UNLOCKING INSIGHTS: NAVIGATING PERCEPTIONS OF DATA PRIVACY IN DIGITAL CREDIT

Oluwabunmi Falebita[1] and Oluwafemi Famakinde[2]

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

ABSTRACT

This qualitative cross-sectional survey delves into the nuanced perceptions surrounding data privacy practices in the realm of digital credit in Nigeria. Through in-depth interviews (IDI) with Digital Credit Users (DCUs) across various economic hubs in Nigeria, we explore their attitudes and concerns regarding the level of sensitivity associated with personal information and their readiness to divulge it to Digital Credit Providers (DCPs). Employing a multi-stage sampling technique, clusters representing Nigeria's six zones were purposively selected, with the South-West zone chosen for its economic significance. In this zone, Lagos, Oyo, and Ogun States were further sampled based on economic activity, with 40 DCUs interviewed per state, totalling 120 DCUs. Local Government Areas (LGAs) within these states were selected based on Central Business District (CBD), urban, rural, and peri-urban criteria. Thematic analysis of interview transcripts using NVIVO 14 software revealed significant findings, suggesting that Bank Verification Numbers (BVN), National Identification Numbers (NIN), and debit card information are considered the most sensitive data for Digital Credit Users (DCUs).They expressed a high level of obligation to disclose information to DCPs and identified perceived risks such as financial loss, data breaches, and unwanted contact. Additionally, DCUs exhibited a strong preference for retaining control over their information, with many expressing a reluctance to proceed with digital credit applications if privacy breaches were anticipated. These findings shed light on the complex interplay between data privacy perceptions, risk assessment, and individual autonomy in the digital credit landscape.

KEYWORDS

Digital Credits, Digital Data Privacy, Digital Credit Providers & Digital Credit Users, Nigeria

1. INTRODUCTION

Recently, the ubiquity of digital credit has increased, particularly in Low- and Medium-Income Countries (LMICs). LMICs are countries with a certain threshold of $1,046-$4,095 per capita gross national income, numbering 140, and having diverse populations and income levels (World Bank, 2022). The prevalence of digital credit services in these climes cannot be dissociated from the increased adoption and penetration of mobile and other ICT devices (Tetteh, 2023). Due to the prevailing economic situation in LMICs, digital inclusion is expected to aid the spread of digital financial options for an enhanced standard of living, especially for underserved/marginalized communities. Digital credit represents a major financial option for short-term loans for the survival of the poor and needy in LMICs (Brailovskaya et al., 2021).

David C. Wyld et al. (Eds): EDUIT, BMLI, NSEC – 2024
pp. 65-85, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141207

Due to digital credit's novelty in LMICs, there is a limited understanding of theconditions and implications for data privacy among underserved/marginalized users, a void that DigitalCredit Providers (DCPs) often exploit. DCPs provide comparatively small loans to their customers throughdigital applications or online platforms without stringent collateral terms (Rao, 2022).DCPs often utilize applications that collect general and personal data of users for credit scoring, thus creating issues regarding data privacy for Digital Credit Users (DCUs). DCUs are customers who patronize DCPs for small loans. As such, the volume of personal and private data collected and used across diverse domains is often without the awareness and actual consent of DCUs. Where they are informed, there are often understatements and concealments as to the intent of DCPs when requesting such access. Hence, the loan terms become rather vague to the DCUs.

The access of DCPs to the private data of DCUs could be leveraged for coercive repayment tactics for non-compliant customers, which could be unethical (Salami, 2021; Etiebet and Matthew, 2022). The value of data privacy to DCUs might also vary across demographics. Consequently, the infringement on DCUs' data privacy might influence their well-being. However, the existing regulations for data privacy are fraught with lapses (Ololuo, 2020), thusthe need for effective regulations.

Furthermore, there is a limited understanding of the privacy-related risks associated with using digital credit services in LMICs (Brailovskaya et al., 2022). Moreover, there is a need for studies geared toward creating an improved understanding of data privacy protection, regulation, monitoring, and ethics in LMICs. The interaction among DCPs and DCUs can be more comprehensively graspedand explored using the stimulus theoretical framework (Lai et al., 2016). This study focuses on Nigeria as a representative of LMICs in Africa.

The subject of data privacy has been of increasing interest over the years across continents. Digitally provided loans (digital credits/digital lending/mobile loans) are rising in emerging economies, as seen in Africa (Brailovskaya et al., 2021). This could be attributable to the less stringent conditions and criteria for loan eligibility in comparison with regular banks (Ogada & Hammond 2021). Nevertheless, there are attendant ills such as harassment, data privacy violations, and cyberbullying of loan defaulters. In addition, there is evidence of exploitation of personal/private information of DCUs by DCPs, without clear-cut legal repercussions, especially when DCUs fail to repay their loans (Etiebet & Matthew, 2022).

This study will thus make available unique insights into digital data privacy by demystifying the perceptions, experiences, and expectations of DCUs in Nigeria. Furthermore, the study will contribute to the knowledge of conditions and implications of digital data privacy for DCPs and DCUs. The study would generate indigenous data which is important for improved management practices, this will, in turn, influence bespoke policy formulation for the country. As such, this study will fill a major gap in the body of knowledge in this regard by significantly contributing to academia.

The focus on privacy in Nigeria is well-dated. In essence, the privacy concern has been inculcated in the law in various forms. In Nigeria, for example, Sections 37 and 38 of the constitution (1999) have provisions for citizens' right to privacy, freedom of thought, conscience and religion. Hence, privacy is widely acknowledged as a cardinal human right, and it is legally enforceable by law. Besides the provisions of the constitution, the Nigeria Data Protection Commission (NDPC) was established by the Federal Government of Nigeria to implement the Nigeria Data Protection Act (NDPA) 2023. The NDPC serves as the Data Controller and is committed to protecting the privacy rights of natural persons, referred to as Data Subjects

(NDPC, 2024). The NDPA is a subsidiary legislation that regulates public and private sector usage of the personal data of Nigerians.

This from the existing framework for data privacy in Nigeria, has been judged to be inherently weak (Etiebet & Matthew, 2022). The advent of digitalization and digital privacy has become of significant interest to LMICs such as Nigeria, leading to movements, publications, and bills for the inclusion of digital data privacy in the constitution.

The study findings will provide a more elucidated comprehensionof the dynamics of data privacy for digital services in Nigeria. This study will serve as a compass for the next line of action for stakeholders such as the Central Bank of Nigeria, Nigeria Data Protection Commission (NDPC),Financial Technology organizations,National Identity Management Commission (NIMC)and DCPs to mention a few. The perceptions, experiences, and expectations of DCUs brought to the fore by this study will guide the formulation of new policies by regulatory agencies in Nigeria. Such policies are expected to include digital privacy, especially with the high rate of adoption of digital services and loans.

