

Data privacy in digital marketing: implications for civic freedom in Nigeria

Ajaegbu Jeremiah Chinonso

Abstract

The growth of Nigeria's digital economy has expanded digital marketing activities and positioned the country as the largest digital consumer market in sub-Saharan Africa. As digital marketing expanded, so did the systematic collection of personal data from millions of Nigerian internet users. However, most consumers neither fully understood how their personal data was processed nor had they explicitly consented to its use. This study investigated consumer awareness of data privacy within Nigeria's digital marketing ecosystem and the implications of prevailing data practices for civic freedom in relation to the Nigeria Data Protection Regulation (NDPR, 2019) and the Nigeria Data Protection Act (NDPA, 2023). The study employed an exploratory, quantitative research design that included structured surveys and questionnaires administered to 53 Nigerian adult digital consumers. Findings revealed that awareness of formal data protection regulation was significantly low: only 20.8% of respondents had heard of the NDPR, while only 11.3% had heard of the NDPA. About 90.6% of respondents had never read an entire privacy policy. On the issue of civil liberties, 68% of respondents expressed concern that their personal data could be used to influence their political views online. In comparison, 81.1% reported having self-censored at least One online action due to fear of surveillance. The study concluded that Nigeria's consent-based data protection framework would be unable to fulfil its protective functions, given the low awareness of data rights found within the sample. Recommendations are provided for key stakeholders, including the NDPC, digital marketers, civil society, and educational institutions.

Keywords: civic freedom, consumer awareness, data privacy, digital marketing, Nigeria

Ajaegbu Jeremiah Chinonso, ajaegbu.jeremiah@delsu.edu.ng, Department of Marketing and Entrepreneurship, Faculty of Management Sciences, Delta State University, Abraka, Nigeria

The Nigerian Journal of Business and Social Sciences, Volume 13, 2026 (Special Issue)
A Journal of the Faculty of Social Sciences, University of Lagos, Akoka, Lagos, Nigeria
© 2026

1. Introduction

The digital economy will continue to play an important role in Africa. Nigeria is at the forefront of this development, with over 103 million internet users tracked in 2023. Furthermore, there has been a significant increase in mobile internet access across Nigerian urban and suburban areas. Therefore, Nigeria is now the largest digital consumer market on the continent (DataReportal, 2024). Additionally, this level of connectivity within the country has made it easier for data-driven digital marketers to practice their craft using established tools. Digital marketers utilise the following tools worldwide today: targeted advertising, social media analytics, and behavioural marketing.

The commercial logic that drives digital marketing is based on the extraction and analysis of customer data. Through every online search query, social media engagement, mobile app usage, and e-commerce purchases, marketers can extract consent and corresponding levels of customer information to classify and influence a customer's eventual purchasing behaviour. While this has created more efficient businesses and provided consumers with a more relevant shopping experience, it has raised concerns regarding consent, transparency, and the usage of customers' data.

In democratic nations, the right to privacy includes both the protection of personal information by consumers and the protection of individual rights through respect and recognition of One another's rights. When individuals' personal data is collected without informed consent, processed without clarity, and easily manipulated through persuasive advertising and/or otherwise, it creates conditions of mistrust that can limit citizens' free participation in a democracy. A citizen cannot truly make an informed judgment about civic society when they do not know how cookies are used to deliver political advertising to them. Likewise, a consumer will generally not aesthetically enjoy their rights under the law towards their personal data if they have never read and/or cannot understand the Privacy Policy governing that data (Acquisti et al., 2016; Zuboff, 2019).

Nigerian legislation has made some significant progress towards addressing these issues over time. The Nigeria Data Protection Regulation (NDPR), which took effect in January 2019, created new foundations of data protection for the first time in Nigeria, while the Nigeria Data Protection Act (NDPA) became effective in January 2023, which formally created the Nigeria Data Protection Commission (NDPC) as the regulatory authority for data protection and more closely aligned Nigeria's data protection framework with global standards like the European Union's General Data Protection Regulation (GDPR); besides, the intentions behind the legislation and the experience of ordinary Nigerian consumers frequently do not match. The important question is, do ordinary Nigerian consumers know their rights, and are they being treated with respect regarding the digital marketing programs and activities they encounter daily?

