IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Analysis of users' perceptions of data privacy on social media networks in Nigeria

Omowumi Hafsat Aliu[1,2], Samuel Omaji[1], Kingsley Eghonghon Ukhurebor[3*], Adeyinka Oluwabusayo Abiodun[3], Olatunji Oluwatosin Onaseso[4]

[1]*Department of Computer Science, Edo State University, Uzairue, Edo State, Nigeria.*
[2]*Department of Computer Science, Auchi Polytechnic, Auchi, Edo State, Nigeria.*
[2]*Department of Physics, Edo State University, Uzairue, Edo State, Nigeria.*
[3]*Africa Centre of Excellence on Technology Enhanced Learning, National Open University of Nigeria, Abuja, Nigeria.*
[4]*SAGE Group Technologies, Hazlet, NJ, United States.*

Corresponding Author: Kingsley Eghonghon Ukhurebor (*Email: ukeghonghon@gmail.com*)

Abstract

This present study aims to classify users' perceptions of data privacy on social media and provide feedback to users on making informed choices. The emergence of social media networks (SMNs) has revolutionized the way people interact and share information online. SMNs have enabled users to connect with friends, family, and colleagues, making communication more efficient and faster. Several studies have highlighted the data privacy challenges without providing a framework for the development of a system for classifying users' perceptions of these data privacy challenges on SMNs. Furthermore, there is limited evidence-based research that examines the level of awareness about these hidden data privacy issues based on perceived threats by users. However, the widespread adoption of social media technologies has also raised concerns about privacy and security. The study explores and adopts a mixed-methods approach, integrating quantitative surveys and qualitative interviews. The survey collects data using Likert scale questions to measure participants' privacy concerns and awareness of data privacy settings. A total of 468 responses were obtained, representing diverse demographics. The findings indicate that the majority of respondents were males aged 18-25 years, with a high school education. Additionally, participants spent an average of 2-4 hours daily on social media. The study highlights the need for users to read privacy policies before registering information on websites. The results of this research contribute to a better understanding of users' perceptions of data privacy on SMNs, facilitating informed decision-making regarding social media usage.

Keywords: Data, Information and communication technology, Internet, Privacy, Security, Social media networks.

DOI: 10.53894/ijirss.v7i3.2959
Funding: This study received no specific financial support.
History: Received: 27 June 2023/**Revised:** 19 January 2024/**Accepted:** 15 February 2024/**Published:** 28 March 2024

Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Institutional Review Board Statement: The Ethical Committee of the Department of Mass Communication, Edo State University Uzairue, Edo State, Nigeria has granted approval for this study on 13 December 2022 (Ref. No. EDSU/DECR/22/0003).
Publisher: Innovative Research Publishing

1. Introduction

The advent of social media networks (SMNs) has brought new dynamics to the way people interact and share personal information and random contents on the internet [1, 2]. The prime reason for this trend is that SMNs enable users to connect with their friends, family, and coworkers on a platform [3, 4]. Social media use has made it possible for users, including businesses, customers, institutions, and many more, to communicate in real-time. As a result of this advancement in the field of technology, communication is more efficient and faster [5, 6]. For many Nigerians, the creation and use of social media technologies have become a way of life. It is noted that SMNs are a resounding advancement in ICT in the twenty-first century [7]. Despite the fact that it is evolving, its widespread adoption and usage are rising every day [8].

Nowadays, there is an array of definitions pertaining to the meaning of SMNs in existing literature. Drury [9] provided a notable definition regarding the subject, describing social media as online sources used by individuals for content sharing such as videos, images, sound, and text to convey insights, humour, opinion, gossip, and news. Amazingly, information can be shared with many people in the blink of an eye; distance is no longer a factor. The development of networks and internet technologies, which offer the platforms for social media applications and make communications simple and hassle-free, makes this possible. Apart from its significantly high adoption by individual users, companies, institutions, and organizations also find relevant use of social media channels for communicating and showcasing their products or services over the internet [6, 10]. According to Balakrishnan and Gan [11] there are many different sorts of SMN sites, like WhatsApp, Facebook, Instagram, LinkedIn, and Badoo to media-sharing platforms like Flickr and YouTube. Other examples include social bookmarking platforms like CiteULike and Delicious, tools for group knowledge development, and creative tools like blogs, WordPress, and Blogger, as well as applications and microblogging sites like WhatsApp and Twitter.

