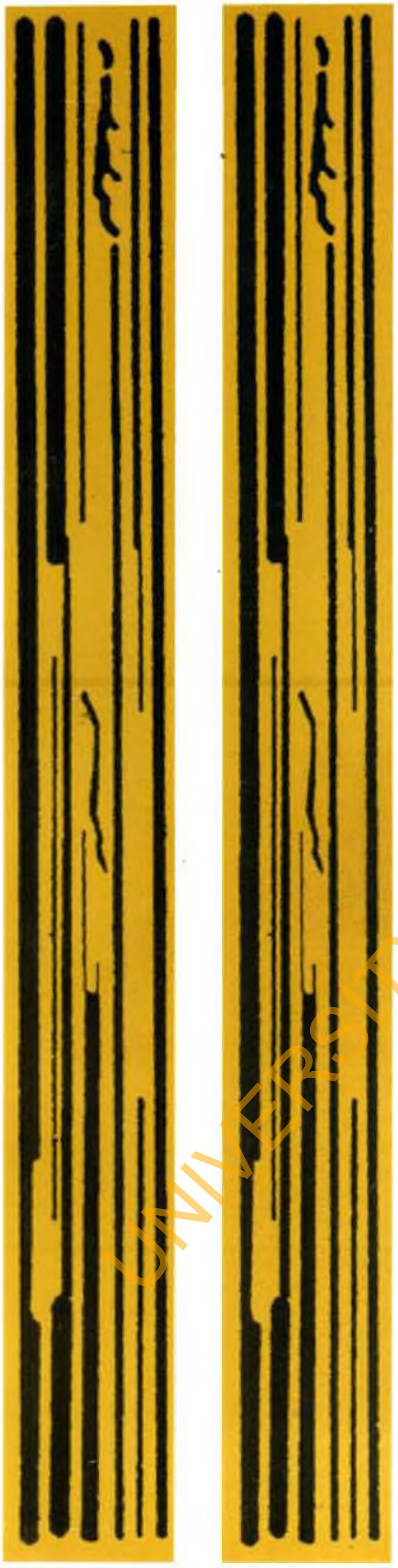


Journal of Environmental and Culture

Volume 13, 2016

Journal of Environment and Culture

Volume 13, 2016.

Publishing philosophy

Journal of Environment and Culture promotes the publication of issues, research, and comments connected with the way, culture determines, regulates, and accounts for the environment in Africa or any other parts of the world. It is interested in the application of knowledge, research and science to a healthy, stable, and sustaining human environment.

Editorial Address
Editor-in-Chief
Journal of Environment and Culrure
Department of Archaeology and
Anthropology, University of Ibadan
Ibadan, Nigeria.
e-mail: journalculture@yahoo.com

ISSN 1597 2755

The Department of Archaeology and Anthropology, University of Ibadan, publishes the Journal of Environment and Culture twice in the year, in June and December. The subscription rates are N3000 a year for local institutions and N1500 for individuals. Foreign institutions will pay US$50 and individuals, US$20.. Changes in address should be sent to Journal of Environment and Culture, Department of Archaeology and Anthropology, University of Ibadan, Nigeria.

Swift Print Limited
Nigeria

Volume 13, 2016.

Contents

© Journal of Environment and Culture
Volume 13, June 2016. Pp. 64-84
ISSB 1597 2755

Students' awareness of privacy risks in Online Interactions: a case study of students of higher institutions in Ibadan Metropolis, Nigeria.

Adeola Obafemi Mobolaji & Olayinka Abimbola Egbokhare

Abstract

Social network sites have influenced communication behaviour in a variety of contexts. This development has brought with it challenges with online privacy, self-disclosure and the overall well- being of the social media users. This study examines the interaction between, privacy awareness, privacy concerns and social media users' online behaviour. Guided by Communication Privacy Management Theory, the study adopted Survey and Focus Group Discussion (FGD) methods. The simple random technique was employed to select the study population from among the students of University of Ibadan and the Polytechnic Ibadan. From this population, Purposive and Convenience sampling techniques were used to select a sample of 330 respondents – 165 respondents respectively from each institution. Findings from this study show that Facebook and Instagram users are aware of the privacy risks attached to their online interactions. However, privacy paradox comes to the fore because, in spite of the identified privacy concerns, findings reveal that individuals still disclose personal information on the social media platforms. This apparent disregard for online privacy by many of the respondents is attributable to some gratifications the respondents claim they derive from these virtual interactions. While responding to the enquiry about what information may be disclosed online, majority of the respondents (78.2%), reported that information that pertains to one's income, financial status and bank transactions should not for any reason be posted on Facebook and Instagram. Moreover, (76.3%) of the respondents agreed that facts relating to one's family affairs should not be posted on Facebook and Instagram.

Swift Print Limited, Nigeria

Key words: Online Behaviour, Online Privacy, Privacy Concerns, Privacy Paradox, Social MediaIntroduction/Problem Statement.

The advent of social network sites such as Instagram, Facebook, Twitter, Badoo, BBM, WhatsApp, LinkedIn, and YouTube has made it possible for information to be easily passed around the globe and to network with people without necessarily meeting them in person. In this age, people communicate mostly through the use of different social media platforms. The use of social media to communicate is not only limited to people because many organisations have adopted the use of social media as a way of passing information internally or externally. Social media has redefined interpersonal communication because of its wide accessibility and fast dissemination of user-generated content. On this, Adaja and Ayodele (2013) note that the new media environment provide possibilities for conversational interaction and participation as well as generate new possibilities.

It is important to note that online sites are experiencing wide-ranging diffusion, because the accessibility and fast dissemination of user-generated content through these sites and online social networks has intensified interpersonal communications, enhanced business transparency, and generated new value creation opportunities. It has led to an era of sharing and making the life of ordinary Internet users more transparent. This justifies the submission Wieslander and Saliaropolou (2016) that the power of social networking sites is not only in terms of communication and self-expression, but also of public opinion shaping, commerce driving and changes to the society. It is obvious that social media has made communication flexible and this is why Agunbiade, Obiyan, and Sogbaike (2013) note that an increasing social category of people adopt and interact on online platforms for purposes such as self-discovery, expression, pleasure seeking and identity presentation.