Through exploratory research on Nigerian digital consumers, this study seeks to answer questions about consumer awareness of their rights to their data, their experiences with data acquisition in digital marketing, and the implications of data collection for civic freedoms. The study finds that many Nigerian consumers lack the knowledge of how their data is being collected and used by digital marketers. As such, this lack of knowledge poses a substantial risk to civic freedoms in Nigeria.

The study will first review the literature surrounding data privacy, digital marketing, and civic freedom in Section 2. The research methodology is discussed in Section 3, while Section 4 presents and discusses the research findings. Finally, Section 5 offers recommendations regarding policy and practice.

1.2 Research questions

The following research questions will serve as the basis for this investigation:

- i. What level of data privacy awareness do Nigerian digital consumers possess?
- ii. How does data privacy awareness impact consent behaviour among Nigerian digital consumers?
- iii. What are the implications of data privacy concerns for civic freedoms among Nigerian digital consumers?

1.3 Research Hypotheses

The following exploratory hypotheses are proposed to guide the analysis:

- i. There is no significant relationship between data privacy awareness and the extent to which Nigerian digital consumers read and comprehend privacy policies.
- ii. There is no significant relationship between data privacy awareness and consent behaviour among Nigerian digital consumers.
- iii. There is no significant relationship between data privacy concerns and civic freedoms among Nigerian digital consumers.

2. Literature review

2.1 Data privacy in the digital marketing context

Data privacy, defined as the right of people to have control over their personal data, i.e., how it is collected, stored, utilised and shared, is One of the main challenges of the digital world to date (Westin, 1967; Warren & Brandeis, 1890). Data privacy is constantly under attack in the world of digital marketing. Digital marketing channels (i.e., social media sites, search engines, and programmatic advertising exchanges) essentially act as surveillance by collecting user data, developing detailed behavioural profiles, and selling advertisers access to highly targeted audiences (Turow, 2011; Matz et al., 2017). Zuboff (2019) refers to this model as "surveillance capitalism", in which the human experience becomes the raw material used to create behavioural predictions. Consumers are not only the targets of advertisements but also the sources of data whose behaviours, preferences and vulnerabilities are continuously mined. This creates issues beyond commercial exploitation. When political advertising and target marketing are done using the same data infrastructure, the line between consumer data and civic impact disappears. Over the past several years, digital advertising expenditure in Nigeria has seen consistent growth from year to year, with social media platforms, predominantly Meta (Facebook and Instagram) and Google, controlling the highest market share of digital advertising dollars spent in Nigeria (PwC, 2023). These platforms collect a tremendous amount of data on users in Nigeria; however, they are primarily governed by their own global terms of service rather than local data protection requirements that apply to them. This Power asymmetry between platforms and information users is a major focus of this research.

2.2 Consumer awareness and the consent paradox

There is a large amount of research that discusses this "privacy paradox", i.e. that people claim to be concerned about data privacy yet act in ways that are not aligned with their stated concerns, most commonly, by agreeing to terms and conditions without having read them (Barnes, 2006; Acquisti et al., 2016). Across all of the different countries studied, researchers found that the vast majority of users do not read privacy policies, do not understand how their data is being monetised, and frequently do not understand the full extent of the collection practices that are being applied to them (McDonald & Cranor, 2008; Auxier et al., 2019). In Sub-Saharan Africa, there are structural barriers that further reduce consumers' ability to access and use data effectively, including low levels of digital literacy among older adults and rural communities; the use of English-only legal documents creates an additional disadvantage to those who do not speak English; limited ways to independently access information regarding their digital rights; and a general lack of organisations designed to advocate on behalf of consumers' data rights (Calandro & Berger, 2020; Maweu, 2021). The complex language landscape of Nigeria (where over 500 languages are spoken) means that consumers have limited access to the data they need in a language they speak. When consumers are asked for consent but do not fully understand what they are consenting to, the consent they have provided cannot be considered to be meaningful. Both the NDPR and NDPA make consent the primary means for consumers to legitimize the processing of their data; therefore, the extent to which these regulations protect consumers will be determined by their understanding of the content to which they consent.