It is also expected that this study will engender increased coverage, precision, and strength of existing legislation for adequate protection of the rights of the populace, especially women, children, the poor, underserved, and marginalized in LMICs. Hence, this study addresses the perceptions, experiences, and expectations of DCUs about data privacy in the study area.

2. REVIEW OF LITERATURE

Previous research on data privacy focused on the broader context without particular interest and attention to digital data privacy (Abdulrauf & Fombad, 2017; Akanbi & Ajepe, 2012; Babalola, 2021). Other studies (Björkegren et al., 2021; Brailovskaya et al., 2021; Suri et al., 2021) have explored the impacts of digital credits on the welfare of DCUs, but not from the perspective of digital data privacy and its ethical implications. These researchers also noted several detrimental effects of implementing digital credits in LMICs, particularly with data privacy and its violation. These are indicators of significant gaps in knowledge and the digital data protection regulatory systems.

Despite the previous theories that have been applied to the study of data privacy, applying the stimulus theoretical framework (Lai et al., 2016), a technology model, in this study will enhance a clearer understanding of digital data privacy in the relationship between DCPs and DCUs.

2.1. The Concept of Privacy

In an era marked by the relentless growth of data, the importance of safeguarding privacy come to the forefront. This is evident in the database community's increasing focus, as reflected in the substantial surge in research papers on the subject. Consequently, numerous propositions have been made concerning its definition.

The concept of privacy as seen by Solove (2002, as cited in Ilobinso 2022), is characterized as a comprehensive concept. Entailing amongst various elements, the liberty to think independently, authority over one's physical being, seclusion within one's abode, power over personal data, immunity from monitoring, safeguarding one's repute, and shielding against invasive interrogations. Altman (1975, as cited in Amao and Ilesanmi 2022) gives another definition of the concept of privacy. They portray it as an individual or a collective entity's capacity to isolate

themselves or selectively reveal information about themselves while retaining the power of choice in self-expression.

The roots of privacy as traced by Fapetu (2020), initially emerged within the framework of English common law, with a primary focus on delineating regions in which individuals were independent and protected from state intervention. Building upon this foundation, Francisco (2020) mentioned that privacy was subsequently recognized as a fundamental human right by the United Nations in response to the state-perpetrated atrocities witnessed during World War II. The right to privacy is also embedded in the Nigerian constitution, as Alafaa (2022) pointed out. The constitution unequivocally affirms the protection of citizens' privacy, the right to privacywithin their residences, personal and telephone correspondenceand any personal data about the individual.

Subsequently, Odiaka et al. (2022) observed that the provision of the constitutional section makes it evident that the entitlement to secrecy holds a central position in any democratic society. Alafaa (2022) noted that it also serves as the foundationfor recognizing information privacy and protecting rights in Nigeria. This perspective resonates with Ololuo's (2020) argument that the rule governing information concealment are inherently rooted in the Nigerian Constitution.

2.2. Digital Data Privacy

In the work by Anya and Jaiyebo (2023), reference is made to the Terrorism Act, which defines data. Data is seen as information that is generated, transmitted, received, or stored and can be retrieved through electronic, magnetic, optical, or analogous methods. Data has become an essential resource to the extent that Adeoti (2023) highlighted the adoption of the colloquial term "the new oil" to describe its significance. This comparison is drawn from the idea that, when collected, managed, and stored effectively, data serves as a valuable asset, much like how oil does. Nonetheless, akin to oil, mishandling or improper storage of data can result in dire consequences. Hence, the adoption of data privacy.

According to Greenleaf (2018, as cited by Odiaka et al. 2022), the notion of "data privacy" began to garner attention around the middle of the 20th Century. Before that era, an individual's notion of "privacy" was confined to physical manifestations connected to them, such as documents, their dwelling, and their day-to-day personal undertakings. Albers (2013, as cited by Odiaka et al. 2022) suggested that we can infer that the concept of data privacy emerged as an extension of the widely acknowledged concept of privacy, functioning as a safeguard to oversee the accumulation, processing, and utilization of individual data, particularly in response to the rapid advancements in technology.

Based on Odiaka et al. (2022), a comprehensive and precise definition of data privacy remains elusive. They note that the challenge primarily arises from the contextualization of these concepts, where they are defined as safeguarding the information, data, and communication of individuals within a specific jurisdictional domain. Ultimately, they recognized that privacy had become a universally acknowledged fundamental human right and, accordingly, concluded that the concept of data privacy originates from this widely accepted idea of privacy. From this standpoint, Umeh (2022) characterizes data privacy as the right of citizens or individuals to exert control over the gathering and usage of their personalized data.

In a similar vein, Alafaa (2022) crafted a definition for data privacy. She described it as the right of individuals to exercise authority over the accessibility of their data and the specific personal information they choose to disclose. Furthermore, she extended this definition by emphasizing

that data privacy entails protecting this data from unauthorized individuals or entities who should not have any legitimate access to it.

Data privacy is a subject that is addressed by diverse legal frameworks, each tailored to the specific needs of various countries and regions. Among these, Lovell and Foy (2018) made mention of the far-reaching impact of the European Union's General Data Protection Regulation (GDPR), which laid down stringent benchmarks for safeguarding data on a worldwide scale. As mentioned by Babalola (2021), Nigeria has also embarked on a regulatory path to oversee data privacy and security by introducing the Nigeria Data Protection Regulation (NDPR) in 2019. This, as expressed by Ilobinso (2022) and Odiaka et al. (2022), is greatly influenced by the GDPR.

As examined by Alafaa (2022) and Odiaka et al. (2022), the Nigerian government, acting through its agency, the National Information Technology Development Agency (NITDA), established under the NITDA Act, 2007, introduced the NDPR. This regulation was designed to provide comprehensive oversight and control over access to users' data within the country. Before the implementation of the NDPR, as Ekweozor (2020) elaborated, there was no dedicated legislation specifically focused on regulating data privacy and protection. Collectively, these legal frameworks contribute to a global effort to safeguard individuals' data privacy rights, highlighting the international acknowledgement of data privacy's importance, particularly in the digital age, as reflected in its definition.

Ekweozor (2020), described digital data as a digital form comprising of characters, symbols, and binary elements used in computer operations. It can be stored or transmitted as electronic signals in various formats and on different devices. Therefore, the internet and smart-phones play a crucual role in improving the value, accessibility, and abundance of digital data. Anya and Jaiyebo (2023) discussed how in 2018, Nigeria saw a staggering 53 million smart-phones connected to the internet. Moving forward to 2021, there were a staggering 108 million internet subscribers, collectively consuming an impressive eighty million gigabytes of data monthly. This surge resulted in a remarkable increase of over 200 per cent in digital data generation between 2019 and 2022. As our homes, vehicles, timepieces, and mobile devices become increasingly linked to the internet, the potential for data generation grows exponentially. These considerations underscore the necessity for digital data privacy.