The motivating factor behind the usage and adoption of this form of media lies largely in the need to communicate, interact, share, and exchange knowledge and ideas over the respective online social networking platforms. But, besides the attractions these SMNs have, they also pose hidden threats to the privacy of their users. Preliminary investigations carried out through an extensive review of available journals, technical papers, books, online news, and interaction with internet and social media users, etc., reveal the existence of insecurity and threats to the privacy of personal and organizational information. Other researchers have also investigated and published articles on these social media insecurity problems, such as Lawler and Molluzzo [12] who state that without the knowledge of these users, SMNs may partner with organizations to utilize information gathered from them for marketing purposes. Similarly, Williams [13] emphasized in his study that users of social media might not be fully aware of the dangers of using them. Also, it appears that they have a poor understanding of the potential uses of the posted information and the appropriate data to share with outside parties.

As of the time of this research, available scientific methods for classifying user's perceptions of SMNs are limited. The available literature, such as the work of Saravanakumar and Deepa [14];Onifade, et al. [15];Bui [16]; Kundu, et al. [6] and Bocar and Jocson [17] have highlighted the data privacy challenges without providing a framework for the development of a system for the classification of users' perceptions of these data privacy issues on SMNs. Furthermore, there is limited evidence-based research that examines the level of awareness about these hidden data privacy issues based on perceived threats by users. To this end, this study aims to classify users' perceptions of data privacy on social media. The study explores and adopts a mixed-methods approach, integrating quantitative surveys and qualitative interviews. The results of the classification will serve as feedback to users regarding their future choices in using social media.

2. Research Methodology

The researchers adopted a mixed-methods approach, integrating quantitative surveys and qualitative interviews to achieve comprehensive perceptions and insights from a diverse range of social media users. The study sample consisted of participants from various age groups, backgrounds, and social media platforms. The surveys were designed to measure participants' privacy concerns, awareness of data privacy settings (PRS), and willingness to disclose personal information. The subsequent interviews allowed for in-depth exploration of participants' motivations, experiences, and decision-making processes regarding data privacy on social media.

2.1. Data Collection Phase

In the data collection phases, an expert survey was conducted to determine the viability of the method relationships, constructs, and guidelines. To achieve this, the research develops survey questions. The research work envisaged in this thesis is qualitative, specifically to measure, identify, organize, and interpret the perceptions of respondents to solve arising questions on data privacy on social media. The survey instrument in use for data gathering is the Likert scale (LS). A common psychometric scale used in studies employs questionnaires (QTNs) to measure findings and impressions. Psychometric scales are normally employed by researchers to understand the opinions and perceptions of a product, brand, or target market, while LS is a unidimensional scale that is utilize to collect participates'respondents' opinions and perceptions. On a five-point scale, choices typically range from strongly disagreeing to strongly agreeing, while on a seven-point scale, choices typically range from very strongly disagreeing to very strongly agreeing. The value will rise by one unit from the most negative to the most positive when the category progresses from one to the next. This enables us to gauge unique attitudes, convictions, or perspectives. Different types of variables are frequently measured using the LS. The seven-point LS is desired in this work because it offers seven different options to choose from. It provides two moderate options, along with two extremes, two intermediates,and one neutral option, to the respondents. The decision-making procedure that follows is linked to the problem's reduction to decisions based on multiple factors on a LS. The work of

Sofian and Rambely [18] justifies that a seven-point scale contains no interpolations among responses; it provides a more sensitive gauge of a participant's actual evaluation than a five-point LS.

The seven-point scale offers more nuanced options, increasing the likelihood of accurately reflecting participants' perspectives. It provides a more comprehensive description of the subject matter, appealing to participants' reasoning abilities [19]. For this reason, this survey adopts a seven-point LS, to which participants can respond with "Very Strongly Disagree," "Strongly Disagree," "Disagree," "Neutral," "Agree," "Strongly Agree," and "Very Strongly Agree."

This study used a Google Form survey as part of the data collection process. Respondents were invited to take the survey through various recruitment techniques, including email invitations, social media posts, and word of mouth. The link led the respondent to the Google Form survey after they clicked it. There were multiple-choice, LS, and open-ended items in the study or survey. The respondents and participants were asked to answer questions regarding their privacy worries and perceptions when using social media networks and demographic questions.

The Google Form survey was made to be intuitive and straightforward to use. All responses to the survey were immediately saved, and participants may finish it on their own time. The Google Form was created to gather responses devoid of personal identification data to preserve the participants' anonymity. The data -gathering procedure took place over a few weeks, during which the survey link was actively disseminated.

Overall, the Google Form survey's data collection method effectively and efficiently obtained the required data for the study. Thanks to the high sample size and the variety of questions, an in-depth picture of the participants' privacy attitudes and views was produced. The data that was collected was further evaluated utilizing the "Statistical Package for Social Sciences (SPSS) version 24.0."