There is no doubt to the fact that majority of people rely on the use of social network sites for their social interaction and this substantiates the position of Omekwu, Eke and Odoh (2012) that social network sites are modern interactive communication channels through which people connect to one another, share ideas, experiences, messages and information of interest. In addition, Graham and Avery (2003) note that social media presence is a trademark of a vibrant and transparent communications strategy. They add that, social media tools can improve interactivity between a government and the public, and they reach populations that do not consume traditional media as frequently as others. The above point confirms that the use of social media has cut across every facet of life. Through the way social media operate, it should be noted that the usage of Social Network Sites (SNS) revolves round constant sharing of information. This indicates that for social media to be enjoyed and appreciated, people must be willing to share their information and also receive from others.

However, the constant sharing of information on social media platforms has brought about the issue of social media users' privacy. This is because people's virtual interaction on social media platforms enables other social media users to have opportunity to get into other peoples' privacy. In view of this, Yat (2012) notes that the privacy problem about disclosure of personal information on social network becomes a serious issue and arouses much public concern and discussion. He adds that along with the increasing social network user base, this problem cannot be ignored because social networks contain plenty of personal information which may bring about commercial interest and illegal usage of the information.

The transparency of social network sites has not only led to privacy issue, it has also encouraged some individuals to engage in cybercrime. Based on this, Hassan, Lass and Makinde (2012) note that cybercrime involves using computer and internet by individuals to commit crime. Although the study by Lee, Im, and Taylor (2008) reveal some of the factors that motivate social media users to reveal some of their private information online, even with this, it is pertinent to know if social media users are aware of the privacy risks that are attached to their online interaction with other social media users.

Nigerian scholars have conducted studies on social media use among students of higher institutions of learning in Nigeria (Ogedegbe, Emmanuel, and Musa, 2012; Adaja and Ayodele, 2013; Folaranmi, 2013; Eke, Olasinde, 2014; Omekwu and Odoh, 2014.) however, in the work reviewed, there appears to be dearth of systematic and empirical investigation in Nigeria, on the level of privacy concerns and privacy management strategies on social network sites by students of higher institutions of learning. These are the obvious gaps that this study attempts to fill. This study therefore aims to contribute to the body of knowledge by doing research in this area in order to help other researchers in Africa and Nigeria to understand more about this phenomenon. Therefore, by using the students of University of Ibadan and the Polytechnic Ibadan as case study, this study aims to investigate the extent to which students in Ibadan metropolis are aware of the privacy risks attached to their online interactions with other social media users. In addition, the study seeks to investigate the categories of information that students believe should be shared or not to be shared on social media platforms.

Research Question

Taking into consideration all that have been explained, the following research question will therefore be the focus of this study:

- To what extent are social media users aware of the privacy risks in their online interactions?

Review of related concepts.

The concept of Internet Privacy and Privacy Concern

In the online context, a common understanding of privacy is the right to determine when, how, and to what extent personal data can be shared with others. Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself through the internet. The issue of privacy can come in different manners. Finn, Wright, and Friedewald, (2013), distinguish between invasion involving extraction and observation and intrusion. They note that, extraction-based privacy invasion involves making a deliberate effort to obtain something from a person. Observation-based privacy invasions are characterized by the active and on-going surveillance of the person, whereas intrusion based invasion involves an unwelcome presence or interference in a person's life (Finn, et al. 2013). The submission of Finn et al shows different ways by which peoples' privacy can be infringed.

Thus, as evidence accumulated about privacy management in the use of social media, scholars began to investigate into the area of social media users' privacy concern. According to Chenamanneni and Taneja (2015:4) "Privacy concern is defined as individuals' concerns regarding how their information could be used or exploited when shared". According to Hongliang, Christopher, Beaudoin and Tracyl (2016), privacy concerns involve peoples' worries about their capacity to control how much of their private information is exchanged with others. In the same vein, Chung and Paynter (2002) note that invasions of privacy occur when individuals cannot maintain a substantial degree of control over their personal information and its usage. Therefore, concerns about privacy are borne out of the fact that the transparency of the internet has allowed people to have access to some important information about others and this seems to have cast a dark shade on the use of social media as a whole.

There seems to be a lot of complexities when exploring the concept of privacy as regards the usage of social media. This complexity stems from the lens through which individuals view privacy. Xu, Dinev, Smith and Hart (2011:80) note that "because of the complexity of and inconsistencies in defining and measuring privacy, per se, and also because the salient relationships depend more on cognitions and perceptions than on rational assessments, almost all empirical privacy research in the social sciences rely on measurement of a privacy-related proxy of some sort". The quote explains that the idea of what privacy means could be determined by the way of reasoning and perceptions of social media users. This suggests that the level of cognition and the variance of privacy perception will also influence the concern of various individuals about their online privacy.

However, Hongliang, Christopher, Beaudoin and Tracy (2016) hold that online privacy concerns and awareness of online information disclosure are predicted by two types of negative privacy experiences: stolen information and relational conflict. They explain further that stolen information is experiencing the theft of sensitive private information such as bank account or security numbers. On the other hand, relational conflict refers to the relational troubles that are brought about by unauthorized use of online postings and which could lead to troubles in relationship with families and friends, damage to personal image and loss of social and other opportunities. Based on Altman□s conceptual definition of privacy as a selective control of access to self, Blank, Bolsover and Dubois (2014) view privacy concern as an individual□s ability to control what personal information is disclosed, to whom, when and under what circumstances.