By blending the definitions of privacy with the digital domain, Leatham (2017) suggested that digital data privacy can be conceptualized as the ability to exercise authority over safeguarding one's online data from unwarranted intrusions. As suggested by Gülsoy (2015), digital data privacy can be explained in simple terms as the entitlement to concealment for consumers of digital media.Gülsoy (2015) highlights two key aspects of digital data privacy: the loss of control over personal data and the intrusion of unauthorized parties. These concerns stem from users' online activities and the unauthorized revelation of their data to third parties.

Delving deeper into the concerns of unauthorized utilization of personal data, as indicated by Carson (2021, as cited by Alafaa, 2022), users possess the entitlement to provide consent for the gathering of their data and should be afforded the opportunity to exercise this right. Alafaa (2022) additionally emphasizes the importance for companies to furnish users with comprehensive steps undertaken to safeguard data against breaches as integral components of their privacy policies.
These policies, prominently displayed on a company's website, should elucidate to users the nature of personal information collected, its intended purposes, the parties with whom it may be shared, and the security measures in place. Such transparency regarding data collection, sharing, and management is the company’s ethical responsibility.

Odusote (2021)expressed that the frequency of digital data privacy concerns being reported is on the rise in Nigeria. There are numerous companies, including prominent multinational corporations, facing substantial security threats and breaches. These incidents have led to the infringement of customer privacy rights and inflicted significant harm on their corporate reputations.

Banubakode et al. (2022) set an example of a breach that happened in a prominent multinational corporation. The breach of Yahoo's computer network, which was previously believed to have impacted one billion accounts in 2013, was revealed by Verizon Communications, Yahoo's parent company, to have affected all three billion user accounts. This major breach resulted in the exposure of critical user information, such as names, birth-dates, phone numbers, and inadequately encrypted passwords. Additionally, it impacted security inquiries and backup email addresses, which could potentially be exploited for unauthorized access to various accounts, including government systems on a global scale.

In conclusion, data privacy and digital data privacy span a diverse spectrum of legal, ethical, and technological dimensions. Data privacy accentuates an individual's control over their personal information in an era marked by burgeoning data quantities and technological progress. Of particular significance is digital data privacy, given the widespread use of the internet and smartphones, enabling the creation and transmission of substantial digital data volumes. This concept revolves around safeguarding one's online personal data from unauthorized intrusions, putting a strong emphasis on maintaining authority over data within the digital realm. A profound comprehension of these concepts is essential in today's interconnected world, where responsible data handling and individual privacy protection are of utmost importance.

2.3. Which Information is Sensitive?

Defining sensitive information is central to its protection. In the digital age, where information is both abundant and easily accessible, the perception of sensitive information in digital data privacy has become a critical concern. As individuals increasingly engage with online platforms, conduct transactions, and share personal details, understanding how sensitive information is perceived and protected is paramount. Hence a need to explore the multifaceted nature of sensitive information in the context of digital data privacy, examining its significance, challenges, and implications for individuals and society.

Some studies investigating the factors influencing individuals' perception of specific information as sensitive have classified data based on their perceived sensitivity. Milne, Pettinico, Hajjat, & Markos, (2016) delineated two groups of data perceived as highly delicate: safe identities (like social security numbers) and monetary details (such as bank and credit card details). The study also observed that basic demographic information (like gender and date of birth) and individual "Penchant" (such as belief and political association) are regarded as less confidential by the participants surveyed.

Similarly, Schomakers et al. (2019) conducted an online cross-national survey targeting German internet users to assess their perception of the sensitiveness of 40 various categories of information. This study compared the German sensitivity evaluations with findings fromBrazil and the United States (Markos et al., 2017) to explore the ethnic influences on these assessments. While some notable variation in sensitivity cognition were identified among the United States, Brazil and Germany, the rating of data sensitivity was quite similar across the countries, suggesting a consensus on what is considered sensitive information globally. Also, factors such as the inclination towards valuing concealment, risk inclination, and educational attainment were found to impact the sensitivity cognition among individuals.

The work of Malheiros et al. (2013) underscores the user's perspective, indicating that personally identifying items is perceived as more sensitive. However, as technological advancements progress, it is unreasonable to assume that all users comprehend the interconnectivity of data for individual identification. Moreover, assessing the risk of users is extremely prejudiced (Renn, 1989). The conceptualization of risks and the perceived necessity of internet securityare significantly influenced by the context of usage (Asplund & Nadjm-Tehrani, 2016).

Similarly, defining data sentiency as the likelihood of loss associated with the exposure of that data underscores the subjective nature of sensitivity evaluations (Mothersbaugh et al., 2012). Additionally, various data forms are connected with distinct kinds of risks (Milne et al., 2016). For example, credit card details are primarily linked with financial hazards, while social media profiles are often related to societal and mental dangers. Markos et al. (2017) delineate a data sensitiveness spectrum by experimentally assessing 52 types of information based on their understanding of sensitiveness and correlating this with the disposition to furnish such data. In essence, the sensitiveness of data is pivotal to online conceptualization of privateness and is contingent upon both the type of information and individual differences.

One of the fundamental challenges in navigating sensitive information in digital data privacy is defining its boundaries and scope. While regulatory frameworks like the General Data Protection Regulation (GDPR) provide road map for identifying sensitive information, the evolving nature of technology and data collection practices complicates this task (Bergström, 2015). Moreover, individuals may have varying perceptions of what constitutes sensitive information, influenced by their personal experiences, privacy preferences, and levels of trust in digital platforms (Schomakers et al., 2019).

The perception of delicate data is closely intertwined with issues about privacy, security, and trust in digital environments. Users are becoming more cautious of the possible dangers linked to disclosing personal information online, such as identity theft, data breaches, and unauthorized surveillance (Rice & Bogdanov, 2019).Heightened awareness of privacy issues, fueled by high-profile incidents of data misuse and surveillance, has led to growing demands for greater transparency, control, and accountability from digital service providers (Powell et al., 2022).

Transparency and consent play crucial roles in shaping individuals' perceptions of sensitive information in digital data privacy. Users expect clear explanations of how their data is gathered, utilized, and distributed, as well as the ability to make informed choices about its disclosure (Koolen, 2020). However, complex privacy policies, opaque data practices, and the prevalence of third-party data sharing often undermine users' trust and confidence in digital platforms (LaMonica et al., 2021; Chen et al., 2022).

Cultural and societal norms also influence the perception of sensitive information and privacy expectations. While some cultures may prioritize individual autonomy and privacy rights (Power, Heavin, & O'Connor, 2021), others may place greater emphasis on communal values or collective security (Ekmekci, & Arda, 2017).

Recognizing these cultural subtleties is crucial for crafting inclusive and user-centered privacy solutions that honor varied viewpoints and preferences. Moreover, the advent of novel technologies like artificial intelligence (AI) and machine learning introduces both possibilities and hurdles in handling sensitive digital information.While AI algorithms can enhance data security and privacy through encryption, anonymization, and predictive analytics, they also raise concerns about algorithmic bias, discrimination, and unintended consequences (Siva, 2024).

