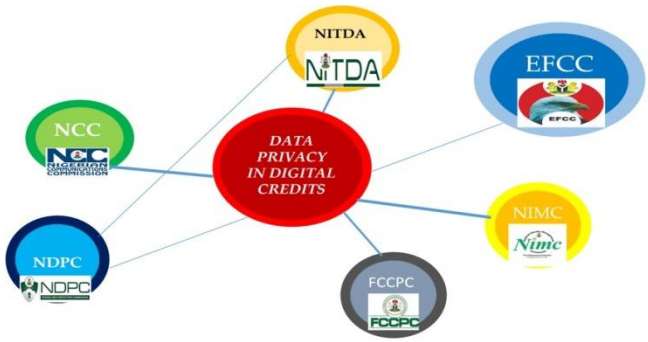

Figure 6: Map of National Stakeholders in Data Privacy in Nigeria (Author's Concept)

3.4. International Stakeholders of Data Privacy in Digital Credits

International stakeholders, such as United Nations agencies, the International Monetary Fund, Interpol and the European Union (see *Figure 7*), play a role in Nigeria's digital credit landscape. Their influence is revealed in the technologies they introduce and the global data protection standards they propagate (Rustad and Koenig, 2019). While their involvement drives innovation and growth, it raises concerns about digital sovereignty and the alignment of Nigeria's digital policies with international interests and standards. The international dimension of Nigeria's digital data privacy and credit landscape is critical, as these stakeholders bring a wealth of resources, expertise, and innovation to the Nigerian digital market. The interrelationships among these stakeholders are germane to the attainment of a realm where citizens' data are private and safe.

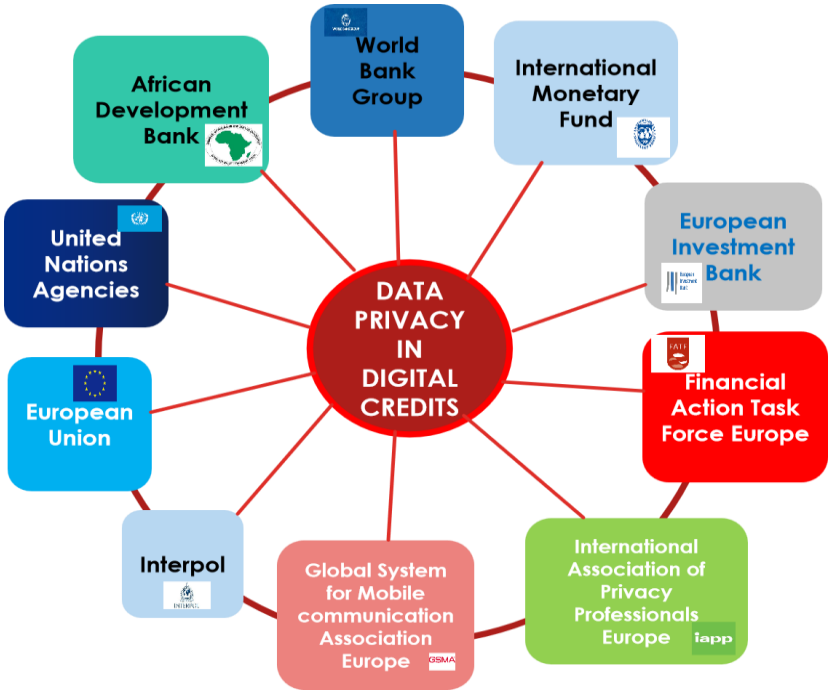

Figure 7: Map of International Stakeholders in Data Privacy in Digital Credits (Authors' Concept)

These stakeholders influence the digital financial services space, provide financial and advisory support, render policy advice and stipulate global standards for data privacy. In addition, they

shape Nigeria's digital credit and data privacy landscape through international regulatory standards such as the GDPR, funding digital and fintech projects, promoting international data protection practices and standards, and monitoring international financial transactions and crime. Their involvement underscores the interconnected nature of the digital economy, where global trends and collaborations increasingly shape local practices.

4. CONCLUSION

The conclusion of this study reiterates the complex interplay of various stakeholders as guardians in shaping the digital data privacy and credit environment. It brings to the fore the collective impact of regulatory authorities, financial technology companies (fintechs), consumers and international organizations on the development and governance of this realm. Regulatory bodies are tasked with creating and enforcing policies that balance innovation with the protection of consumer data. Their directives and frameworks are foundational to the establishment of a secure digital credit system. Fintechs, on the other hand, are both innovators and disruptors, responsible for transforming traditional financial services into streamlined and accessible credit options for a wider audience. Furthermore, through data-driven models, they shoulder the responsibility of safeguarding the personal information they collect, necessitating robust data protection measures that instil trust among users (consumers).

Consumers as the end-users of digital services, and their perceptions and attitudes towards data privacy and digital credits are crucial. Increased awareness among consumers of their data rights and the implications of their digital footprints, strengthens their demands for transparency and security thus influencing the services provided by fintechs and regulations enacted by governing bodies. Lastly, international organizations continually shape the digital realm by setting higher standards for data protection across countries, promoting international cooperation on data privacy guidelines and encouraging responsible development and implementation of digital credit systems to address data security concerns.