2.2. Research Design

As stated earlier, this study aimed at ascertaining users' level of knowledge regarding data access privileges on particular SMNapps and how this knowledge affects their privacy concerns and perceptions. Through the implementation of a Google Form, a pre-test survey was carried out to determine the respondents' initial privacy concerns and impressions. The following describes the methodology used in carrying out the survey:

- Secure Informed Consent.
- Gather Demographic Data.
- Conduct Pre-Test Survey.
- Privacy Information Conditions.

2.3. Background Information and Demographic Queries

Basic demographic information about the participants and respondents was collected, comprising age, gender, and level of education, to examine if any demographic characteristics influenced the respondents' privacy attitudes. Furthermore, to acquire an initial understanding of the respondents' privacy attitudes, the "Westin/Harris Privacy Segmentation Model" was employed [20]. This model utilizes tripartite questions to categorize individuals into three groups "privacy fundamentalists, privacy pragmatists, and privacy unconcerned."

3. Results and Discussions

3.1. Questionnaires Distribution

A total of 500 random respondents to the Google Form QTNs designed were run with open-source access to unidentified respondents online and monitored by the targeted respondents and participants of a system classification of users' perceptions of data privacy on SMNs. A total of 468 responses from the returned filled-out Google Form QTNs (sample size for the study) were found operational, which represents about 95.80%, which affirms the prospects of the least usage rate of about 70.00% in a face-to-face study or survey as suggested by Bateman, et al. [21].

3.2. Respondents' Demographic Profile of Analysis of Users' Perception of Data Privacy on SMNs

A general profile of respondents' demographic statistics of a system classification of users' perceptions of data privacy on SMNs was analysed (see Tables 1a-d). The results in Table 1a-d display the summarized demographic features of the participants and respondents utilized in a system classification of users' perceptions of data privacy on SMNs.

3.2.1. Gender Distribution

The gender distribution of participants/respondents utilized consisted of 67.90% males and 32.10%female in the survey. This shows that the majority of respondents to analysis of users' perceptions of data privacy on SMNs were males, followed by females (see Table 1a).

3.2.2. Age Group Distribution

The age distribution of the participants or respondents was segmented into five clusters, and the main age group of the participants and respondents was the age group cluster of 18–25 years, which comprised 79.30%. Furthermore, the analysis indicated that about 9.60% of the respondents were within the age range of 26–35 years, while those within the age range of 36–45 years were about 5.60%. In addition, 46–55 years represent 4.3%, respectively. The age range between 56 and above comprises 1.3%. This implies that the majority of respondents are between the ages 18 to 25, and the lowest percentage age of the study's analysis of users' perceptions of data privacy on SMNs was 56 years and older (see Table 1b).

Table 1.
The summarized demographic features of the participants/respondents utilized in a system classification of users' perception of data privacy on SMNs.

(a) Gender	Frequency (F)	Percent (%)
Male	318	67.90
Female	150	32.10
Total	468	100.00
(b) Age	F	%
18-25years	371	79.30
26-35years	45	9.60
36-45years	26	5.60
46-55years	20	4.30
56years above	06	1.30
Total	468	100.00
(c) Educational background	F	%
PhD	19	4.10
Masters	37	7.90
Bachelor	71	15.20
High school	176	37.60
Others	165	35.30
Total	468	100.00
(d) Profession/Job	F	%
Students	376	80.30
Educators	32	6.80
Professionals	33	7.10
Artisans	03	0.60
Entrepreneurs	16	3.40
Others	08	1.70
Total	468	100.00

3.2.3. Educational Background

The educational qualifications of participants and respondents were segmented into five clusters, and the main qualification group of respondents in the study, an analysis of users' perceptions of data privacy on SMNs, were those with other qualifications, which comprised 37.60% of those with high school qualifications. The analysis further shows that about 35.30% of the respondents had other qualifications, while those with bachelor degrees comprised 15.20%, master's degree holders make up 7.90% and 4.10% are PhD holders. The finding shows that the majority of respondents had high school qualifications and other qualifications (see Table 1c).

3.2.4. Profession/Job Distribution

Respondents in the study's analysis of users' perceptions of data privacy on SMNs whose job and profession were students comprised 80.30% of the sample size. Furthermore, the analysis indicated that about 7.10% of the participants/respondents were professionals, while those who are educators make up 6.80%. Artisans comprised 0.60%, and entrepreneurs accounted for 3.40% and others 1.70%. The findings, as shown in Table 1d, reveal that the majority of respondents were students, followed by those who were professionals, then educators.

3.3. Distribution of Respondents on Time Spent Daily on Social Media

The distribution of respondents based on how long you spend on social media daily reveals that 46.20% spent 2-4 hours while 31.20% spent 5 hours and above, as shown in Table 2. About 22.60% spent 0-1 hour daily. This shows that users of online services spent mostly 2-4 hours analysing users' perceptions of data privacy on SMNs.