In conclusion, the perception of sensitive information in digital data privacy is a complex and evolving landscape shaped by technological advancements, regulatory frameworks, cultural norms, and individual attitudes. Successfully traversing this terrain necessitates a comprehensive strategy that harmonizes the advantages of data-driven innovation with the safeguarding of individual privacy rights. Throughtransparency, accountability, and user empowerment, we can cultivate a more dependable and robust digital environment that upholds the importance of personal information sensitivity and preserves individuals' privacy in the digital era.

3. METHODOLOGY

This section outlines the systematic approach employed to address the research objectives. It elucidates the methods chosen to gather, analyze, and interpret data, ensuring rigor and reliability in the study's findings. It serves as a blueprint, offering insight into the study's design, participant selection criteria, data collection instruments, and analytical techniques employed, thereby providing transparency and facilitating reproducibility.

3.1. Design and Setting

The study adopted a qualitative approach in a cross-sectional survey to harvest a myriad of data for a better understanding of the perceptions concerning data privacy practices for digital credits in Nigeria. This was achieved via in-depth interviews (IDI) with DCUs in the study area. Nigeria, has a very high number of DCUs, with the prevalence rate of subscriptions for digital financial services at 35% (EFInA, 2021).

3.2. Sampling

A multi-stage sampling technique, comprising cluster, purposive, and systematic random sampling techniques was adopted. Cluster sampling is a type of probability sampling technique often used to study large populations, particularly those with extensive geographic spread. Since Nigeria can be divided into six (6) zones, these pre-existing zones were taken as clusters. One zone (cluster) with a constellation of economic hubs was purposively selected to represent the country. The three stages of sampling are presented as follows.

Stage One

Nigeria has six geopolitical zoneswhich are North-East, North-West, North-Central, South-West, South-East and South-South, (https://en.wikipedia.org/wiki/Geopolitical_zones_of_Nigeria); each zone is subdivided into six (6) states. The South-West zone was purposively selected due to its constellation of economic hubs. The three (3) states with the highest economic activity in the zone - Lagos, Oyo, and Ogun States were purposively selected, and 40 DCUs were interviewed per state, for a total of 120 DCUs in Nigeria.

Stage Two

The states are further divided into Local Government Areas (LGA), the lowest level of government. Four (4) LGAs are purposively selected per State, based on four criteria – Central Business Districts, Rural, Urban & Peri-urban (See Table 1 for details). 10 DCUs were interviewed in each LGA.

Table 1: List of States and LGAs sampled

	STATES		
LGA Type	**LAGOS**	**OYO**	**OGUN**
Central Business District (CBD)	Ikeja	Ibadan South-West	Abeokuta North
Urban	Surulere	Ibadan North	Abeokuta South
Peri-Urban	Agege	Egbeda	Ijebu North
Rural	Epe	Ibadan South-East	Obafemi Owode

Stage Three

In each of the selected LGAs, DCUs were interviewed using the Systematic Random Sampling technique. Every nth household was selected.The sampling frame (number of houses) for each Local Government Area (LGA) was established using data from the National Household Survey.The nth term for each LGA will be determined by dividing the sampling frame by 10 (the number of participants required per LGA). Nevertheless, the initial participant was chosen randomly from among the first 'n' participants.

3.3. Instrument and Procedure

A structured interview guide was developed for this study. The draft interview guide was subjected to face and content validity, such that rejected items were deleted. The final guide contains 20 items; 5 demographics and 15 interview questions with probes. Research assistants were recruited, trained, and deployed to conduct in-depth interviews (IDIs) with consenting DCUs in each of the selected LGAs. Interview transcripts were cleaned, coded, and thematically analyzed using NVIVO 14.

3.4. Ethical Consideration

Research involving humans is obligated to adhere to specific ethical principles. Hence, this study abided by such. National and Institutional Review Board of Nigeria - National Health Research Ethics Committee (NHREC) approved the study protocol before commencement. At the core of this study are considerations encompassing informed consent, namelessness, cultural competency, beneficence, privacy, voluntariness, confidentiality, debriefing and risk-benefit ratio to mention a few. All participants were at/above the age of consent; hence, their consent was obtained before each interview; they were also informed of and afforded the right to withdraw from the study at any stage, a principle that was duly respected.

Hypothetical names/codes were used to conceal the identity of participants while ensuring no sensitive questions were asked. The questions were well adapted to the cultural orientation of the participants and designed for their benefit. Since deception was not employed, participants were given the chance to clarify any aspects of the research that appeared unclear at the conclusion of all interactions.

4. RESULTS AND DISCUSSION

This section presents the outcomes of the study's investigation, elucidating key findings and their implications within the context of the research objectives. It serves to synthesize the data collected, analyze patterns, and interpret the results. Through a comprehensive examination of the findings, this section provides insight into the research questions, highlight significant trends, and offer a deeper understanding of the phenomenon under study.

4.1. DCUs' perceived Sensitive Information

The information requested by DCPs from DCUs before they are given digital credits or mobile loans is diverse. Findings show that DCUs consider this information as sensitive, such information includes Bank Verification Number (BVN), National Identification Number (NIN), debit card details, guarantor details, personal contacts of DCUs, phone number, and address of DCUs. The information considered highly sensitive by DCUs is the BVN (33.33%) followed by the NIN (16.67%) and debit card/ATM details (11.90%) as shown in Table 2 and Figure 1 below.

Table 2: DCUs Perceived Sensitive Information

WORD	LENGTH	COUNT	WEIGHTED PERCENTAGE (%)
BVN	3	28	33.33
NIN	3	14	16.67
GUARANTOR DETAILS	16	7	8.33
DEBIT CARD/ATM	12	10	11.90
PHONE NUMBER	11	6	7.14
PERSONAL CONTACT	23	8	9.52
ADDRESS	19	4	4.76
INTERNATIONAL PASSPORT	21	4	4.76
CVV	3	1	1.19
DRIVER LICENSE	13	2	2.38
	TOTAL	**84**	**100.00**

Figure 1: Word Cloud of DCUs Perceived Sensitive Information

The question directed to DCUs about the types of information they perceived to be sensitive yielded responses such as those presented below.

Responses:

"Except from BVN, I feel that's all I see to be sensitive."

"My home address. It's sensitive because nothing is safe, especially with all these microfinance banks where maybe a staff is laid off and they use the opportunity to get your information and start to come to people's home addresses. An example is also turning on your location which palmpay then used to track people and visit people in their homes."

"BVN and ATM card details and the CVV."

The significance attributed to the BVN by DCUs underscores its critical role as a unique identifier linked to individuals' banking activities and financial transactions. Given its association with financial records and identity verification processes, DCUs likely perceive the BVN as central to their financial security and privacy. Fraudulent activities, identity theft, or unauthorized access to financial accounts are common consequences of any compromise or unauthorized access to this information. Similarly, the recognition of other identifiers such as the NIN, debit card details, and personal contacts as sensitive highlights their role in facilitating financial transactions and identity verification processes. DCUs are likely cognizant of the possibleperils linked with divulging such information, which may encompass financial fraud, impersonation, and privacy infringements.

