The African Journal of Information Systems

Volume 15 | Issue 1 Article 3

February 2023

Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria

Funmilola Olubunmi Omotayo
University of Ibadan, Nigeria, lolaogunesan@yahoo.com

Joy Oluwabukola Olayiwola
Federal Polytechnic, Ilaro, Nigeria, olu23_2002@yahoo.com

Recommended Citation

Omotayo, Funmilola Olubunmi and Olayiwola, Joy Oluwabukola (2023) "Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria," *The African Journal of Information Systems*: Vol. 15: Iss. 1, Article 3.
Available at: https://digitalcommons.kennesaw.edu/ajis/vol15/iss1/3

The African Journal of Information Systems

Privacy and Security Information Awareness and Disclosure of Private Information by Users of Online Social Media in the Ibadan Metropolis, Nigeria

Research Paper

Volume 15, Issue 1, February 2023, ISSN 1936-0282

Funmilola Olubunmi Omotayo
Department of Data and Information Science
Faculty of Multidisciplinary Studies
University of Ibadan, Nigeria
lolaogunesan@yahoo.com

Joy Oluwabukola Olayiwola
Department of Computer Engineering
Federal Polytechnic, Ilaro, Nigeria
olu23_2022@yahoo.com

(*Received October 2021, accepted November 2022*)

ABSTRACT

The purpose of this paper is to investigate information privacy and security awareness among online social media (OSM) users in the Ibadan metropolis, Nigeria. Building upon the social exchange theory, some factors that could influence the disclosure of private information on social media were identified. Findings from the analysis of data of 255 respondents revealed that most were aware of information privacy and security measures available on OSM, and the risks associated with the disclosure of private information on OSM. Privacy and security awareness, the perception of benefits associated with the use of OSM, the perception of risks associated with the use of OSM, trust in the security of OSM, and the respondents' privacy and security self-efficacy influenced the disclosure of private information, while gender did not. Social media providers should provide more enlightenment on privacy settings available on the platforms to create more security and privacy consciousness.

Keywords

Information disclosure, online social media, privacy on social media, social exchange theory.

INTRODUCTION

The use of information communication and technology (ICT) for communication and interaction, and the increasing availability and affordability of internet-enabled devices brought innovations in online social media (OSM) and made it a popular medium for finding and interacting with new and old friends. Online social media are increasingly being used as platforms for communication, consolidating former relationships, staying in touch with contacts, reconnecting with old acquaintances, and creating new relationships with other people based on shared features such as hobbies, schools attended, interests, and religion, among others. The use of OSM has created an information technology culture that can be described as social networking culture or Internet culture.

With the advent of social networking, individuals voluntarily disclose personal information in various forms as the use of OSM requires users to create an account or profile in which users have to provide information such as names, gender, date of birth, home, workplace and email addresses, phone number, work experience, educational institutions attended, pictures, interests, religious affiliation, views, likes, and other socio-demographic information. While creating profiles, users are required to make some private information available. Some of this private information are mandatory, while some are voluntary because as users create their profiles, they have the option to make the profiles “private” or “public”. Most OSM offer users privacy settings to manage and control the privacy of their information. In most cases, users’ online profiles are available to the general public, while some can be restricted; that is, profile security settings can be “private” (i.e., limiting some or all profile information access to online friends approved by the profile owner), or “public” (i.e., allowing any user access to the profile). This means that privacy settings can limit access to some information of the user, or settings can be customized to limit access to certain profile viewers or particular sections of the profile. On Facebook and LinkedIn, for example, profile owners have the choice to protect their displayed information through profile security settings. Similar settings are available on Twitter and Telegram and some other ones; thus, users can choose whether or not their posted content is publicly available or not.