2.3 Digital rights, civic freedom, and the Nigerian context

The correlation between data privacy and freedom of civic engagement has been explored in detail in political philosophy and digital rights. Alan Westin's original conception holds that without the ability to control the dissemination of One's personal information, an individual cannot maintain an independent opinion, engage with others, or participate in politics free from observation or manipulation (Westin, 1967). Many contemporary scholars have subsequently extended this line of reasoning into a digital context by demonstrating how commercialised data-collection and surveillance mechanisms

have created a chilling effect on political micro-targeting and damaged the substantive public discourse processes of democracy (Lyon, 2014; Deibert, 2019). In Nigeria, this theory has also been shown to have practical manifestations. In the lead-up to the 2023 general election, social media has been used by multiple political entities for targeted political communication. Investigative journalism and civil society organisations have observed the use of data-driven targeting tools by various political campaigns. However, there remains a need for further detailed analysis of how such tools were used (Paradigm Initiative, 2023). The possibility of repurposing consumer data collected by companies for commercial marketing to influence the political sphere demonstrates the civic implications of privacy in marketing. Although there have been many regulatory changes in Nigeria since 2019 to address challenges faced by Nigeria's data protection system, more needs to be done. The Nigeria Data Protection Regulation (NDPR) laid down basic frameworks and principles governing the collection, usage, and sharing of personal data in Nigeria, including obligations related to informed consent, minimisation of data collection, defining purposes for collecting data, and recognition of data rights. In addition, the NDPC was established by the Nigeria Data Protection Act (NDPA) in 2023 to create a fully independent regulatory authority with enforcement powers and to impose criminal penalties for breaches of data protection laws. The NDPA also harmonised Nigeria's data protection laws with international best practices. Some critics claim that the enforceability of these measures is still limited. This applies particularly to the general public's awareness of data protection and cybersecurity issues, as public awareness campaigns were not as comprehensive as they could have been. Possibly due to their nature, digital marketing companies located outside Nigeria, mainly foreign-based platforms, also appear to have limited accountability for compliance with Nigeria's data protection laws (Makulilo, 2016; Osei-Bonsu, 2022).

2.4 Theoretical framework

This study combines three complementary theoretical traditions into a unified conceptual basis that grounds the research questions and exploratory hypotheses. Each theory addresses a distinct dimension of the problem, including individual rights awareness, structural data extraction, and the behavioural gap between stated privacy concern and actual consent practice.

2.4.1 Westin's Privacy Theory

According to Westin (1967), individuals have the right to choose how and when their personal information is disclosed. This is referred to as privacy. The concept of privacy is not only legally protected but also necessary for citizens' civil participation. Individuals who are deprived of meaningful control over their personal information have limited freedom to express opinions, establish relationships, and participate in democratic activities without fear of being monitored or manipulated. Based on the privacy theory, this study is conducted.

2.4.2 Surveillance Capitalism and the Chilling Effect

The primary driving force behind the platform economy, as described by Zuboff (2019), is the extraction, analysis, and Creation of commercial applications that utilise human behaviour to predict and influence future behaviour. Platforms serve both commercial and surveillance purposes, as they provide opportunities for commercial entities to use consumer data for political micro-targeting and political entities (governmental or non-governmental) to influence individual behaviour through commercial channels. The chilling effect, as defined by Lyon (2014) and Deibert (2019), is a social and legal phenomenon that occurs when people believe their online activities are being monitored, leading to changes in their behaviour or in their involvement in democratic processes, such as political expression.