But despite the online privacy concerns by social media users, literature has revealed that some social media users still reveal their private information on social media platforms; and this is where privacy paradox comes in (Van der Velden and El Eman, 2012). Privacy paradox is the dichotomy of information privacy attitude and actual behaviour, Kokolakis (2015). In another perspective, the privacy paradox is the discrepancy between privacy concerns and actual privacy settings (Barnes cited by Utz and Kramer, 2009). This is also pondered on by Acquisti and Gross (2006), and they state that due to the free flow of interaction that Social Network Site like Facebook has given to its users, millions of privacy concerned people wittingly reveal highly personal information to friends and strangers. They however note that 'nobody is literally forced to join an online social network to reveal sensitive information like dates of birth, phone numbers, and location. And yet, one cannot help but marvel at the nature, amount and detail of personal information some users provide'. They further submit that online social networks' security and access control are weak by design-to leverage their value as network goods and enhance their growth by making registration, access and sharing of information uncomplicated.

Online Privacy Risks

Online communication through the use social media is a trend that has come to stay. A lot of people in this global age prefer communicating online to face-to-face interaction due to its dynamic and participatory nature (Cann, 2011, Sawyer 2011, Baruah 2012, Ezeah, Asogwa and Edogor, 2013). Though privacy was always valued, it has now become more significant, especially since the advent of Internet (Chennamaneni and Taneja, 2015). The use of social media has brought with it issues of online privacy where many social media users tend to be carried away by the pleasure of online virtual interactions, thereby forgetting to secure their online privacy boundaries. Reacting to this, Acquisti, Brandimarte and Loewestein (2015) reveal that due to online communication, activities that were once private or shared with the few now leave trails of data that expose our interests, traits, beliefs, and intentions. A lot of risks are attached to the sharing of personal information online.

Aldhaferri, Watson and Sajeev (2013) point out that there are several risks surrounding the posting of personal information details on social networks. They add that these threats can be caused by hackers or spammers who obtain users' personal information details. This shows that hacking of personal information is one of the common risks associated with sharing of one's personal information online. But even with this, social media users still reveal vital personal information online and this justifies the argument of Koehorst (2013) that despite existing threats like privacy issues, potential for misuse of data, unwanted access to information, risk for child safety and online bullying, and negative psychological effects of social networking, people continue to reveal massive amounts of personal information on online social networks (OSNs).

Another online privacy risk that is worthy of mentioning is the one that has to do with service providers. Based on this, Aldhafferi, et al. (2013) submit that users usually upload their personal information when they trust the service provider. However, the provider can use these details for business purposes such as advertising. In the same vein, Ladan (2015:2) writes that:

> Facebook, along with MySpace, and a handful of other social networks, have been sharing users' personal data with advertisers without users' knowledge or consent. The data shared includes names, user IDs, and other information sufficient to enable ad companies, such as the Google-owned DoubleClick to identify distinct user profiles. Moreover, Facebook appears to have gone farther than the other networks when it comes to sharing data. When Facebook's users clicked on ads appearing on a profile page, the site would at times provide data, such as the username behind the click, as well as the user whose profile page from which the click came.

The above excerpt has shown that many companies engage in data mining to obtain customers' information without consent through their social media platforms. In the light of this, Chewae, Hayikader, Hassan and Ibrahim (2015) also highlight the potential risks of posting personal information on social network. According to Chewae, et al. (2015), some of these risks are: stolen identity, advertising harassment scam, personal information identity theft, phishing, and government spy. Similarly, Strater and Lipford (2008) reveal that the most reported privacy concern of social media users is being stalked and physically located by a stranger.

Based on this, Strater and Lipford (2008) argues that, social media users should be careful in disclosing information that has to do with contacts, home addresses, and course schedules. Paine, Reips, Stieger, Joinson, and Buchanan (2007:532) however state how social media users can achieve some level of online decorum as they note that "for example, social media users may not reveal their real name, change it or use a nickname, and they can limit the amount of information they provide: Not to show e-mail address, phone number and details about them to everyone".

There is no doubt about the fact that social media users are at the risk of losing their privacy while using social media platforms. The privacy risks that are attached to the use of social media are endless; however, ensuring some levels of online privacy depends on how well social media users can secure and manage their privacy boundaries. However, another argument was foregrounded by Li, Sarathy and Xu (2010:3) that "the effect of privacy concern is very likely to be overridden by various situational factors at a specific level; individuals are more likely to disclose personal information if risks could be offset by benefits". The implication of this is that rewards and enticements could influence peoples' level of privacy concern in their online engagements with other social media users.

Communication Privacy Management Theory

The study of social media privacy is situated in Communication Privacy Management theory which is a systematic theory that is designed to develop an evidence based understanding of the way people make decisions about revealing and concealing private information. Communication Privacy Management Theory is a lens through which scholars analyse how individuals manage their private information and the ways in which they negotiate sharing it with others. By focusing on privacy, CPM changes the focus from information about the self to the communicative process by which people conceal or reveal private information (Brittain, 2013).

In LittleJohn and Foss (2009), Communication Privacy Management Theory was explained to have used a metaphoric boundary between what is personal and what is public to illustrate how people conceptualize the process of privacy management. According to Petronio (2002), when people disclose private information, they depend on a rule-based management system to control the level of accessibility. Petronio adds that an individual's privacy boundary governs his or her self-disclosure. Once a disclosure is made, the negotiation of privacy rule between the two parties is required. This simply means that the rate at which someone divulges his secret to another party is determined by the level of privacy boundaries.

Communication Privacy Management Theory operates on six principles. On the six principles, Petronio and Rierson (2009:366) explain that people believe they own private information, which defines the parameters of what constitutes the meaning of private information; secondly, because people believe they own private information, they also believe that they have the right to control that information. Furthermore, to control the flow of their private information, people use privacy rules they develop based on criteria important to them; in addition, once they tell others their private information, the nature of that information changes, becoming co-owned by the confidant. The fifth principle says that once the information is co-owned, ideally the parties negotiate collectively held and agreed-upon privacy rules for third-party dissemination. Lastly, people do not consistently, effectively, or actively negotiate collectively held privacy rules, there is the possibility of "boundary turbulence" which means that there are disruptions in the way that co-owners control and regulate the flow of private information to third.