Table 2.
Respondents' distribution on the time spent daily on social media.

How long do you spend daily on social media	F	%
0-1 hour	106	22.60
2-4 hours	216	46.20
5 hours above	146	31.20
Total	468	100.00

3.4. Respondents on Social Media Platform

Investigating the distribution of social media platforms frequently used based on an analysis of users' perceptions of data privacy on social media networks, the analysis reveals that 51.10% of the respondents used WhatsApp frequently, 16.90% used WhatsApp and Facebook,and7.90% adopted WhatsApp, Facebook and Instagram. The findings show that the most frequently used social media is WhatsApp, as represented in Table 3.

Table 3.
The respondents on social media platform.

Which of the following social media platform do you frequent (You can make multiple selection)	F	%
WhatsApp	239	51.10
Facebook	17	3.60
Instagram	10	2.10
Others	09	1.90
WhatsApp and Facebook	79	16.90
WhatsApp and Instagram	29	6.20
WhatsApp and others	13	2.80
Instagram and others	01	0.20
WhatsApp, Facebook and Instagram	37	7.90
WhatsApp, Facebook and others	08	1.70
WhatsApp, Instagram and others	11	2.40
WhatsApp, Facebook, Instagram and others	15	3.20
Total	468	100.00

3.5. How Long on the Average Have You Been Using the Social Network

How long on average have you been using the social media platform? The analysis reveals that 179 of the respondents, representing 38.20%, said they have been using the preferred social media network, WhatsApp for about 2-4 years. 231 of the respondents, comprising 49.40%, have been using the SMNs of WhatsApp and Facebook for over 5 years. Those who used the SMNs between 0-1 year were 57, representing 12.20% (see Table 4). Table 4 shows the analysis of how long, on average a respondent has been using SMN. The study shows that most of the users have been using the social media network of their choice for over 5 years.

Table 4.
The analysis of how long on average have a respondent been using social media network.

Talking about the SMN(s) you frequent most, how long on the average have you been using it	F	%
0-1 year	57	12.20
2-4 years	179	38.20
5 years above	231	49.40
Invalid responds	01	0.20
Total	468	100.00

3.6. Respondents on Reading a Website's Privacy Policy (WPP) before Registering Information Is Necessary

A distribution analysis of reading a WPP before registering information is necessary of a system classification of users' perception of data privacy on SMNs (Table 5) shows that 22.60% of the respondents spent 0-1 hour reading a WPP before registering information is necessary, 46.20% spent 2-4 hours reading a WPP before registering information is necessary, and 31.20% spent 5 hours and above on reading a WPP before registering information is necessary. This implies that the majority of the participants and respondents in this study spent, on average, 2-4 hours reading a WPP before registering information is necessarily followed by those who spent 5 hours and above.

Table 5.
The analysis of how long on average have a respondent been using social media network.

Reading a WPP before registering information is necessary	F	%
0-1 hour	106	22.60
2-4 hours	216	46.20
5 hours above	146	31.20
Total	468	100.00

3.7. Reliability of Measures a System Classification of Users' Perception of Data Privacy on SMNs

The reliability of dimensions of a system classification of users' perceptions of data privacy on SMNs was assessed based on "Cronbach's Alpha."The "Cronbach's Alpha" value of all the respective items for each of the five dimensions of factors in a system classification of users' perceptions of data privacy on SMNs ranges between 0.789 and 0.916, as indicated in Table 6.

Table 6.
Reliability of items of a system classification of users' perception of data privacy on SMNs.

Dimensions	Composite Cronbach's alpha	Items Cronbach's alpha
Privacy policy online (PPO)	PPO	0.788
Concern on social media networks	SMNs	0.916
Privacy settings	PRS	0.821

Due to the results and findings in Table 6, all the items measure or quantify their underlying dimensions consistently. The composite reliability for each of the three aggregate dimensions of a system classification of users' perceptions of data privacy on SMNs ranges between 0.788-0.916 (Table 6). This suggests that PPO, (α=0.788), Concern for SMNs, (α=0.916), and PRS, (α=0.821). This justifies or validates that all the items for the three dimensions of a system classification of users' perceptions of data privacy on SMNs are internally reliable and consistent at 86.80%. As the "Cronbach's alpha" values are > 0.70. Hence, it suffices to say that constructs satisfy the conditions and requirements of the internal consistency [22].

3.8. Percentage Item Analysis of a System Classification of Users' Perception of Data Privacy on SMNs

The Table 7 displays the mean (average) score and rank analysis of the items that were utilized for gathering information from participants and respondents regarding the PPO as factors in a system classification of users' perceptions of data privacy on SMNs.

Table 7.
Percentage item analysis of privacy online.