Along with the technological advancements brought by OSM, the significance of information security and privacy awareness is gaining recognition with increased risks associated with the use of this technology. As OSM user profiles provide a rich source of personal information, this is usually covered in the terms and conditions of service of the OSM. The information that is supplied or exchanged on these platforms is to be kept undisclosed and secure. Third-party applications connected to OSM can extract data from users without their knowledge and users are unaware of who controls these third-party applications, have no idea of how and where these data are stored, or for what purpose they use their information. Some service providers can track users’ online engagement using agents such as “cookies”. This makes personal data available to a wide audience and exposes users to privacy risks (Krasnova et al., 2010; Tan et al., 2012). Unauthorized access to personal data through third-party applications can create privacy risks, especially if the personal data are processed to reveal other more sensitive information about the users, such as name, gender, photographs, location, phone number, medical records, social security data, tax information, and personal preferences through various data-matching processes. Hence, while OSM provides users a platform to develop an online identity and social relationships, there can be some grave privacy concerns about user data. Privacy disclosure problems can arise on OSM as the user’s identity and data are closely linked and visible to a large audience (Beye et al., 2012). Reports have provided anecdotal evidence about risks and other damaging activities as a result of unauthorized access to users’ personal information supplied on OSM, such as financial fraud, cyberbullying, blackmail, and terrorism activity, carried out by unauthorized data-matching activities (Aldhafferi et al., 2013; Dwivedi et al., 2018).

As a result, individuals and organizations are increasingly given attention to security and privacy issue associated with OSM use. It has been found that, even though OSM provides information and privacy settings to safeguard users from falling vulnerable to unintended risks, many online social media users are still not aware and do not use the privacy settings that have been provided. Many OSM users do not realize that the provision of personal information on these public platforms puts them in danger of opening up to total strangers who can misuse their personal information for purposes like identity theft, embarrassment, blackmailing, and stalking, and can also cause physical harm. The dramatic rise in cyber-attacks reveals that social networks and millions of users have to do a lot more to protect themselves from hackers, spammers, identity fraudsters, etc. who prey on the information made available by social media users on their profiles and pages.

Information privacy and security are two important concepts that have drawn the attention of various scholars, especially on the need to protect the data of Internet users on social media. Privacy is the ability of individuals to determine how, when, to whom, and for what purposes any personal information will be divulged (Serenko & Fan, 2013). This means keeping people's personal information within its intended scope, and privacy is breached when the information is taken beyond its scope (Beye et al., 2012; Stutzman et al., 2012). Westin (1967) defines privacy as the claim of individuals, groups, or institutions to determine when, how, and to what extent, information about them is communicated to others. Privacy is also considered as the desire of an individual to enjoy autonomy, to be left alone, and to determine whether and how information about one's self is revealed to others (Stein & Sinha, 2002). Information privacy, therefore, is the ability to control who accesses, uses, and manipulates an individual's information or data that has been used for one or more purposes on the Internet. Consequently, for this study, OSM privacy is defined as a user's right to control the usage and distribution of his personal information.

Information security is the protection of information assets through the use of technology, processes, and training. As the popularity of OSM grows, users' data are at risk of security threats even in well-protected sites. In OSM, security threats are viewed as technical vulnerabilities of the network (Altshuler et al., 2013), such as insufficient authentication controls, cross-site scripting, cross-site request forgery, phishing, information leakage, injection flaws, information integrity, and insufficient anti-automation. Other security threats include virus attacks, identity theft, spam, scam, hacking, bullying, blackmail, embarrassment, and stalking, among others. Being ignorant about these risks could expose users to security threats and loss of privacy. In recent years, some academics have argued that in a networked world, information privacy and security are no longer under the control of individuals but rest with the organizations that hold the information (Conger et al., 2013).

However, studies (e.g., Magolis & Briggs 2016; Potter, 2014) have noted that public awareness of information privacy and security on OSM is very low, as many users do not bother to read the privacy information provided by these sites. Acquisti and Gross (2006) explained that even though OSM users are not forced to join an online social network, most OSM encourage but do not force users to reveal personal information. It is noted that despite existing privacy and security issues associated with social networking, people continue to reveal massive amounts of personal information on OSM. Many studies (e.g., Hugl, 2011; Koohang et al., 2018a; Richey et al., 2018) have shown that, despite the awareness of information privacy and security threats associated with the disclosure of private information on OSM, users continue to reveal their personal information. Magolis and Briggs (2016), Taddei and Contena (2013), and Taddicken (2013) also found that, despite pronounced privacy concerns associated with OSM, people still share intimate details of their lives on the platforms. For instance, Magolis and Briggs (2016) found that the participants in their study who were worried about their privacy being violated by someone physically locating them still felt comfortable sharing their personal information. This made the researchers wonder whether OSM users are aware of these threats. Do users of OSM value their security and privacy? Or do they have strategies they employ to overcome these issues? And do factors exist that affect the disclosure of personal information on OSM?