The application of this theory is relevant in examining the level of privacy awareness and privacy concerns of social media users. Apart from this, the theory explains how social media users can manage and coordinate their privacy boundaries by applying the principles that are laid down by the theory. In addition, this theory is relevant to this study because its knowledge and application will guide the way people make decisions about revealing and concealing private information. Thus, since the theory is a lens through which scholars analyse how individuals manage their private information and the ways in which they negotiate sharing it with others (Brittain, 2013); its understanding will help social media users to properly understand what is personal and what is public and which will tell how they conceptualize the process of privacy management

Methodology

The research methods adopted for this study were survey and Focus Group Discussion (FGD). Survey was suitable for this study because the researcher was able to elicit information concerning respondents' beliefs, behaviours views and perceptions. Focus Group Discussion (FGD) was also chosen to get the detailed knowledge, reasons and rationale behind each of the respondents' views and responses on the following research question.

- To what extent are social media users aware of the privacy risks in their online interactions?

Sampling and Sample

The study made use of the Purposive, Convenience and Quota sampling techniques to select the sample for this study. Purposive sampling technique was used to select students with accessibility to social media tool, especially Facebook and Instagram. Students were considered suitable for this study because it is believed that students are the highest users of social media and they fall within the demographs of online citizen. Therefore, students with accessibility to social media tool, especially

Facebook and Instagram were purposively sampled. Facebook and Instagram were chosen for this study because they are part of the most popular social networks used by Nigerian students (Anyanwu, Ossai-Onah and Iroeze, 2013; Akanni, 2014). In addition, the selected students were those that are active on a social network site, at least twice a week and who are willing to participate in the study.

Moreover, University of Ibadan and Polytechnic Ibadan were selected for the study. The reason for this selection was because the two institutions were considered accessible to the researcher. Secondly, the two institutions are the most populated in Ibadan metropolis and to a large extent, they represent the heterogeneous Nigerian youths. For survey, the representative sample drawn from the population for this study was a total of 330 across the two selected higher institutions in Ibadan, that is, 165 respondents from each institution. Quota sampling was also used by the researcher to select a total of 16 participants to participate in the two sessions of Focus Group Discussion (FGD).

Data Collection and Analysis

A total number of 330 Copies of the questionnaires were administered to respondents by the researcher and some research assistants in the selected locations for the study. Out of the 330 questionnaires administered, only 312 copies were retrieved. Data were analysed through frequency counts and simple percentage score with findings presented in tables while responses from the Focus Group Discussion were recorded, transcribed and extracted to support findings from the study.

Results

Participants for the study

Table 1: Classification of Respondents' by Age

AGE (years)	Frequency	Percentage (%)
16-20	155	49.7
21-25	128	41
26-30	26	8.3
31-35	3	1
Total	**312**	**100**

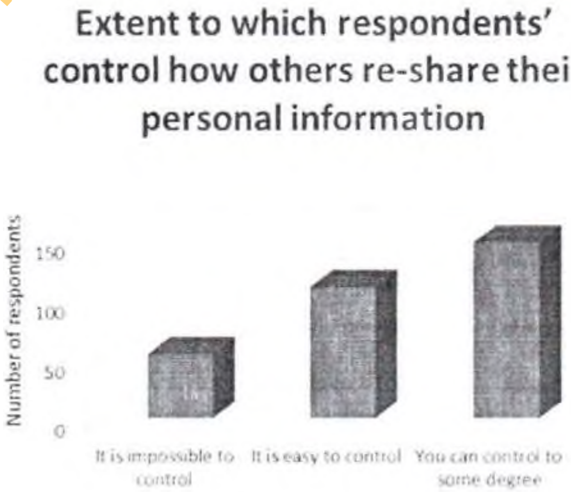
Table 1 shows that majority of the respondents 155(49.7%), 128(41%) are within the age range of 16-20 and 21-25 years respectively. Two factors may account for this age distribution; it is either because the study was conducted in an academic environment dominated by young adults or because students in the institutions sampled are active users of social media

Table 2: Extent of Respondents' concern about online privacy

Respondents' level of privacy concerns	Frequency	Percentage (%)
Not at all concerned	22	7.1
Slightly concerned	55	17.6
Moderately concerned	81	26
Very concerned	110	35.3
Extremely concerned	44	14.1
Total	**312**	**100**

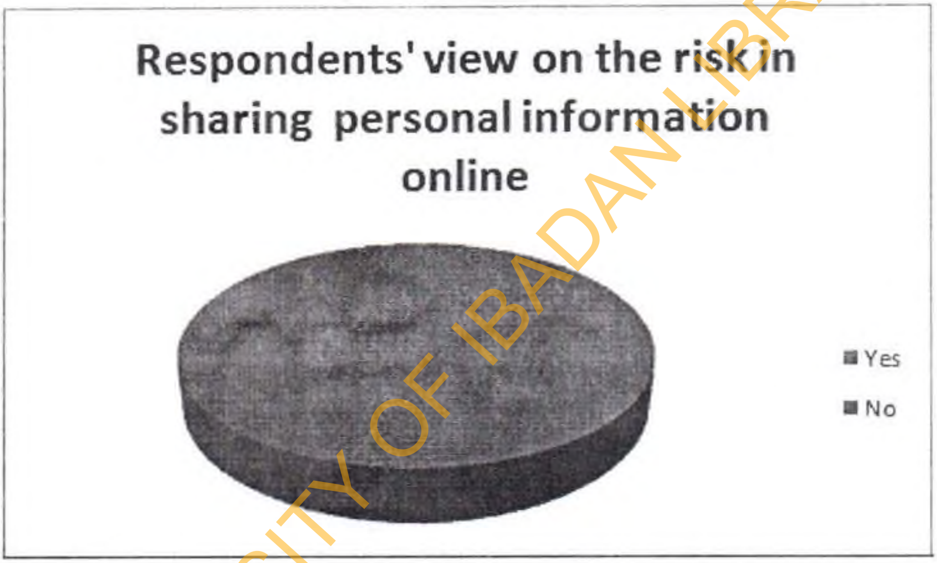
As regards privacy concerns on Facebook and Instagram, 110 respondents, representing 35.3% of the sample affirmed that they are very concerned about their privacy on Facebook and Instagram, while 81 (26%) respondents reported that they are moderately concerned. Moreover, 55 (17.6%) of the respondents said that they are slightly concerned while 44 (14.1%) respondents revealed that they are extremely concerned. Only 22 respondents, representing 7.1% of the sample revealed that they are not concerned about their privacy on Facebook and Instagram.