PPO	Agree	Disagree	Neutral	Strongly agree	Very strongly agree	Mean	Ranking
Blocking people on SMN that I do not want to see my information is necessary	27.8	15.6	5.8	23.9	26.9	3.51	1st
The use of SMN apps is necessary	28.4	13.7	10.0	24.1	23.7	3.38	2nd
Privacy is a major concern while using SMN	27.8	15.6	5.8	23.9	26.9	3.24	3rd

Note: "Total mean is 2.87. Strongly disagree = 1, Disagree= 2, Neutral= 3, Agree =4, Strongly agree = 5".

The result as depicted in Table 7 shows that the elicited response on the PPO scale implies that the statement "Blocking people on SMN that I do not want to see my information is necessary" constitutes a mean response score of 3.51 with a percentage of 27.8% agreeing, 23.9 strongly agreeing, and 26.9% very strongly agreeing that blocking people on SMN that they do not want to see their information is necessary. The statement "The use of SMN apps is necessary" has 28.4% agree, 24.1% strongly agree, and 23.7% very strongly agree. The response on the use of SMN apps is necessary has mean score of 3.38. Item with statement "Privacy is a major concern while using SMN" has 27.8% fall under LS (agree); 33.9% fall on strongly agree and 26.9% on very strongly agree with the mean score response of 3.24. The result of the analysis indicates the main PPOs are: blocking people on SMN because they do not want to see their information, and the use of SMN apps is necessary.

Also, Table 8 displays the mean (average) score and rank analysis of the items that was utilized for gathering information from participants/respondents regarding their concern on SMN as factors of a system classification of users' perception of data privacy on SMNs.

Table 8.
Percentage item analysis of concern on SMN.

Concern about SMNs	Agree	Disagree	Neutral	Strongly agree	Very strongly agree	Mean	Ranking
I am concerned that SMN will sell or release my personal information to a third party	28.4	15.0	13.5	20.7	22.4	3.24	4th
I am concerned that I am asked to grant access to too much personal information when installing the SMN app	27.4	14.7	8.1	23.3	26.5	3.45	1st
I am concerned about online identity theft via SMN	20.3	25.0	16.9	19.4	18.4	2.97	8th
I am concerned about strangers obtaining personal information about me from SMN	26.5	22.4	11.8	19.7	19.7	3.13	5th
I worry that individuals outside of my intended audience may view the content I post on SMN	27.4	16.2	10.3	23.5	22.6	3.32	2nd

Concern about SMNs	Agree	Disagree	Neutral	Strongly agree	Very strongly agree	Mean	Ranking
I am concerned that the SMN app could post to my timeline using my name	27.4	16.5	11.1	21.2	23.9	3.30	5th
I am concerned that a seemingly legitimate SMN app may be fraudulent	24.6	19.7	15.4	17.7	22.6	3.13	4th
I am concerned that SMN apps could collect my data	21.6	22.2	14.5	23.5	18.2	3.09	7th

Note: "Total mean is 2.57. Strongly disagree = 1, Disagree= 2, Agree =3, Strongly agree = 4".

Table 8 displays the responses to concerns about SMN. The statement "I am concerned that I am asked to grant access to too much personal information when installing the SMN app" constitutes the highest mean score response rate of 3.45, with 23.30% strongly agree, 14.70% agree, and 26.50% very strongly agree. While the item with statement "I worry that individuals outside of my intended audience may view the content I post on SMN" comprises 27.40% agree; 23.50% strongly agree and 22.60% very strongly agree with the mean score response rate of 3.32. The statement "I am concerned that SMN will sell or release my personal information to a third party" shows that 28.40% agree; 20.70% strongly agree, and 22.40% very strongly agree with mean score of 3.24. The item with the statement "I am concerned about strangers obtaining personal information about me from SMN" constitutes 26.50% agree; 19.70% strongly agree, and very strongly agree, respectively, with mean value of 3.13. In addition, the item with the statement "I am concerned that a seemingly legitimate SMN app may be fraudulent" has response rate of 24.60% agree, 17.70% strongly agree and 22.60% very strongly agree with mean value of 3.13. While item with statement "I am concerned that the SMN app could post to my timeline using my name" comprises 27.40% agree; 21.20% strongly agree, and 23.90% very strongly agree with the mean score response rate of 3.30. The item with the statement "I am concerned that SMN apps could collect my data" constitutes 21.60% agree; 23.50% strongly agree, and 18.20% very strongly agree, with a mean value of 3.09. In addition, the item with the statement "I am concerned about online identity theft via SMN" has response rate of 20.3% agree, 19.4% strongly agree and 18.4% very strongly agree with mean value of 2.94. The main concern about SMNs is that they are "asked to grant access to too much personal information when installing the SMN app," worry that individuals outside of my intended audience may view the content I post on SMN and SMN may sell or release my personal information to a third party.