The inclusion of guarantor details in the list of sensitive information underscores the trust and confidentiality associated with guarantor relationships in credit transactions. Revealing such information could potentially impact the relationship between DCUs and their guarantors, as well as expose both parties to financial risks. Moreover, the sensitivity attributed to personal contacts, phone numbers, and addresses reflects DCUs' concerns about privacy and unauthorized access to their personal information. In an era where digital privacy breaches are increasingly common, DCUs are likely cognizant of the risks posed by the disclosure of such details, including unsolicited communication, harassment, or identity-related crimes.

4.2. Obligation to Divulge

Regarding the level of obligation of DCUs to divulge their information to DCPs before gaining access to digital credits/mobile loans, results show that DCUs are highly obliged to divulge. Oftentimes, DCUs are in dire need of the funds, hence they could be desperate to give whatever information is requested by the DCPs just to access the loans. Some of the DCUs however reveal that they are not obliged to divulge, while the least category is that of DCUs who are moderately obliged to divulge information to DCPs as depicted in Figure 2.

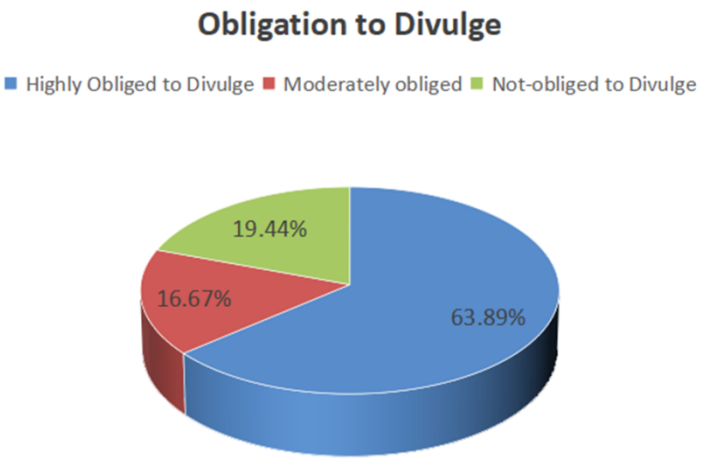

Figure 2: Obligation to Divulge

The urgency of financial constraints may lead DCUs to prioritize immediate access to credit over concerns about data privacy or security. For many DCUs, the pressing need for financial assistance may outweigh any reservations they have about sharing sensitive information.

Digital credit may serve as a crucial lifeline for individuals confronting financial hardship or emergencies in scenarios where traditional lending options are unaccessible. Consequently, DCUs may perceive divulging personal information as a necessary trade-off for accessing much-needed funds, even if it entails potential risks to their privacy or security.In response to the question about DCUs' obligation to divulge personal information to DCPs, participants provided some information as presented below.

Responses:

"when I need to get the money needed at that moment and I see that without these info needed I can't get the money, I would release the info."

"When there is a need for it especially when there is money loan involved in this scenario and there is a benefit that is accrued to this aspect. Some even go to an extent of due to the need, they would provide all the necessary info needed."

Nonetheless, it's important to acknowledge that not all Digital Credit Users (DCUs) feel equally compelled to disclose their personal information to Digital Credit Providers (DCPs). Some individuals may assert their right to privacy and refuse to divulge certain details, particularly if they have concerns about the legitimacy or trustworthiness of the digital credit provider. These DCUs prioritize safeguarding their personal information over immediate access to credit, reflecting a more cautious approach to digital lending. Additionally, there is a subset of DCUs who fall somewhere between feeling highly obliged and entirely reluctant to divulge information to DCPs. They evaluate the advantages and drawbacks of sharing personal data individually considering items such as the loan terms, the reputation of the Digital Credit Provider, and their own financial situation. Their inclination towards data disclosure could vary based on the perceived advantages and dangers linked with the transaction.

4.3. Types of Risk Perceived by DCUs

Taking into account the types of risks perceived by Digital Credit Users (DCUs) depending on the extent of information shared with Digital Credit Providers (DCPs), these perceived risks

encompass financial risk and scams, the possibility of DCUs' information being accessed by unauthorized parties, DCPs contacting individuals in DCUs' contacts, potential data breaches or misuse, public shaming of DCUs, and DCPs reaching out to DCUs' guarantors. The greatest risk perceived by DCUs is financial risk and scams (60.61%), followed by the likelihood of DCUs'data falling into the wrong hands (15.15%), DCPs reaching out to DCUs'contacts and data breach/ misuse (9.09%), and lastly shaming of DCUs and DCPs reaching out to DCUs guarantors (See Figures 3 and 4). The perception of DCUs reveals that they are afraid that their information shared with DCPs could expose them to the aforementioned risks.

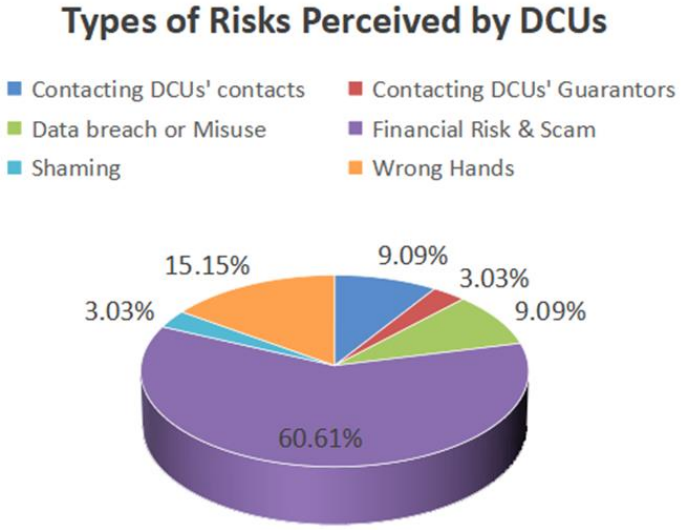

Figure 3: Types of Risk

Figure 4: Word Cloud of Types of Risks Perceived by DCUs

The heightened concern about being at risk of financial loss and scams indicates that DCUs are acutely aware of the prevalence of financial scams and fraudulent activities in the digital realm, and they fear falling victim to such schemes. Given the sensitive nature of financial transactions and the potential for exploitation by malicious actors, DCUs prioritize safeguarding their financial assets and identities. DCUs' concern about the possibility of their information falling into the wrong hands also remains significant. This includes the risk of identity theft,

unauthorized access to personal data, and potential misuse of sensitive information for fraudulent purposes.

Some of the responses provided by DCUs to the question about anticipated risks associated with the provision of their details to DCPs are as follows.