Figure 1: How respondents control how others re-share their personal information



When the respondents were asked the extent to which they can control how others re-share personal information which they share on Facebook and Instagram, 54 respondents, representing 17.3% revealed that it is impossible to control. 110 (35.3%) respondents indicated that it is easy to control, while 148 (47.4%) respondents posited that it can be controlled to some degree.

Figure 2: Respondents' view on the risk in sharing personal information on Facebook and Instagram



Respondents were asked if there are privacy risks in sharing personal information on Facebook and Instagram. 278 respondents representing 89.1% concurred with this view, while only 34 respondents of 10.9% disagreed with this notion.

Information categories (variable)	Yes, we should post them. *(frequency and percentage)*	No, we should not post them. *(frequency and percentage)*	Total	%
Income, Financial Status and Bank Transactions	68 (21.8%)	244, (78.2%)	312	100
Family Affairs	74 (23.7%)	238 (76.3%)	312	100
Health Condition	90 (28.8%)	222 (71.2%)	312	100
Sexual Life	98(31.4%)	214 (68.6%)	312	100
Future Plans	99 (31.7%)	213 (68.3)	312	100
Current Location	99 (31.7%)	213 (68.3)	312	100
Travelling or Movement Plans	97 (31.1%)	215 (68.9%)	312	100
Potentially Stigmatising information	103 (33%)	209 (67%)	312	100
Personal Fears	107 (34.3%)	205 (65.7%)	312	100
Pictures or videos showing in your living room or bedroom and layout of your home	113 (36.2%)	199 (63.8%)	312	100
Relationship Status	114 (36.5%)	198 (63.5%)	312	100
Success Story	126, (40.4%)	186 (59.6%)	312	100
Deeply held religious convictions	137 (43.9%)	175 (56.1)	312	100

Table 3: Respondents' reaction on specific information that should be shared or not shared at all on Facebook and Instagram

When respondents were asked about their views on various online behaviours that Facebook and Instagram users' exhibit, findings as reported in Table 4.6 make it clear that the study population perceives the online behaviour of Facebook and Instagram users as poor. Table 4.6 shows that 291 respondents, representing 93.3% of the sample agreed that people are generally careless about what they say on social media platforms. Furthermore, a total number of 296 (94.8%) respondents affirmed that people accept friend requests from strangers without minding the risk. Findings further show that, 265 (84.9%) respondents agreed that people always lose their sense of privacy while on Facebook and Instagram, while 278 (89.1%) respondents posited that people think social media platforms are okay for regular updates of ones activities.

Discussion of Findings

The study reveals that majority of the respondents aware of privacy risks in their online interactions with other social media users. In essence, irrespective of the reason people make use of Facebook and Instagram; they still place high value on their privacy. It is important to note that one of the reasons social media users are concerned about their online privacy is because the information they post online could be wrongly obtained and abused by other social media users. Social media users place high regard on their privacy because they can be exploited by criminals who fraudulently obtain information from unsuspecting users (Okesola, Onashoga and Ogunbawo, 2016). According to Chenammaneni and Taneja (2015), such social media abuses also include online stalking, bullying, slandering one's reputation, digital dossier aggregation, organisational threats and more. However, in one of the Focus Group Discussions conducted, one of the discussants expressed a contrary view that there should not be any concern about privacy while using Facebook and Instagram. The discussant noted that

When individuals maintain self-discipline as regards what to disclose and what to keep private in his online activities, he may not have any privacy related issue. There are privacy settings that can help users to maintain a reasonable level of privacy. Facebook and Instagram can authorise users to use the privacy control setting.

Majority of the discussants however concluded that many Facebook and Instagram users have a careless attitude towards the use of privacy control settings and this makes protection of online privacy difficult to achieve. This view is justified by Ellison et.al (2011) that, Facebook users' attention to the use of privacy control is very poor and this makes it difficult for them to navigate the privacy settings of the Facebook interface. Poor attitude and poor attention of Facebook and Instagram users towards privacy control settings are likely to be caused by online distractions, online negligence and eagerness for online interaction. By implication, the instant gratification that is being derived from Facebook and Instagram could easily distract users from making use of privacy control settings. Thus, much information is being posted in order to keep up with the online trend and social media tempo without minding the privacy risks attached.