A review of the literature showed sparse studies that have investigated the level of awareness of information privacy and security by OSM users, while no known study was found to have investigated this in Nigeria. A preliminary investigation conducted among some social media users outside the scope of this study revealed that many were not aware of the security and privacy policies of OSM. Many were not aware of the risks associated with the disclosure of private information on OSM and even the security threats they face while using OSM. Investigation of the profile pages of some OSM users also revealed the nature, amount, and detail of personal information users provide on their profiles, which is worrisome. It is against this background that the study was designed to investigate the information privacy and security awareness of social media users in the Ibadan metropolis, Nigeria, as well as the factors influencing the disclosure of personal information on OSM. The study investigated the types of OSM used, the types of personal information users made available on OSM, the various information privacy and security threats users are exposed to, the methods or strategies adopted or used to protect their privacy and security, and the factors influencing disclosure of private information on OSM.

LITERATURE REVIEW

Social media encourage people to disclose personal information via profiles and posts, which has made personal information handling and self-disclosure through social networking media areas of major concern. A significant concern in the press and academic literature has been about OSM vendors' or providers' collection of the data of individual users, particularly the use of OSM for data harvesting of users' personal information. Recent studies have explored the factors that influence users to reveal their personal information to other users, that is, self-disclosure (Benson et al., 2015; Ostendorf et al., 2020; Zhang, 2015). Whilst overall, self-disclosure is seen as positive and beneficial in interpersonal communication and relationships (Lowry et al., 2011; Liu et al., 2022) research shows that many factors could influence self-disclosure of private information on SM.

Several studies have identified some of the factors that could influence the disclosure of information on online platforms: level of knowledge about private information (Correia & Compeau, 2017; Edwards, 2015), privacy and security awareness (Benson et al., 2015; Correia & Compeau, 2017; Malik, et al., 2016a; McGuinness & Simon, 2018; Warner, & Wang, 2019), social capital (Ellison et al., 2011; Stutzman et al., 2012, identity presentation **(**Stutzman, 2006); perception of benefits (Cheung et al., 2015; Elmi et al., 2013; Krasnova et al., 2010; Richey et al., 2018), and perceived risks (Beldad et al., 2011; Cheung et al., 2015; Elmi et al., 2013). Some other factors are perceived control (Beldad et al., 2011; Krasnova et al. 2010; Taddei & Contena, 2013), trust (Beldad et al., 2010; Cheung et al., 2015; Elmi et al., 2013; Gurung & Raja, 2016; Malik et al., 2016a) identity formation (Van Dijk, 2012) habits (Lankton et al., 2012), social interaction and identity (Ghamari & Mellbin, 2015; Joinson & Paine, 2007), enjoyment (Elmi et al., 2013; Krasnova et al., 2010), and socio-demographic factors such as gender (Baddeley, 2011; Thelwall, 2008; Tufekci, 2008; Weinberger et al., 2017), age (Rideout et al., 2010; Taddicken, 2013); cultural background (Cong, 2007) and Internet experiences (Yao & Zhang, 2008), among others.

These studies have also used different theories to investigate the disclosure of private information on social media platforms. Prior studies (e.g., Cheung et al., 2015; Zhang et al., 2019) about self-disclosure in social networking sites have mostly applied the Social Exchange Theory (SET) to explain why users are willing to disclose personal information on social networking sites (Krasnova et al., 2010). In other words, previous studies have mainly focused on how perceived cost and perceived benefits affect self-disclosure on social networking sites. However, it is believed that trust is an important element for the success of any website, social media or not, as it is necessary to have highly secure and easily manageable privacy settings in OSM that can guarantee user privacy and security. Likewise, the level of awareness of users about privacy and security threats (Malik et al., 2016a; McGuinness & Simon, 2018; Warner & Wang, 2019) and self-efficacy of users could influence the disclosure of information on OSM (Hocevar et al., 2014; Weinberger & Zhitomirsky-Geffet, 2017). Moreover, the relative influence of privacy and security awareness, perceived benefit, perceived risk, trust and privacy, and security self-efficacy on disclosure of private information on OSM has not been tested under a single study. To this end, the current investigation endeavors to shed light on the influence of these variables on the disclosure of private information on OSM. Extant literature was synthesized to advance a research model that posits that these variables could influence the disclosure of private information on OSM. This study contributes to the extant literature in two ways: to consolidate antecedents of disclosure of private information on OSM within a single study, and to empirically investigate the relative influence of privacy and security awareness, perceived benefit, perceived risk, trust and privacy, and security self-efficacy on disclosure of private information on OSM; particularly, some hypotheses were formulated.