Percentage item analysis of PRS profile is represented in Table 9, which shows information from respondents regarding their PRS profile.

Table 9.
Percentage item analysis of PRS of profile.

PRS of profile	Agree	Disagree	Neutral	Strongly agree	Very strongly agree	Mean	Ranking
The PRS of my profile on SMN can be rated as high	22.9	19.7	14.5	22.0	20.9	3.15	2nd
I feel comfortable sharing personal information on SMN	23.9	19.2	13.0	23.1	20.7	3.19	1st
I feel in control when specifying and updating my profile on SMNs	25.0	15.4	16.9	23.9	18.8	3.12	4th
I feel that the privacy of my personal information is protected by SMNs	19.2	24.4	13.5	20.1	22.9	3.15	2nd

The result suggests that the statement "I feel comfortable sharing personal information on SMN has 23.90% agree; 23.1 strongly agree, and 20.70% very strongly agree, with mean score of 3.19. Item with the statement "The PRS of my profile on SMN can be rated as high" has 22.90% agreed, 14.50% strongly agree, and 20.90% very strongly agreed, and the mean score is 3.15. The statement "I feel that the privacy of my personal information is protected by SMNs" has 19.12% falling on agree, LS followedat22.00% strongly agree, and 20.90% agree. The mean score is also 3.15. It was also revealed that items with the statement "I feel that the privacy of my personal information is protected by SMNs" have 23.30% agree; 23.10% strongly agree and 19.90% very strongly agree with value 3.14. More so, items with statement "I feel in control when specifying and updating my profile on SMNs" have 25.00% agree; 23.90% strongly agree and 18.80% very strongly agree with mean score of 3.12. All of the responses fall under the LS (strongly agree and agree). The results/findings show that most of the privacy setting profiles (PSPs) are: comfortable sharing personal information on SMN, the PRS of their profile on SMN can be rated as high; and they feel that the privacy of their personal information is protected by SMNs.

The model of PPO on SMNs and PSP data collected were analysed using "Pearson correlation" to estimate the relationship. The findings and results as indicated in Table 10 imply that the two dimensions of a system classification of users' perceptions of data privacy on SMNs were found to be; PSP (r = -0.521; p =0.000), and social media network (SMN) (r = 0.632; p = 0.012).

Table 10.
Correlations of factor of a system classification of users' perception of data privacy on SMNs.

Variables	R	P	Level
(Constant)	--	--	--
PSP	-0.521**	0 .000	Medium
SMNs	0.632**	0 .012	High

Note: “** Correlation is significant at 0.01level (2 tailed)”.

This proposes that all the tested variables of SMN have a positive (true) and significant relationship with PPO in a system classification of users' perceptions of data privacy on SMNs and PSP profiles. PSP (r = -0.521; p =0.000) has a negative and significant relationship with PPO in a system classification of users' perceptions of data privacy.

3.9. Research Hypotheses

The research hypotheses for this study utilized regression analysis (RA). This analysis was done to estimate the dimensions of a system classification of users' perceptions of data privacy. Multiple RA was utilized to estimate the relative contributions and most significant predictors of each independent variable (IV) towards dependent variable. Additionally, it served as a tool for determining how much of the dependent variables' variance the IV might be able to interpret. In this regard, the following hypothesis was tested accordingly: Hence, this study would test the following null hypotheses (H_0):

H_{01}: There is no significant relationship between PPO and SMNs.
H_{02}: There is no significant relationship between PPO and PSP.
H_{03}: There is no significant relationship among PPO, SMNs and PSP.

Table 11.
The estimates of model of PPO.

-	Unstandardized coefficient	Standardized coefficient	T	Sig.
(Constant)	20.38		5.12	0.000
PSP	0.74	-0.556	0.75	0.000
SMNs	1.47	0.696	0.47	0.012

Note: Privacy policy online (PPO): Dependent variable.
$PP0=a_o+a_1SMN+a2PSP+e$.
$PPO=20.38+0.696SMN-0.556PSP$.

In comparing the contribution of each IV, the "Beta values (β)" are utilized. As shown in the standardized coefficient column, the SMN makes the strongest unique contribution to the explanation with β = .696. The PSP with β= -.556 made the moderate negative contribution in predicting PPO (Table 11).Table 11 shows that the alternative hypothesis, which says that there is a strong link between the dimensions of PPO, SMN, and PSP, was accepted when looking at how each dimension affects PSP. This infers that whenever there is any modification to any of these factors, the SMN and PSP will impact the PPO. The finding of the result indicates that an upsurge in the SMN will increase the PPO. An increase in the PSP contributed negatively to the PPO.