Responses:

"The BVN details could lead to fraudulent acts by the people."

"The aspect of using my personal details to conduct other forms of activities."

DCUs recognize the potential consequences of their data being compromised, such as financial fraud, reputational damage, and loss of privacy. DCUs' apprehension about DCPs reaching out to their contacts, which could result in unwanted solicitation, invasion of privacy, or embarrassment underscores DCUs' value for their relationships. Therefore, they may hesitate to expose their personal contacts to unsolicited communication or to the possible risks linked with personal information sharing. Data breaches or misuse represent another significant risk perceived by DCUs. In an era marked by growing instances of data breaches, Digital Credit Users (DCUs) are cautious about entrusting their information to Digital Credit Providers (DCPs) without guarantees of robust security measures and data protection protocols. The potential repercussions of data breaches, such as identity theft, financial loss, and reputational harm, significantly influence DCUs' decision-making processes.

Additionally, DCUs' concerns about the possibility of public shaming, whereby their financial difficulties or borrowing activities are exposed to public scrutiny or judgment reflects their fear of social stigma or negative repercussions which may deter DCUs from seeking digital credit or disclosing certain information to DCPs.

Finally, concerns about privacy, consent, and the integrity of guarantor connections are raised by the possibility of DCPs contacting the guarantors of DCUs.. DCUs may be hesitant to involve their guarantors in digital credit transactions, fearing potential strains on their relationships or the imposition of financial obligations on their guarantors without their explicit consent.

4.4. Likely Reaction to Privacy Breach

Findings reveal that DCUs would rather not proceed with the digital credits/mobile loans application process if there is any likelihood that their privacy would be breached. Hence most of the DCUs would exhibit what can be termed as "breach-motivated withdrawal" as shown in Figure 5.

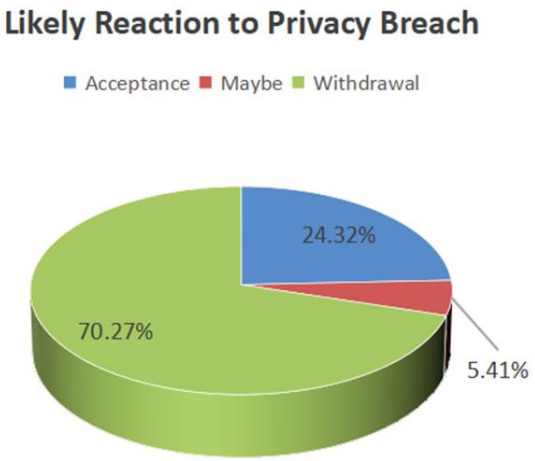

Figure 5: Likely Reaction to Privacy Breach

This withdrawal behaviour underscores the paramount importance that DCUs place on safeguarding their personal information and privacy. It reflects a reluctance to engage with digital credit services if there are perceived risks to their privacy, even if it means forgoing access to much-needed financial assistance. The choice to pull out from the application cycle is driven by a craving to moderate potential dangers related to information breaks, unapproved access, or abuse of individual data. This phenomenon highlights the critical role that trust and confidence play in the digital credit ecosystem. DCUs must have confidence that their personal information will be handled responsibly and securely by digital credit providers. Any perceived threat to their privacy undermines this trust and prompts DCUs to prioritize privacy preservation over financial convenience.

When the respondents were inquired, for example, whether they could have proceeded with the loan decision par adventure they realized their security would be compromised, an excerpt of their responses are presented as follows

Responses:

"No, I cannot."

"No. I would rather stop."

"At all."

"At all ooo"

From a broader perspective, breach-motivated withdrawal reflects the growing awareness and concern among individuals about digital privacy risks. In an era where data breaches and privacy violations are increasingly common, DCUs are becoming more vigilant and discerning about sharing their personal information online. They recognize the potential consequences of privacy breaches, including identity theft, financial fraud, and reputational damage, and are therefore unwilling to take unnecessary risks with their data.

To encourage trust and commitment, DCPs should consider and manage the privacyconcerns of DCUs. This can be achieved via the implementation of robust digital data privacy policies, transparent data handling practices, and effective security strategies that has the potential to

assure and alleviate DCU's concerns about privacy breaches. Besides, offering clear and accessible data on the use, storage, and protection of individual information can enable DCUs to take informed choices regarding their privacy and financial well-being.

4.5. DCU's Desire for Control Over Personal Information

Among DCUs, the desire to have control over the information supplied to DCPs is quite high. Findings show (See Figures 6 and 7) that most of the DCUs would rather have control over how their information is used by DCPs. This inclination towards retaining control underscores the importance that DCUs place on autonomy and agency in managing their data.

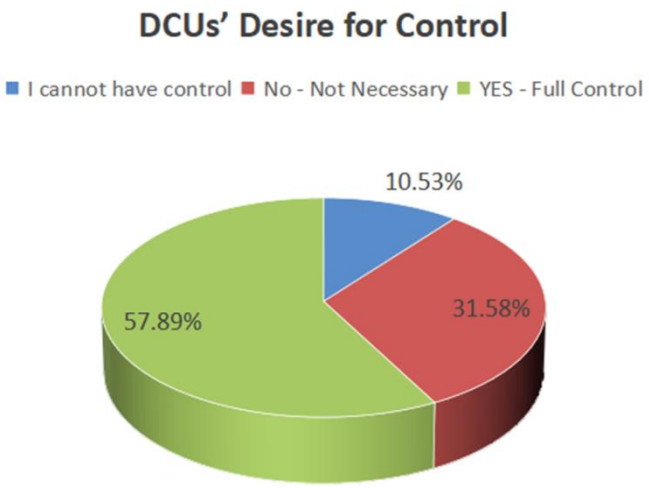

Figure 6: Desire for Control Over Personal Information

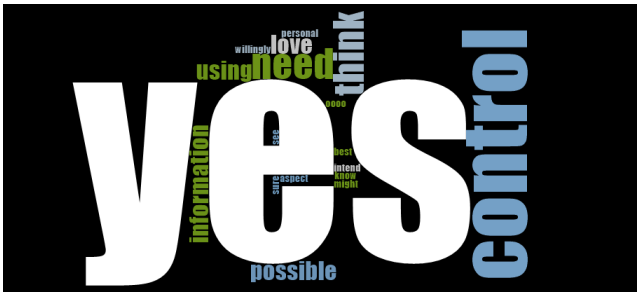

Figure 7: Word Cloud Showing Desire for Control Over Personal Information

The inclination to manage information provided to DCPs mirrors DCUs' anxieties regarding privacy, data security, and the possible misuse of their personal information. DCUs recognize the sensitivity of the information they share, particularly when it pertains to financial details, personal identifiers, and contact information. By exerting control over how their information is used, DCUs seek to safeguard their privacy, minimize risks, and maintain a sense of ownership over their data. This preference for control aligns with broader trends in digital privacy and data protection, where individuals increasingly assert their rights to control the gathering, utilization, and divulgence of their personal data.This trend is driven by growing awareness about privacy risks, data breaches, and the implications of sharing personal data in digital environments. DCUs are becoming increasingly aware of the significance of exercising control over their information to mitigate potential privacy violations and protect their interests.