2.4.3 The Privacy Paradox and the Consent Dilemma

Barnes (2006) and Acquisti et al. (2016) identified the "privacy paradox" as the persistent gap between stated privacy concern and actual privacy-protective behaviour, most commonly manifested in users agreeing to terms and conditions without reading them. Solove (2013) expanded on this concept to develop the "consent dilemma," which emphasises that the regulatory framework built around informed and voluntary consent is undermined when those giving consent lack the knowledge to make informed decisions about privacy issues. Additional structural barriers exist for data subjects in Nigeria due to the use of English-only privacy notices within a multilingual society of over 500 languages (Calandro & Berger, 2020) and low digital literacy among certain demographic segments (Maweu, 2021). Taken

together, these three separate but related areas come together to produce an overall theoretical framework: Westin's (1967) theory connects informational self-determination and civic autonomy; Zuboff's (2019) "surveillance capitalism framework" connects the commercial data economy with the potential to inflict political harm; and the privacy paradox/consent dilemma articulates the process through which consent-driven regulatory frameworks might fail in practice.

2.5 Research gap

There is very limited empirical research at the consumer level on awareness of and attitudes toward consumer-level data protection laws and their social/civic implications, despite extensive research on data protection in Nigeria. Much of the work that has been done focuses on the adequacy of Nigeria's data protection legal and regulatory framework and, as such, has primarily been conducted from the perspective of legal/regulatory experts. (Makulilo, 2016; Osei-Bonsu, 2022). This study seeks to address gaps in this research by generating empirical data on Nigerian consumers' awareness and understanding of data privacy in the context of digital marketing, including their views on the social and civic implications of data privacy. In doing so, this study will contribute to the body of evidence on digital rights and civic space in West Africa.

3. Methodology

3.1 Data collection procedure

The study utilised a quantitative research design and adhered to positivist principles. The data collection method utilised was a structured survey instrument that provided a systematic approach to quantifying levels of consumers' awareness, attitudes, and perceptions within this consumer demographic. The study is descriptive, providing an overview of consumers' levels of awareness regarding data privacy protection, and explanatory in its examination of the relationship between their perceived freedom as citizens and their willingness to provide private data. The study population included Nigerian adults aged 18 years and above who regularly use at least One digital platform. Using purposive sampling, participants were selected based on their willingness to engage with digital platforms and provide informed consent. The questionnaires were intended for Nigerian adults (18 years and over) who regularly utilised the internet. Participants were primarily selected via WhatsApp, email and social media networks, supplemented by in-person administration in Abraka, Delta State. This recruitment strategy is believed to have biased the sample towards urban, educated and digitally active citizens, particularly from South-South and Southwestern Nigeria (52.8%). The final dataset contains 53 usable responses. The sample is not adequate to achieve robust population generalisation. It should be regarded as an exploratory dataset to identify initial patterns and generate hypotheses for future large-scale empirical validation. The survey questionnaire had four sections: Section A (demographics), Section B (data privacy awareness and knowledge of the regulations), Section C (experiences with data collection in digital marketing), and Section D (perceived implications on civic freedom). The items used Likert scales (1 = strongly disagree to 5 = strongly agree), as well as both dichotomous (two-choice) and multiple-choice options. Data for the study were collected using Google Forms in May 2025. Data were collected by sending a survey link via WhatsApp, email, and social media, supplemented by in-person administration in Abraka, Delta State. No identifiable information was collected from participants, and participation in the survey was anonymous and voluntary. This study was conducted in compliance with the ethical standards of Delta State University, Abraka. As the study did not involve any medical procedures or sensitive personal identifiers, and all participants gave full voluntary participation with informed consent, it was not required by the institution's research ethics policy to seek formal Institutional Review Board (IRB) approval. The research remained consistent with the principles of beneficence, non-maleficence and respect for participant autonomy.

3.2 Data analysis

Data gathered were analysed using IBM SPSS Statistics version 26. Descriptive statistics (frequency distribution, percent distribution), mean score, and standard deviation were used as analyses, along with chi-square tests and Pearson product-moment correlation. A p-value < 0.05 was used to determine statistical significance. A methodological limitation is the use of Pearson correlation between a dichotomous awareness variable and Likert-scale civic confidence scores, which typically requires reliance on unbiased semiparametric alternatives, such as Spearman's rho, for this variable pairing.