Furthermore, findings from this study revealed that that it is not every social media user that knows about the privacy control settings. It was also found out that some social media users do not have the proper knowledge of the social media platforms they are using. Therefore, this lack of understanding of the demands of the application affects the proper engagement of privacy control setting. Also, majority of the discussants in the Focus Group Discussions noted that the reason for their extreme privacy concerns on Facebook and Instagram is because the platforms are so wide and open. A discussant in the Focus Group Discussion stated that:

Once someone tags you on a post or a friend mentions your name in a comment, the post reaches you automatically

On a general note, findings from this study revealed that Facebook and Instagram users are aware and very concerned about their online privacy. Moreover, in a bid to know how respondents control how others re-share their personal information online, findings from this study revealed that through a proper knowledge of the usage of privacy settings that are available on Facebook and Instagram, one can still exercise some control on how one's information is re-shared by other users. It could also be inferred that the level at which social media users control how others re-share their personal information could be determined by the kind of privacy rules and privacy boundaries that they operate. This corroborates the view of Petronio and Rierson (2009) that people treat their private information in different ways, adjusting the level of permeability according to rules that protect and rules that grant access. They further pointed out that in order to ensure confidentiality and boundary co-ordination, social media users must have privacy rules for ownership of information, privacy rules for permeability, and privacy rules for linkages.

Thus, the level at which social media users make use of the privacy co-ordination rules will determine how others can have access to their information. In line with this, one of the FGD discussants affirmed that:

The use of privacy control settings is still the most reliable way to control how others re-share one's information on Facebook and Instagram

The discussant noted that this could be done by setting privacy control for information access and visibility. Privacy control settings for access and visibility will limit the number of people that can see what one posts online. The discussant stressed that:

Through the use of the privacy control setting, Facebook and Instagram users can control peoples' access to their profile and information.

Moreover, part of the risks involved in online sharing of personal information online is that the information shared may be used against the owner. Similarly, in the FGD discussion, a discussant noted that:

Facebook is a platform where people can be easily duped because; hackers and fraudsters get information about their victims mostly from the platform

The response from the respondents substantiates the view of Okesola etal (2016:3) that "majority of the website users do not pose a threat, malicious individuals might be drawn to them because of the ease of access of data and the volume of available personal information". According to the findings, personal information that should not be posted on Facebook and Instagram include financial status, family affairs, sexual life, future plans, current locations, relationship status, travelling or movement plans. As regards this, one of the discussants in the Focus Group Discussion shared a story that goes thus...

A house was burgled and when the police apprehended the robber, he was asked how he managed to gain entrance to the big mansion without fear and he answered the police that he saw the Facebook update of the owner of the house that all the family members are presently in Dubai for a family vacation.

This shows that sharing personal information on wide social media platforms like Facebook and Instagram is risky, Furthermore, based on the results on Table 3, findings revealed that information about one's success story can be posted on Facebook and Instagram. Moreover, the study also revealed that information about one's strongly held religious belief should not be posted online. However, some of the respondents (43.9%) viewed that there is no risk in posting information about one's strongly held religious beliefs on Facebook and Instagram. Similarly, some of the FGD discussants also added that personal information about their religious beliefs and success stories are posted online 'so that others can learn and receive inspirations from them'. The implication of this finding is that Facebook and Instagram users have different views about privacy in their online interactions, especially in the aspect of information that pertains to religion and success stories. To some social media users, religion may occupy a private space, while some individuals may see their deeply held religious views as something that can be made public on social network sites.

Bobkowski and Pearce (2011:7) also joined the argument on religion that "no matter how profile owners are, their likelihood and rate of religious self-disclosure may be shaped by their attitudes and perception about religion". Those who believe religion is a private matter or have more negative evaluations of organised religion will likely disclose less religion content on their social networking profiles (Bobkowski and Pearce, 2011:7). It could be inferred from the foregoing that religion is a delicate issue and social media users' post on religion is determined by their religious attitude and perception. In the light this, Bobkowski and Pearce, (2011) conclude that those who view religion as private are less likely to disclose about their religiousity than those who view religion as something to share publicly.

In addition, it is noteworthy that, different individuals' privacy uncertainty, privacy beliefs and perception may perhaps be the reason for divergent views by respondents as regards what kind of information one should share or not share on Facebook and Instagram (Paine, et al. 2007; Acquisti, et al. 2015). In essence, social media users hold different views about privacy and the kind of understanding they have on privacy will define the kind of information they post on social media platforms. However, Acquisti, et al. (2015) advanced that, some social media users are ignorant and they lack privacy awareness. Thus, they are likely to be uncertain about how much information to share. It is evident that, there is a relationship between social media users' privacy perception and their online behaviour. Simply put, privacy perception could shape social media users' online behaviour in terms of privacy management and relationship with other social media users.

The results shown on Table 4 reveal some online behaviour that some Facebook and Instagram users exhibit. Findings as reported in Table 4 make it clear that the study population perceives the online behaviour of Facebook and Instagram users as poor. Findings from this study reveal that people are generally careless about what they say on social media platforms. Supporting this fact, one of the FGD discussants said that:

Most users of Facebook and Instagram have turned Facebook and Instagram into a diary pad where they update all their daily activities
Another discussant in the FGD said that:

Some personal information that social media users share on Facebook and Instagram make them easy target for bad people; and in most cases, the carelessness of social media users about information they post online could be motivated by their personal intention to oppress and compete with other social media users.
Also, the discussants were of the opinion that many users of Facebook and Instagram lack online literacy and due to this, they do not understand the privacy risks that are attached to their online engagement.

As regards lack of online literacy, a male discussant warned that even before social media users sign up on any social media platform,
They need to pay attention to the privacy- related terms and conditions of the particular social media platform they want to use.

His point was accompanied with a chorus from other discussants that 'we don't read it'. This further shows that the attitude of social media users towards online privacy is poor. In addition, one of the discussants said that, if the purpose of something is not known, abuse is inevitable. Based on this, the discussant explained that many social media users do not know the 'why and how' of the usage of social media, and that is why they abuse it.

Another discussant was of the view that:
People don't really care about what they post as far as they are able to gain online attention, initiate online interaction with others and gather many "likes" through that particular post.

It was also found out from the discussion that some Facebook and Instagram users beg people to like and comment on their post. People with this kind of online behaviour may not mind any privacy threat in their social media activities. Similarly, Rime (2016) note that online social interactions have led to an increased interest in how much information individuals reveal and share about themselves in such encounters. This finding has further revealed that, the gratification sought by Facebook and Instagram users could easily distract them from taking necessary precautions to managing their privacy in their online engagement.