As revealed by the responses of DCUs to the question on their desire to have control over the information supplied to DCPs.

Responses:

"I would love to"

"Yes."

"If I have access to do that, I willingly will have control."

Psychologically, the longing for control over personal data can be ascribed to autonomy, trust, and self-determination. DCUs value the ability to make enlightened choices regarding their data andexert influence over how it is managed by DCPs. By retaining control, DCUs seek to maintain a sense of autonomy and agency in their interactions with digital credit providers, thereby enhancing their trust and confidence in the digital credit ecosystem.

For DCPs, understanding and respecting DCUs' desire for control is essential for building trust and fostering positive relationships. Providing DCUs with greater transparency, choice, and control over their information can help alleviate privacy concerns and enhance engagement with digital credit services. Furthermore, embracing privacy-enhancing technologies and implementing strong data protection measures can showcase DCPs' dedication to respecting the privacy rights of DCUs and upholding trust within the digital credit ecosystem.

5. CONCLUSION AND RECOMMENDATION

This study examines the perceptions, experiences, and expectations of DCUs about data privacy in the study area. This study demonstrates that BVN and NIN are sensitive information about DCUs collected by DCPs. Similarly, evidence suggests that most DCUs experience a high obligation to divulge their personal information to DCPs given the fact that they are often desperate and have little or no choice. If they fail to provide the requested information, they will not be granted the credits/loans. This study provides additional evidence indicating that financial risks and scams are the greatest risks perceived by DCUs to be associated with the action of divulging personal information to DCPs.

In summary, DCUs' perceptions of risk associated with providing information to DCPs reflect their concerns about financial security, privacy, identity protection, and social consequences. Addressing these concerns requires DCPs to enforce vigorous safety practices, lucid information management measures and ethical communication strategies to foster trust and mitigate risks in the digital credit ecosystem. Balancing the imperative of financial inclusion with the imperative of data protection is essential for building a sustainable and trustworthy digital credit ecosystem that prioritizes the interests and well-being of DCUs.

Overall, the identification of certain information types as sensitive highlights the importance of robust data protection measures and privacy safeguards in digital credit transactions. Providers of digital credit services must prioritize the security and confidentiality of DCUs' personal information to foster trust, mitigate risks, and ensure compliance with regulatory requirements. Additionally, empowering DCUs with greater control over their data and enhancing awareness about privacy best practices can further strengthen their confidence in digital credit platforms.

Concurrently, the level of obligation felt by DCUs to divulge personal information to DCPs varies depending on individual circumstances, financial needs, and risk perceptions. While some

DCUs may prioritize immediate access to credit and willingly share sensitive information, others may exercise caution and assert their right to privacy. Understanding these dynamics is essential for DCPs to develop transparent and ethical practices that respect DCUs' privacy rights while meeting their financial needs. However, DCU's breach-motivated withdrawal among underscores the fundamental requirement for trust, transparency, and accountability in how digital credit providers handle personal information.By prioritizing privacy preservation and addressing DCUs' concerns about data security, the digital credit industry can build a more resilient and trustworthy ecosystem that promotes financial inclusion without compromising privacy rights. It is no gainsaying to reiterate that the strong desire for control over information among DCUs, a reflection of a fundamental need for autonomy, privacy, and trust in digital credit transactions is a fundamental right that needs safeguarding. Hence, empowering DCUs to maintain control over their data will enhance DCPs' promotion of transparency, accountability, and ethical data practices, thereby fostering a more secure and trustworthy digital credit environment for all stakeholders.

ACKNOWLEDGMENTS

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].

REFERENCES

[1] Abdulrauf, L.A., & Fombad, C.M. (2017). Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms. Liverpool Law Review, 38, 105-134.

[2] Adeoti, E. (2023). A New Era of Data Protection and Privacy; Unveiling Innovations & Identifying Gaps in the Nigeria Data Protection Act of 2023. Social Science Research Network. https://doi.org/10.2139/ssrn.4520238

[3] Akanbi, M. & Ajepe S., "Rule of Law in Nigeria" (2012) 3:1 Journal of Law, Policy and Globalization 1-9 at 3.

[4] 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

[5] Amao, F. L., & Ilesanmi, A. O. (2022). Residents' perception of privacy in selected public housing estates in Ibadan, Nigeria. Urban, Planning and Transport Research, 10(1), 204–233. https://doi.org/10.1080/21650020.2022.2076730

[6] Anya, A. K., & Jaiyebo, O. O. (2023). The concept of "Personal data" in the Nigerian data privacy laws. ResearchGate. https://www.researchgate.net/publication/373490970_The_Concept_of_%27Personal_Data%27_in_the_Nigerian_Data_Privacy_Laws

[7] Asplund, M. & Nadjm-Tehrani, S. (2016). Attitudes and Perceptions of IoT Security in Critical Societal Services. IEEE Access. 4. 1-1. 10.1109/ACCESS.2016.2560919.

[8] Babalola, O., A Bird's Eye Rundown on Nigeria's Data Protection Legal and Institutional Model (March 20, 2021). Available at SSRN: https://ssrn.com/abstract=3808570

[9] Banubakode, A., Darshi, S., & Bhalke, D. G. (2022). Study of Data Privacy and User Data Control. SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, 14(Spl-2 issue), 244–248. https://doi.org/10.18090/samriddhi.v14spli02.8

[10] Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Computers in Human Behavior, 53, 419-426. https://doi.org/10.1016/j.chb.2015.07.025

[11] Björkegren, D, J E Blumenstock, O Folajimi-Senjobi, J Mauro and S R Nair (2021), "Welfare impacts of digital credit: A randomised evaluation in Nigeria", Center for Effective Global Action, unpublished.

[12] Brailovskaya, V., Dupas, P. and Robinson, J. (2022). The impact of digital credit in low-income countries. Columns in VOXEU.https://voxeu.org/article/impact-digital-credit-low-income-countries. Accessed 25/05/22.

[13] Brailovskaya, V, P Dupas and J Robinson (2021),"Digital credit: Filling a hole, or digging a hole? Evidence from Malawi", CEPR Discussion Paper 16848.