4. Findings and Discussion

4.1 Demographic profile of respondents

A total of 53 valid responses were analysed (58.5% female and 41.5% male). Most respondents were aged 18-24 (52.8%), followed by 25-34 (41.5%). This subset reflects the youth as the primary users of the internet in the country. Most respondents had university degrees (69.8%) and were from South-South (41.5%), South-West (39.6%) and South-East/North (18.9%) Nigeria. Over half of the respondents (50.9%) reported spending more than 5 hours daily on internet platforms.

Table 1

Demographic Profile of Respondents (n = 53)

Variable	Category	n	%
Age	18 – 24 years	28	52.8
	25 – 34 years	22	41.5
	35 – 44 years	3	5.7
Gender	Female	31	58.5
	Male	22	41.5
Education	Bachelor's degree	37	69.8
	Secondary school	8	15.1
	Diploma / Vocational	5	9.4
	Postgraduate degree	3	5.7
Region	South-South	22	41.5
	South-West	21	39.6
	South-East / North	10	18.9
Daily screen time	5 hours or more	27	50.9
	3 – 4 hours	20	37.7
	1 – 2 hours / Less than 1	6	11.3

4.2 Consumer awareness of data privacy rights and regulations

While 75% of respondents were aware that online platforms collect personal information, only a few were aware of any government regulation governing this data, leading to a clear gap between general awareness and knowledge of legal protections. In particular, 20.8% of respondents were familiar with the NDPR (2019), while only 11.3% were aware of the more recent NDPA (2023), suggesting that public information dissemination has not kept up with changes in data protection legislation. A mere 24.5% knew about the NDPC. Similarly, 90.6% had never read a comprehensive privacy policy. Individuals had a limited understanding of legal rights related to data control, with 30.2% acknowledging their right to request access to personal information and 22.6% knowing how to complain to the NDPC, suggesting that few individuals have sufficient awareness to exercise their data rights.

Table 2

Consumer Awareness of Data Privacy Rights and Regulations (n = 53)

Awareness Measure	Aware (n)	%	Not Aware (n)	%
Platforms collect personal data (Q9)	40	75.5	13	24.5
Browsing used to personalise ads (Q10)	40	75.5	13	24.5
Ever read a full privacy policy (Q11)	5	9.4	48	90.6
Aware of NDPR 2019 (Q12)	11	20.8	42	79.2

Aware of NDPA 2023 (Q13)	6	11.3	47	88.7
Aware of NDPC (Q14)	13	24.5	40	75.5
Right to access personal data (Q15)	16	30.2	37	69.8
Right to delete personal data (Q16)	18	34.0	35	66.0
Right to complain to NDPC (Q18)	12	22.6	41	77.4

The Likert scale results support these findings, with all four NDPR-related statements scoring between 1.80 and 2.00, indicating general disagreement with awareness of data practices. All four statements related to awareness of the NDPR received mean scores between 1.80 and 2.00 (Strongly Disagree to Disagree on a 1–5 scale), placing responses at the low end of agreement and indicating that respondents do not feel they understand data practices, cookie preferences, and legal rights. Chi-square analysis showed no statistically significant association between Education level and data privacy awareness of the NDPR ($\chi^2 = 0.890$, $df = 1$; $p = 0.346$). A non-significant result does not confirm that awareness is uniformly low across groups; it simply means the study lacked the statistical Power, given the $n=53$ sample, to detect any variation. Taken together with the low mean scores, the overall pattern suggests that low NDPR awareness is widespread across Education levels. These findings are exploratory and should be interpreted accordingly.

4.3 Consumer experiences with data collection in digital marketing

A significant proportion of respondents (94%) were aware of online behavioural targeting; only One quarter (24.5%) could explain how it operates, suggesting that this knowledge does not translate to practical use. Despite not reading the cookie consent banner options, more than half (58.5%) of respondents clicked on the 'Accept All' button without any knowledge of the relevant information, and 47.2% were unaware that they had the option to reject non-essential cookies, suggesting that their agreement was given without realising the choice. Despite being lower, app permissions were still significant: 41.5% of people approved all requests without reviewing them. This finding suggests that the 'consent paradox' in the sample is a real phenomenon in which people often give their consent without understanding what they are actually consenting to.