Finally, the study calls for a concerted effort from all stakeholders to build a digital realm where personal privacy is respected, secure transactions are guaranteed, and financial growth is inclusive. This joint effort is the key to unlocking a digital future that benefits the entire Nigerian society.

ACKNOWLEDGEMENTS

This research was made possible in whole or in part by the Digital Credit Observatory (DCO), a program of the Center for Effective Global Action (CEGA), with support from the Bill & Melinda Gates Foundation [INV-032608].

We gratefully acknowledge the invaluable contributions of our desk review research assistants, whose meticulous efforts have significantly enhanced the quality of this research.

REFERENCES

[1] Alafaa, P. U. (2022). Data privacy and data protection: the right of users and the responsibility of companies in the digital world. Social Science Research Network. https://doi.org/10.2139/ssrn.4005750

[2] Anand, N. and Brass, I. (2021). Responsible innovation for digital identity systems. Data & Policy, 3, e35.

[3] Eke, D., Oloyede, R., Ochang, P., Borokini, F., Adeyeye, M., Sorbarikor, L. and Akintoye, S. (2022). Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns. Journal of Responsible Technology,11: 100039.

[4] Falebita, O. A. and Famakinde, O. P., Unlocking Insights: Navigating Perceptions of Data Privacy in Digital Credit (May 07, 2024). David C. Wyld et al. (Eds): EDUIT, BMLI, NSEC – 2024 pp. 65-85, 2024. CS & IT - CSCP 2024, Available at SSRN: https://ssrn.com/abstract=4884134 or http://dx.doi.org/10.2139/ssrn.4884134

[5] Francis, E., Blumenstock, J. and Robinson J. (2017). Digital Credit: A Snapshot of the Current Landscape and Open Research Questions. Center for Effective Global Action White Paper.

[6] Greenleaf, G. (2018, April 12). Data privacy laws and bills: Growth in Africa, GDPR influence. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212713

[7] Iheanachor, N., Umukoro, I. and Aránega, A. Y. (2023). Ecosystem emergence in emerging markets: Evidence from the Nigerian digital financial services ecosystem. Technological Forecasting and Social Change, 190: 122426.

[8] Ladagu, N. D. (2021). Factors for Sustainable Operations in the FinTech Industry. A Survey of Nigerian Users, Providers and Regulators. University of Wales Trinity Saint David (United Kingdom).

[9] Lottu, O. A., Abdul, A. A., Daraojimba, D. O., Alabi, A. M., John-Ladega, A. A. and Daraojimba, C. (2023). Digital Transformation in Banking: A Review of Nigeria's Journey to Economic Prosperity. International Journal of Advanced Economics, 5(8): 215-238.

[10] NDPC (2023). Nigeria Data Protection Act, 2023. A 718 2023 No. 37. Printed and Published by The Federal Government Printer, Lagos, Nigeria FGP 97/62023/1,200 Available at https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf

[11] Nwafor, I. E. (2022). Digital Rights in Nigeria: Through the Cases: edited by Solomon Okedara, Olumide Babalola and Irene Chukwukelu, Noetico Repetum Inc & Global Macron Pace Limited, 2022. 372 pp, ISBN: 9789789707.

[12] Odusote, A. (2021). Data misuse, data theft and Data Protection in Nigeria: A call for more robust and more effective legislation. Beijing Law Review, 12(04), 1284–1298. https://doi.org/10.4236/blr.2021.124066

[13] Robinson, J., Park, D. S. and Blumenstock, J. E. (2023). The impact of digital credit in developing economies: A review of recent evidence. KDI School of Pub Policy & Management Paper, (23-04).

[14] Rustad, M. L. and Koenig, T. H. (2019). Towards a global data privacy standard. Florida Law Review, 71: 365.

[15] Soetan, T. O., Mogaji, E., & Nguyen, N. P. (2021). Financial services experience and consumption in Nigeria. Journal of Services Marketing, 35(7): 947-961.

[16] Sule, M. J., Zennaro, M. and Thomas, G. (2021). Cybersecurity through the lens of digital identity and data protection: issues and trends. Technology in Society, 67:101734.

[17] Umeh, C. N. (2022). Appraisal of Data Privacy and Protection Under Nigerian Law. ResearchGate. https://doi.org/10.6084/m9.figshare.23618541

[18] Wang, C., Zhang, N., & Wang, C. (2021). Managing privacy in the digital economy. Fundamental Research, 1(5), 543–551. https://doi.org/10.1016/j.fmre.2021.08.009

[19] Yang, Y., Liu, Y., Li, H. and Yu, B. (2015). Understanding perceived risks in mobile payment acceptance. Industrial Management & Data System. 115: 253–269.

AUTHORS

Oluwabunmi A. Falebita PhD, [0000-0001-6506-4011] has over a dozen years of research and teaching experience. Her research interests include Technology and Product Management, Entrepreneurship and affiliated studies. She is an alumnus of Obafemi Awolowo University, Nigeria. She is a recipient of the OWSD PhD Research Fellowship and has published several scholarly articles and books.

Oluwafemi P. Famakinde PhD. (ORCID ID - 0000-0002-5677-5660) has years of research experience in Psychology and allied fields. He has published several scholarly articles and presented at conferences. His research interests are in the domains of emerging technology, forensics, and security.