[14] Chen, S., Tamilmani, K., Tran, K. T., Waseem, D., & Weerakkody, V. (2022). How privacy practices affect customer commitment in the sharing economy: A study of Airbnb through an institutional perspective. Industrial Marketing Management, 107, 161-175. https://doi.org/10.1016/j.indmarman.2022.08.020

[15] Ekmekci, P. E., & Arda, B. (2017). Interculturalism and Informed Consent: Respecting Cultural Differences without Breaching Human Rights. Cultura (Iasi, Romania), 14(2), 159. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5890951/

[16] Ekweozor, E. (2020). An analysis of the data privacy and protection laws in Nigeria. Social Science Research Network. https://doi.org/10.2139/ssrn.3639129

[17] Etiebet, I. & Matthew, U., (2022). Nigeria: The Online Lending Boom and Data Privacy Concerns In Nigeria. S.P.A. Ajibade & Co. Available at Mondaq: https://www.mondaq.com/nigeria/privacy-protection/1185312/the-online-lending-boom-and-data-privacy-concerns-in-nigeria

[18] Fapetu, S. (2020). Protection Of The Right To Privacy In Contemporary Nigeria: Implications Of Data Protection Laws And. . . Researchgate. Https://Www.Researchgate.Net/Publication/370066861_protection_of_the_right_to_privacy_in_contemporary_nigeria_implications_of_data_protection_laws_and_administration

[19] Gülsoy, T. (2016). Advertising ethics in the social media age. In IGI Global eBooks (pp. 64–81). https://doi.org/10.4018/978-1-4666-9624-2.ch003

[20] Ilobinso, I. (2022). CONSUMER PRIVACY AND DATA PROTECTION IN NIGERIA. ResearchGate. https://www.researchgate.net/publication/366139828_CONSUMER_PRIVACY_AND_DATA_PROTECTION_IN_NIGERIA

[21] Koolen, C. (2020). Transparency and Consent in Data-Driven Smart Environments 7 European Data Protection Law Review 174 - 189, Available at SSRN: https://ssrn.com/abstract=3597736 or http://dx.doi.org/10.2139/ssrn.3597736

[22] LaMonica, H. M., Roberts, A. E., Lee, G. Y., Davenport, T. A., & Hickie, I. B. (2021). Privacy Practices of Health Information Technologies: Privacy Policy Risk Assessment Study and Proposed Guidelines. Journal of Medical Internet Research, 23(9). https://doi.org/10.2196/26317

[23] Leatham, H. (2017). Digital privacy in the classroom: an analysis of the intent and realization of Ontario policy in context. CORE. https://core.ac.uk/display/286916859?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1

[24] Malheiros, M., Preibusch, S., and Sasse, M. A. (2013). "'Fairly truthful': the impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure," in International Conference on Trust and Trustworthy Computing (London: Springer), 250–266.

[25] Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. Journal of Public Policy & Marketing. https://doi.org/10.1509/jppm.15.159

[26] Milne, G. & Pettinico, G. & Hajjat, F. & Markos, E. (2016). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. Journal of Consumer Affairs. 51. 10.1111/joca.12111.

[27] Mothersbaugh D., Foxx W., Beatty S., & Wang S., (2012). Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. Journal of Service Research, 15 (1), pp. 76-98

[28] Odiaka, N., Ichaba, I. J., & Olipede, D. E. (2022). The Need For Data Privacy And Legal Protection In Nigeria. Researchgate. Https://Www.Researchgate.Net/Publication/361770855_the_need_for_data_privacy_and_legal_protection_in_nigeria#Pf2

[29] 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

[30] Ogada, J. & Hammond, P., (2021). The digital credit landscape focuses on Kenya, Nigeria and India. Gates Digital Credit Report. Available at Busara: https://busaracenter.org/report-pdf/Gates-Digital-Credit-Report.pdf

[31] Lai, Yanqing & Saridakis, George & Blackburn, Robert & Johnstone, Stewart, 2016. "Are the HR responses of small firms different from large firms in times of recession?" Journal of Business Venturing, Elsevier, vol. 31(1), pages 113-131.

[32] NDPC (2024). Our Data Privacy Policy. https://www.ndpc.gov.ng/Home/Privacy

[33] NDPR (2019). NIGERIA DATA PROTECTION REGULATION 2019. Nigeria Data Protection Regulation. https://ndpr.nitda.gov.ng/Content/Doc/NigeriaDataProtectionRegulation.pdf

[34] Ololuo, F. (2020). Data Privacy and Protection Under The Nigerian Law. Nigeria. S.P.A. Ajibade & Co. Available at Mondaq: https://spaajibade.com/data-privacy-and-protection-under-the-nigerian-law-francis-ololuo/

[35] Powell, M. (2023). Consent, Background Justice and Patterned Privacy Principles. Political Studies. https://doi.org/10.1177/00323217231167074

[36] Power, D. J., Heavin, C., & O'Connor, Y. (2021). Balancing privacy rights and surveillance analytics: a decision process guide. Journal of Business Analytics, 4(2), 155–170. https://doi.org/10.1080/2573234X.2021.1920856

[37] Rao, K.S. (2022). Digital Lending in India- Progress and Prospects. The Times of India, March 26, 2022. Link: https://timesofindia.indiatimes.com/blogs/udayasrinivas-com/digital-lending-in-india-progress-and-prospects/ Accessed: 15/05/22.

[38] Renn, O. (1989). Risk perception and risk management. 14th Congress of the World Energy Conference.

[39] Rice, M. D., & Bogdanov, E. (2019). Privacy in Doubt: An Empirical Investigation of Canadians' Knowledge of Corporate Data Collection and Usage Practices. Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de L'Administration, 36(2), 163-176. https://doi.org/10.1002/cjas.1494

[40] Salami, K. (2021). Investigation: How Digital Loan Providers Breach Data Privacy, Violate Rights Of Nigerians. Premium Times. https://www.premiumtimesng.com/news/headlines/499999-investigation-how-digital-loan-providers-breach-data-privacy-violate-rights-of-nigerians.html

[41] Schomakers, E., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. International Journal of Information Management, 46, 142-150. https://doi.org/10.1016/j.ijinfomgt.2018.11.01

[42] Siva K. (2024). AI in Data Privacy and Security. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 3(1), 2024, pp. 35-49.

[43] Suri, T, P Bharadwaj and W Jack (2021), "Fintech and household resilience to shocks: Evidence from digital loans in Kenya", Journal of Development Economics 153: 102697.

[44] Tetteh, G.K. Local digital lending development and the incidence of deprivation in Kenya. Financ Innov 9, 102 (2023). https://doi.org/10.1186/s40854-023-00507-0

[45] Umeh, C. N. (2022). APPRAISAL OF DATA PRIVACY AND PROTECTION UNDER NIGERIAN LAW. ResearchGate. https://doi.org/10.6084/m9.figshare.23618541

[46] World Bank, (2022). World Bank Country and Lending Groups. Link: https://datahelpdesk.worldbank.org/knowledgebase/articles/906519-world-bank-country-and-lending-groups Accessed: 16/06/2022.

AUTHORS

Oluwabunmi A. Falebita PhD, [0000-0001-6506-4011] has over a decade of cumulative research and teaching experience in Technology Management 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 the field of Psychology. He has published several scholarly articles and presented at conferences. His research interests are in the domains of emerging technolo gy, forensics, and security.