Table 3

Consumer Experiences with Data Collection (n = 53)

Behaviour Experience /	Response	n	%
Noticed targeted ads (Q23)	Yes (very often or occasionally)	50	94.4
Can explain how targeting works (Q24)	Yes, clearly	13	24.5
	Rough idea only / No idea	40	75.5
Cookie consent behaviour (Q25)	Click 'Accept All' immediately.	31	58.5
	Read options / Reject non-essential	17	32.1
Know can decline cookies (Q26)	Yes	28	52.8
	No	25	47.2
App permissions (Q27)	Approve all without reviewing	22	41.5

	Review and approve selectively	21	39.6
--	--------------------------------	----	------

Table 4

Likert Scale Means for Section C: Perceptions of Data Collection Practices (n = 53)

Likert Statement (Section C)	Mean	SD
I feel in control of what personal data companies collect from me	2.00	1.18
I trust digital platforms to handle my personal data responsibly	2.19	1.23
I am concerned about data collected without my clear understanding	3.64	1.51
Information about data collection is clear and easy to understand	2.36	1.35
Data is used in ways I would not agree to if I understood them	3.17	1.61

Note. Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. SD = standard deviation.

4.4 Perceived implications for civic freedom

From the civic perspective, two findings from the survey stand out: 68.0% of responding individuals expressed at least a degree of concern (very or somewhat) about their personal data being used to influence their political opinions or voting behaviours, and 47.2% stated that they were not very confident or not confident at all in using digital platforms for civic participation. A further finding was that 81.1% of respondents (43 of 53 individuals) reported engaging in at least One instance of online self-censorship due to concerns about data or surveillance, including refraining from expressing their political opinions, declining to join civic networks, and limiting their digital communications on sensitive issues.

Table 5

Likert Scale Means for Section D: Perceived Implications for Civic Freedom (n = 53)

Likert Statement (Section D)	Mean	SD
I feel free to express my political opinions openly on digital platforms	1.94	1.15
I am concerned that political actors could access my data	3.34	1.45
Political data advertising threatens free and fair elections in Nigeria	3.36	1.51
I would engage more civically if my data were better protected	3.43	1.53
Knowing about data collection has made me less active online	3.36	1.47
Nigerians should be educated about their data privacy rights	3.83	1.49

Note. Likert scale: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. SD = standard deviation

A weak and non-significant Pearson correlation between civic confidence and awareness ($r = 0.024$, $p = 0.865$) indicates that, in this sample, awareness alone does not appear to translate into greater civic confidence. The test should be interpreted with caution for two reasons: the limited sample size ($n=53$) constrains statistical Power, and pairing a dichotomous awareness measure with Likert-scale outcome

results in a mismatch that can further reduce the test's sensitivity. The absence of a significant result does not preclude the existence of a relationship in the broader population. Future studies with larger samples and non-parametric methods, such as Spearman's rho, would provide a more robust assessment of this relationship, as Spearman's rho better handles the ordinal and dichotomous nature of these variables.

4.5 Test of hypotheses

Responses obtained from the sample were used to test the hypothesis associated with data privacy and civic freedom in Nigeria. Regarding H01, that there is no significant connection between data privacy awareness and privacy policy reading, the null hypothesis is descriptively inconsistent with the data, as respondents who were unaware of the NDPR and NDPA had an average rate (90.6%) of never reading a complete privacy policy. Because a formal test of the two specific variables was not carried out in the statistical analysis, the first hypothesis cannot be formally rejected. It should be tested again in future research. Regarding the second hypothesis, that there is no significant relationship between data privacy awareness and consent behaviour, the null hypothesis is similarly challenged by the descriptive data. Low regulatory awareness was associated with high rates of uninformed consent (58.5% acceptance of cookies without reading and 41.5% approval of app permissions without review), consistent with this trend. As Solove (2013) noted, consent-based frameworks are undermined when awareness is low, a pattern reflected in the descriptive data here. Until further investigation can be conducted, the second hypothesis will be retained, as there is no formal inferential test of the relationship between awareness and consent behaviour. Regarding the third hypothesis, that there is no significant relationship between data privacy concerns and civic freedoms, the null hypothesis is directly addressed by the lack of a significant connection between data privacy concerns and civic freedoms, as indicated by available statistics. The Pearson correlation between civic confidence and awareness ($r = 0.024$, $p = 0.865$) was not significant; therefore, the third hypothesis is retained. The descriptive pattern — 81.1% self-censorship rate, a mean of 1.94 for freedom to express political opinions, and 68% concern about political data use — is directionally consistent with a relationship between privacy concerns and constrained civic participation. However, the statistical test does not confirm this at the sample level. The overall trend suggests that privacy concerns are associated with limited civic participation.