The findings from the FGD also revealed that especially on Facebook, people carelessly accept and add strangers to their friends' lists just for the sake of maintaining connections and relate with a large network of people. This view is expressed by, Farrugia (2013:11) who observes that:

Facebook creates attraction through display of profile pictures; seeing a profile picture online is comparable to seeing a person from across the room where then a person can decide if they are attracted to them. From the point of initial attraction, Facebook allows users to add the individual as a friend, inbox message them, or 'poke' them with just a few clicks.

Moreover, findings from this study show that on Instagram, people compete with the number of followers they have. Thus, in a situation where people celebrate the number of followers they have on Instagram, creating privacy boundary on such platform will be of no use. Based on the results on Table 4, it was revealed that social media users always lose their sense of privacy while on Facebook and Instagram. In the same vein, it was found out that people think social media platforms are okay for regular updates of ones activities. To further confirm this opinion, discussants at the FGD revealed that people regularly update their activities on Facebook and Instagram in order to show off and create an online identity.

The implication of this finding is that, social media has become the way of life of so many people, and they cannot live any moment of their lives without posting information about themselves on social media platforms. This standpoint is justified by Herring and Kapzidic (2015) that, social media users post cute pictures, textual information, links in order to present an online self. They add that self-presentation is generally considered to be motivated by a desire to make a favourable impression on others, or an impression that corresponds to one's ideals. Thus, in a bid to be gratified on social media, Facebook and Instagram users tend to be relaxed when it comes to online privacy management.

Conclusion and Recommendations

At the outset, it was stated that as social media and the communicative flexibility they offer become fundamental in many individuals' life, social norms and daily experiences, privacy concerns, what to disclose, to whom, and how to ensure that others are not invading on someone's privacy are increasingly salient. This study has established the fact that there are privacy risks in individuals' engagement on Facebook and Instagram, and social media users are aware. The study also confirmed that Facebook and Instagram users are very concerned about their privacy, they are conscious of different privacy sensitive online behaviour and they know some categories of information that they are not meant to post on the platforms. But despite the privacy concerns, social media users still exhibit some careless online behaviour by disclosing some of their private information on Facebook and Instagram; this inconsistency of privacy attitudes and privacy behaviour is what Kokolakis (2015) referred to as the "privacy paradox". In addition, the study established that social media users' privacy concern is defined by individual's perception of privacy. This is particularly evident in the aspect of religion as the study confirmed that individual's perception of religious matter will govern what they post about religion on social networks; people that view religion as a private matter will not disclose their deeply held religious belief publicly and vice versa.

Based on the findings and the conclusion reached, Facebook and Instagram users should be careful of the kind of information they post about themselves on the platform. They should have online self-consciousness and self-monitoring so that their online privacy can be safeguarded to a great extent. Individuals should also let their privacy concerns spur them to creating their privacy boundaries on the platforms. Moreover, individuals should cultivate the habit of learning and making use of the privacy control settings that are provided by Facebook and Instagram. In the same vein, social media users should be orientated on social media use so as to increase their online literacy; with this, they will make use of every social media platform effectively without risking their privacy. As it was revealed in this study, it is suggested that Nigeria's social media users should be mindful of their environmental and social cultural context. This to a great extent will guide individuals' online behaviour. In addition to this, Federal Government of Nigeria should come up with social media law that will regulate social media use.

References

Acquisti, A. and Gross, R. 2006. Imagined Communities: Awareness, Information Sharing and Privacy on the Facebook. Pre-Proceeding Version. Privacy Enhancing Technology Workshop (PET) Carnegie Mellon University. Pittsburgh, PA

Acquisti, A., Brandimarte, L. and Loweinstein, G. 2015. Privacy and Human Behaviour in the Age of Information. Sage Publications

Adaja, T.A.; Ayodele, F.A.(2013). Nigeria Youths and Social Media: Harnessing the Potentials for Academic Excellence. Singaporean Journal of Business

Economics and Management Studies Volume 1, No 6.

Agunbiade, O.M.; Obiyan, M.O.; Sogbaike, G.B. (2013) identity construction and gender involvement in online social networks among undergraduates in two universities, Southwest, Nigeria. Inkayiso Journal of Humanities and Social Sciences 5(1). Page 41-52

Aldhaferi, N, Watson, C, Sajeev, A.S.M. (2013). Personal Information Privacy Settings of Online Social Networks and their Suitability for Mobile Internet Devices. International Journal of Security, Privacy and Trust Management. Volume 2, No 2.

Anyanwu, E.U.; Ossai-Onah, V.O.; Iroeze, P. (2013). Use of Social Media Tools among Nigerian Undergraduates in three selected tertiary institutions in Imo State, Nigeria. Journal o: Information and Knowledge Management. Volume 4, No 2 pp. 46-52

Baruah, T. D. 2012. Effectiveness of Social Media as a Means of Communication and its Potential for Technology enabled Connection: A Micro-Level Study. International Journal of Scientific and Research Publication, 2(5)

Blank, G., Bolsover, G. and Dubois, E. 2014. A new Privacy Paradox: Young People and Privacy on Social Network Sites. Published by Oxford Martin School, United Kingdom.

Bobkowski, P.S. and Pearce, L.D. (2011). Baring their souls in online profiles or not? Religious self-disclosure in social media. Journal for the scientific study of religion. 50(4), 744-762.

Brittain, K. A. C. 2013. "This is not about me: Communication Privacy Management theory and Public confession". Thesis prepared for the Degree of Masters of Science. University of Texas.

Chennamaneni and Taneja 2015. Communication Privacy Management and Self-Disclosure on Social Media: A Case of Facebook. A paper delivered at the 21st America conference on information systems, Puerto Rico.