4. Conclusion

The creation of this model is for classifying user perceptions and as a method for drawing relevant inferences from the hidden attributes and relationships within the users' perception data. The user perception indicates that an increase in the SMN leads to an increase in the PPO. According to the study, an increase in the PSP contributed negatively to the PPO. The study further shows that users were mostly students aged 18-21years with high school qualifications that spent over five hours on their preferred SMNs, which are mostly WhatsApp. Thus, the users' privacy perception towards SMNs lies in the flexibility of their usage of social media apps.

The summarised key findings from this study are:

- Of the total estimated responses from returned filled-out Google Form QTNs, 95.8% were found usable, conforming to expectations of the minimum usage rate of 70% in a face-to-face method of QTN administration.
- Demographic characteristics of the study show that the age distribution of users was 18-25 years. Majority of users of online facilities said reading a WPP before registering information is necessary for a system classification of users' perceptions of data privacy on social media networks, spending on average 2-4 hours on reading a WPP before registering information. The educational qualifications of respondents show that they had high school qualifications and other qualifications. Majority of respondents used for the current study were students, followed by those who were professionals and then educators. The users online said on a daily basis they spent mostly 5 hours and above in the study of a system classification of users' perceptions of data privacy on SMN.
- Investigating the social media platforms frequently used based on a system classification of users' perceptions of data privacy on social media networks, the findings reveal that WhatsApp and Facebook were frequently used. On average, users who have been using social media platforms said they preferred the social media networks-WhatsApp and Facebook for over 5 years as the social media networks of their choice in the study of a system classification of users' perceptions of data privacy on social media networks.

- The reliability of dimensions of a system classification of users' perception of data privacy on social media networks was based on Cronbach's Alpha, which confirmed that dimensions of factors of a system classification of users' perception of data privacy on social media networks range between 0.789 and 0.916. Therefore, justifying that all the items for the three dimensions of a system classification of users' perceptions of data privacy on social media networks are internally consistent at 86.80%.
- Main privacy policy online is to block people on SMN that they do not want to see their information, and the use of SMN apps is necessary.
- The main concern about social media networks is based on the study, which suggested that users are usually asked to grant access to too much personal information when installing the SMN app and worry that individuals outside of my intended audience may view the content I post on SMN, and SMN may sell or release my personal information to a third party.
- PSP are; comfortable sharing personal information on SMN, the privacy settings of their profile on SMN can be rated as high; and these individuals may feel that the privacy of their personal information is protected by SMNs.
- The model of privacy policy online has a correlation with SMN and PSP data privacy.
- The SMN has a positive and significant relationship with privacy policy online in a system classification of users' perceptions of data privacy on SMN and PSP.
- PSP has a negative and significant relationship with privacy policy online in a system classification of users' perceptions of data privacy.
- There is a significant relationship among the dimensions of privacy policy online, Social Media Network and PSP. Therefore, changes to any of these factors-Social Media Network and PSP impact privacy policies online.
- The adaptive k-means algorithm shows better performance as compared to the existing k-means.
- The users' privacy perception towards social media networks lies in the flexibility of their usage of social media apps.
- This study confirms that the users were influenced by their privacy perceptions using the "very strongly agree" decision.

Based on the findings and conclusion of the study, the following recommendations are made:

- As the choice of SMN increases the privacy policy online, there is a need to monitor and evaluate user perceptions from time to time to enhance data security and privacy.
- Since, PSP contributed negatively to the privacy policy online, system classification should be designed for a proper matching profile identifier.
- Online security measures should be developed to capture the SMN and PSP and enhance data privacy in Nigeria.
- An adaptive K-means algorithm is considered the best classifier; hence, online privacy experts or researchers should focus attention on the use and application of the adaptive K-mean algorithm.

References

[1] W. Nwankwo and K. E. Ukhurebor, "Web forum and social media: A model for automatic removal of fake media using multilayered neural networks," *International Journal of Scientific & Technology Research,* vol. 9, no. 1, pp. 4371-4377, 2020.