4.6 Discussion

The survey results, particularly the low rates of policy reading and NDPA awareness, suggest that respondents in the sample are operating in a data-driven marketing environment that most do not fully grasp, at least with respect to the privacy frameworks governing their data. The consent structure of the NDPR and the NDPA (grounded on informed, voluntary data subject decisions, where individuals genuinely understand and agree to how their data is used) does not appear to be functioning as intended among this sample. The low rate of full privacy policy reading (90.6%), minimal awareness of the NDPA (11.3%), and the high proportion of respondents who accepted all privacy notices without reading them (58.5%) collectively suggest that, within the bounds of this sample, consent appears to function as a legal formality rather than a meaningful protective mechanism, and no broader generalisation is intended. This finding is consistent with Solove's (2013) 'consent dilemma' and provides preliminary evidence of its manifestation in the Nigerian digital marketing context, particularly given that 58.5% of respondents accepted all privacy notices without reading them. The civic implications are equally concerning. With 81.1% of respondents reporting at least one instance of online self-censorship due to data and surveillance concerns, a substantial proportion of the sample is modifying their behaviour online in direct response to perceived monitoring, which is a key behavioural marker of the chilling effect. The majority of respondents did not feel free to express their political opinions on the Internet (mean = 1.94), suggesting that, for many in this sample, digital platforms are perceived as monitored spaces rather than open public spheres. This pattern is consistent with the chilling effect theorised by Lyon (2014) and empirically demonstrated by Penney (2016); these findings offer preliminary evidence that a similar dynamic may be present among digitally active Nigerians, though larger, representative studies are needed to confirm this at the population level. Notably, the item stating that Nigerians should be educated about their data privacy rights received the highest mean score across all items (mean = 3.83). While this finding is drawn from a non-representative

sample, it nonetheless signals a perceived need among respondents for broader public Education on data rights with clear implications for policy and practice.