Chewae, M, Hayikader, S, Hassan, M.H, Ibrahim, J (2015). How Much Privacy We Still Have on Social Networks? International Journal of Scientific and Research Publications, Volume 5, Issue 1.

Ellison, N.B., Vitak, J., Steinfield, C., Gray, R., Lampe, C. 2011. Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. S. Trepte and L. Reinecke (eds.), Privacy Online. Michigan State University. USA.

Ezeah, G.H.; Asogwa, C.E.; Edogor, I.O. (2013) Social Media Use among Students of Universities in South East Nigeria. Journal of Humanities and Social Sciences. Volume 16, Issue 3, pp. 23-32

Farrugia, R. C. 2013. "Facebook and Relationships: A Study of How Social Media Use is Affecting Long-Term Relationships". A thesis of the Rochester Institute of Technology, Department of Communication, College of Liberal Arts.

Finn, R. L., Wright, D., Friedewald, M. 2013. 7 Types of Privacy. Retrieved from www.researchgate.net. On 23rd of January, 2016

Folaranmi, O.A. (2013). A survey of Facebook Addiction level among selected Nigerian University Undergraduates. New media and Mass Communication. Volume 10 pp. 70-80

Graham, M and Avery, E. J. 2013. Government Public Relations and Social Media: An analysis of the Perceptions and Trends of Social Media use at the Local Government Level. Journal of the Public Relations Society of America, 7(4)

Harvey, J. and Soltren, J. H. 2005. Facebook: Threats to Privacy. Retrieved from www.groups.csail.mit.edu on the 23rd of May, 2017

Hassan, A.B.; Lass, F.D.; Makinde, J. (2012) Cybercrimes in Nigeria: Causes, Effects and the Way Out. Journal of Science and Technology. Volume 2, No 7. Pp 626-631.

Herring, S. C. and Kapidzic, S. 2015. Teens, Gender and Self Presentation in Social Media. International Encyclopaedia of social and Behavioural Sciences, 2nd edition. Oxford: Elsevier

Hongliang, C., Christopher, E., Beaudoin and Tracy, H. 2016. Protect One Online: The Effect of Negative Privacy Experiences on Privacy Protective Behaviours. Journalism and Mass Communication quarterly, 93(2): 409-429

Kokolakis, S. 2015. Privacy Attitude and Privacy Behaviour: A Review of Current Research on Privacy Paradox Phenomenon. Retrieved from www.researchgate.net on the 28th of January, 2015.

Ladan, M.I. (2015). Social Networks: Privacy Issues and Precautions. A Publication of the 9th International Conference of the Digital Society.

Lee, D. H., Im, S. and Taylor, C. R. 2008. Voluntary Self-Disclosure of Information on the Internet: A Multi-method Study of the Motivations and Consequences of Disclosing Information on Blogs. Journal or Psychology and Marketing, 25(7): 692-710

Li, H.; Sarathy, R.; Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. Journal of computer information system.

LittleJohn, S. and Foss, K. 2008. Theories of Communication (9th edition) Thomas USA, Wardsworth.

Littlejohn, S. W. and Foss, K. 2009. Encyclopaedia of Communication Theory. Sage Publication.

Ogedegbe, P.M.; Emmanuel, J.A. Musa, Y (2012). A survey of Facebook and Academic Performance in Nigerian Universities. International Journal of Engineering Research and Application. Volume 2, Issue 4, pp. 788-797

Okesola, O.; Onashoga, A.,; Ogunbanwo, A. (2016). An investigation into users' information security awareness on social networks in South Western Nigeria. South African Journal of Information Management. 18 (1) page 1-7

Olasinde, E. A. (2014). An analysis of the influence of social media sites on Nigerian undergraduates. international policy brief series- Education & Science Journal. Volume 4, No 1, pp. 53-65

Omekwu, C.O.; Eke, H.N.; Odoh, N.J. (2014). The use of social networking sites among the undergraduate students of University of Nigeria, Nsukka. Journal of Library Philosophy and Practice (1).

Paine, C. Reips, U., Stieger, S., Joinson, A., and, Buchanan, T. 2007. Internet Users Perception of Privacy Concerns and Privacy Actions. International Journal of Human Compu.er Studies. 65: 526-536

Petronio, S. 2002. Boundary of Privacy: Dialectics of Disclosure. Sunny Press.

Petronio, S. and Rierson, J. 2009. Regulating Privacy of Confidentiality: Grasping the Complexities through Communication Privacy Management Theory. Routledge.

Rime, B, 2016 Self-Disclosure. Encyclopaedia of Mental Health, 2nd edition, Volume 4, Waltham MA: Academic Press, 66-74

Strater, K.; Lipford, H.R. (2008). Strategies and Struggles with Privacy in an Online Social Networking Community. Published by the British Computer Society.

Utz, S., and Kramer, N. C. 2009. The Privacy Paradox on Social Sites Revisited. The Role of Individual Characteristics and Group Norm. Journal of Psychological Research on Cyberspace 3(2) Article 1

Van der Velden, M.; El Emam (2012). "Not all my friends need to know". A qualitative study of teenage patients, privacy and social media. Retrieved from Google scholar on the 13th of March, 2019.

Wieslander, J. and Saliaropoulou, P. 2016. Individual Privacy Management Behaviour on Social Networking Sites (SNS) Examining the Actual Use of Privacy Settings. Master□s thesis 15 HEC, Course INEM 10 in informatics presented in 1st June, 2016

Xu, H. Dinev, T., Smith, J. and, Hart, P. 2011. Information Privacy Concerns: Linking Individual Perceptions with Institutional Assurances. Journal of the Association of Information Systems. Volume 12, pp. 798-824

Yat, S. C. 2012. "Factors affecting Online Self Disclosure of University Facebook Users". An Honour Degree Project submitted to the School of Business in partial fulfilment of the Graduation Requirement for the Degree of Bachelor of Business Administration (Honours) Hong Kong Baptist University. Hong Koong.