[2] M. P. Asanga, U. U. Essiet, K. E. Ukhurebor, A. Afolorunso, and P. Hussaini, "Social media and academic performance: A survey research of senior secondary school students in Uyo, Nigeria," *International Journal of Learning, Teaching and Educational Research,* vol. 22, no. 2, pp. 323-337, 2023. https://doi.org/10.26803/ijlter.22.2.18

[3] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: Comprehensive review and analysis," *Complex & Intelligent Systems,* vol. 7, no. 5, pp. 2157-2177, 2021. https://doi.org/10.1007/s40747-021-00409-7

[4] C. C. Nneji, R. Urenyere, K. E. Ukhurebor, S. Ajibola, and O. O. Onaseso, "The impacts of COVID-19-induced online lectures on the teaching and learning process: An inquiring study of junior secondary schools in Orlu, Nigeria," *Frontiers in Public Health,* vol. 10, p. 1054536, 2022. https://doi.org/10.3389/fpubh.2022.1054536

[5] W. G. Mangold and D. J. Faulds, "Social media: The new hybrid element of the promotion mix," *Business Horizons,* vol. 52, no. 4, pp. 357-365, 2009. https://doi.org/10.1016/j.bushor.2009.03.002

[6] P. Kundu *et al.*, "Analysis of security and privacy in social media platforms," *American Journal of Electronics & Communication,* vol. 2, no. 3, pp. 20-29, 2022. https://doi.org/10.15864/ajec.2304

[7] A. R. Hussaini *et al.*, "The influence of information and communication technology in the teaching and learning of physics," *International Journal of Learning, Teaching and Educational Research,* vol. 22, no. 6, pp. 98-120, 2023. https://doi.org/10.26803/ijlter.22.6.6

[8] T. A. Adaja and F. A. Ayodele, "Nigerian youths and social media: Harnessing the potentials for academic excellence," *Kuwait Chapter of Arabian Journal of Business and Management Review,* vol. 2, no. 5, pp. 65-75, 2013. https://doi.org/10.12816/0001189

[9] G. Drury, "Opinion piece: Social media: Should marketers engage and how can it be done effectively?" *Journal of Direct, Data and Digital Marketing Practice,* vol. 9, no. 3, pp. 274-277, 2008. https://doi.org/10.1057/palgrave.dddmp.4350096

[10] Z. Asif and M. Khan, "Users' perceptions on Facebook's privacy policies," *ARPN Journal of Systems and Software,* vol. 2, no. 3, pp. 119-121, 2012.

[11] V. Balakrishnan and C. L. Gan, "Students' learning styles and their effects on the use of social media technology for learning," *Telematics and Informatics*, vol. 33, no. 3, pp. 808-821, 2016. https://doi.org/10.1016/j.tele.2015.12.004

[12] J. P. Lawler and J. C. Molluzzo, "A survey of first-year college student perceptions of privacy in social networking," *Journal of Computing Sciences in Colleges*, vol. 26, no. 3, pp. 36-41, 2011.

[13] J. Williams, "Social networking applications in health care: Threats to the privacy and security of health information," in *Proceedings of the 2010 ICSE Workshop on Software Engineering in Health Care. New York, NY, USA*, 2010, pp. 39–49.

[14] K. Saravanakumar and K. Deepa, "On privacy and security in social media–a comprehensive study," *Procedia Computer Science,* vol. 78, pp. 114-119, 2016. https://doi.org/10.1016/j.procs.2016.02.019

[15] O. Onifade, M. Olomu, B. F. Ajao, M. Atoyebi, and O. Ilevbare, "Social media users perception on privacy issues in a Nigerian university," *Journal of Digital Innovations & Contemporary Research in Science, Engineering & Technology,* vol. 6, no. 2, pp. 35-46, 2018.

[16] H. T. Bui, "Exploring and explaining older consumers' behaviour in the boom of social media," *International Journal of Consumer Studies*, vol. 46, no. 2, pp. 601-620, 2022. https://doi.org/10.1111/ijcs.12715

[17] A. C. Bocar and G. G. Jocson, "Understanding the challenges of social media users: Management students' perspectives in two Asian countries," *Journal of Business, Communication & Technology,* vol. 1, no. 1, pp. 24-34, 2022. https://doi.org/10.56632/bct.2022.1103

[18] S. S. Sofian and A. S. Rambely, "Measuring perceptions of students toward game and recreational activity using fuzzy conjoint analysis," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 20, no. 1, pp. 395-404, 2020. https://doi.org/10.11591/ijeecs.v20.i1.pp395-404

[19] A. Joshi, S. Kale, S. Chandel, and D. K. Pal, "Likert scale: Explored and explained," *British Journal of Applied Science & Technology,* vol. 7, no. 4, pp. 396-403, 2015. https://doi.org/10.9734/bjast/2015/14975

[20] P. Kumaraguru and L. F. Cranor, "Privacy indexes: A survey of Westin's studies," Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, Technical Report CMU-ISRI-5-13, 2005.

[21] B. Bateman, F. Colin Wilson, and D. Bingham, "Team effectiveness–development of an audit questionnaire," *Journal of Management Development,* vol. 21, no. 3, pp. 215-226, 2002. https://doi.org/10.1108/02621710210420282

[22] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate data analysis*, 7th ed. Upper Saddle River: Pearson Education, 2014.