5. Conclusion and Recommendations

This study aims to examine the level of data privacy awareness among Nigerian digital consumers and its implications for civic freedoms. Data were collected via an online survey, yielding responses from 53 participants. The study has yielded three core conclusions: Firstly, consumer awareness of data privacy rights and regulations is extremely low among the study sample, with fewer than 1 in 8 respondents having heard of the NDPA and 90.6% indicating they have never read a privacy policy in its entirety. Secondly, while a majority of respondents consented to allow their data to be collected, they did so with little to no understanding of the interfaces and terms to which they agreed; this pattern is consistent with the "Consent Paradox" described in the literature (Barnes, 2006; Solove, 2013) and provides exploratory evidence of its presence within this Nigerian sample. Thirdly, the high rate of online self-censorship among respondents (81.1%), the low mean score for freedom to express political opinions digitally (mean = 1.94), and the low levels of confidence in civic digital participation together suggest that data privacy concerns carry measurable civic and democratic implications, findings that warrant further investigation at a larger, more representative scale. The findings show that the gap between Nigeria's legal data protection framework and the lived experience of digital consumers is more than just a regulatory failure; it also reflects social and civic concerns. The NDPR and NDPA represent two significant legislative accomplishments; however, if individuals do not understand these new laws, they have not been protected. The disparity between Nigeria's data protection framework and the lived experience of digital consumers can be addressed through coordination and collaboration between regulators, advertisers, civil society, and educational institutions. Although 53 respondents comprise an exploratory sample, limiting generalisability, administering the study online is likely to bias toward more educated urban Nigerian participants, and reliance on self-reported data has the potential for social desirability bias. Future research needs to use larger samples, longitudinal designs and qualitative methodologies to expand the evidence base. The study recommends that the Nigerian Data Protection Commission (NDPC) undertake ongoing, multilingual public Education and awareness campaigns in Hausa, Yoruba, Igbo, and other languages to increase understanding of data rights. These campaigns should be co-designed with civil society organisations that are genuinely embedded in their communities to reach those communities effectively. The NDPC should provide sector-specific enforceable guidelines for the digital marketing sector prohibiting the use of dark design patterns for consent and mandating that 'managing my preferences' options be similarly prominent to 'accept all' buttons. In addition, the digital marketing sector operating in Nigeria should develop and implement plain-language, multilingual privacy notices as an ethical baseline, rather than merely to comply with regulations. The evidence that most users in Nigeria do not understand what they are consenting to should not be relied upon as a legal defence. Also, civil society organisations ought to frame data privacy Education as a civic rights issue and launch awareness campaigns paired with practical means of action (e.g., guides for platform settings, NDPC complaint processes, and explanatory documents on users' rights). Furthermore, Nigeria's educational institutions ought to integrate digital rights and data literacy into their secondary- and tertiary-level curricula. The findings of this study reinforce this recommendation: the item stating that Nigerians should be educated about their data privacy rights returned the highest mean Likert score across all items (mean = 3.83), signalling strong perceived need for this intervention among the respondents surveyed. Finally, future studies should continue to utilise larger (geographically representative) samples, longitudinal designs, and comparative studies within countries in West Africa to develop the regional evidence base to support data rights policies.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2016). Privacy and human behaviour in the age of information. *Science*, 347(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling a lack of control over their personal information*. Pew Research Centre.

- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). <https://doi.org/10.5210/fm.v11i9.1394>
- Calandro, E., & Berger, G. (2020). *Digital rights in Africa: Understanding the landscape*. Research ICT Africa.
- Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.
- DataReportal. (2024). *Digital 2024: Nigeria*. <https://datareportal.com/reports/digital-2024-nigeria>
- Deibert, R. (2019). The road to digital unfreedom: Three painful truths about social media. *Journal of Democracy*, 30(1), 25–39. <https://doi.org/10.1353/jod.2019.0002>
- Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, 1(2), 1–13. <https://doi.org/10.1177/2053951714541861>
- Makulilo, A. B. (2016). *African data privacy laws*. Springer.
- Matz, S. C., Kosinski, M., Nave, G., & Stillwell, D. J. (2017). Psychological targeting as an effective approach to digital mass persuasion. *Proceedings of the National Academy of Sciences*, 114(48), 12714–12719. <https://doi.org/10.1073/pnas.1710966114>
- Maweu, J. M. (2021). 'Fake elections': Cambridge Analytica, data exploitation and digital electoral interference in Kenya. *African Journalism Studies*, 42(1), 19–33. <https://doi.org/10.1080/23743670.2021.1874890>
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3), 543–568.
- National Information Technology Development Agency. (2019). *Nigeria Data Protection Regulation*. Federal Republic of Nigeria.
- Nigeria Data Protection Commission. (2023). *Nigeria Data Protection Act*. Federal Republic of Nigeria.
- Nunnally, J. C. (1978). *Psychometric theory* (2nd ed.). McGraw-Hill.
- Osei-Bonsu, N. (2022). Data protection regulation in West Africa: Comparative perspectives. *Journal of African Law*, 66(2), 211–234.
- Paradigm Initiative. (2023). *Digital rights in Africa report 2023*. <https://paradigmhq.org>
- Penney, J. W. (2016). Chilling effects: Online surveillance and the use of Wikipedia. *Berkeley Technology Law Journal*, 31(1), 117–182.
- PwC Nigeria. (2023). *Nigeria entertainment and media outlook 2023–2027*. PricewaterhouseCoopers.
- Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7), 1880–1903.
- Turow, J. (2011). *The daily you: How the new advertising industry is defining your identity and your worth*. Yale University Press.
- Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- Westin, A. F. (1967). *Privacy and freedom*. Atheneum.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of Power*. PublicAffairs.