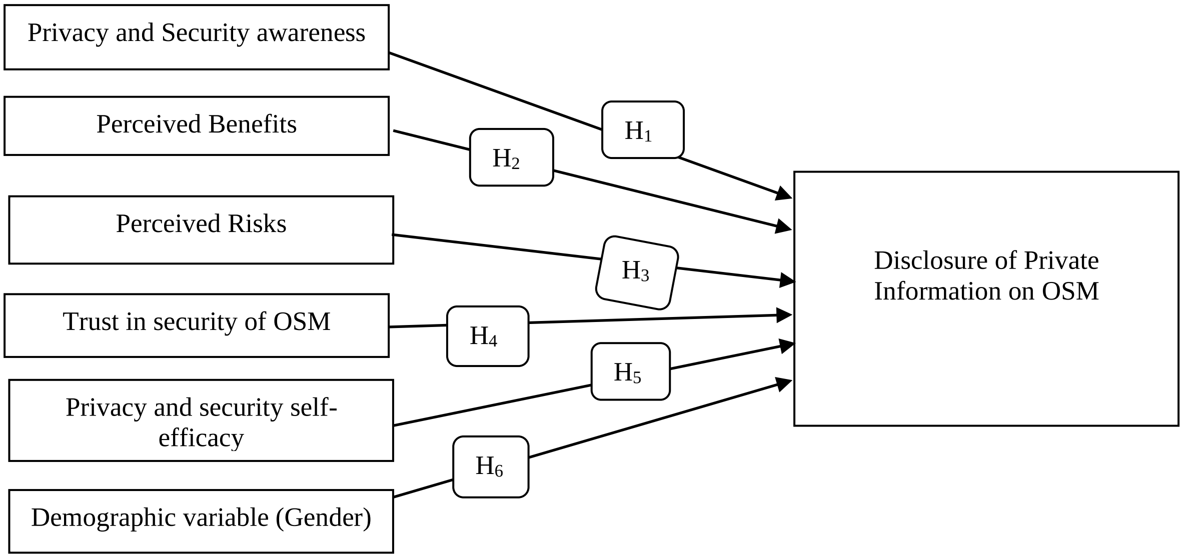
RESEARCH FRAMEWORK AND HYPOTHESES

The Social Exchange Theory (SET) and the Self Efficacy Theory (Bandura, 1977) provided the framework for the study. The SET was introduced in the works of Homans (1958) and Blau (1964). The SET explains that individuals engage in a behavior because of the perception of the benefits that may result from such behavior. It explains that humans weigh each relationship and interaction with another human on a reward cost scale without realizing it (Homans). If the interaction was satisfactory, then that person or relationship is looked upon favorably, but if unsatisfactory, then the relationship will be evaluated for its costs compared to its rewards or benefits. All social behavior is based on each actor's subjective assessment of the cost-benefit of contributing to a social exchange; hence, individuals engage in behaviors they find rewarding and avoid behaviors that have too high a cost. The theory also explains that social exchange involves trust, reciprocity, and cooperation which is associated with positive development outcomes (Beard, 2005). The theory assumes that perceived benefit, perceived risk, and trust drive relationship decisions. Perceived benefits are the elements of a relationship that have positive value, which can be a sense of acceptance, support, companionship, etc. Perceived risks are the elements of relational life that have negative value to a person, such as the effort put into a relationship and the negatives of a partner (West & Turner, 2007). Trust is the amount of control that an individual has in a relationship (Koohang et al., 2021). This study adopted three variables (perceived benefits, perceived risk, and trust) from the SET.

Self-efficacy refers to an individual's belief in his or her capacity to execute behaviors necessary to produce specific performance attainments (Bandura, 1977). It is explained as the judgment of one's ability to accomplish a particular job or task or succeed in a particular situation. Psychologist Albert Bandura described these beliefs as determinants of how people think, behave, and feel. Self-efficacy reflects confidence in the ability to exert control over one's motivation, behavior, and social environment. These cognitive self-evaluations influence all manner of human experience, including the goals for which people strive, the amount of energy expended toward goal achievement, and the likelihood of attaining particular levels of behavioral performance. Unlike traditional psychological constructs, self-efficacy beliefs are hypothesized to vary depending on the domain of functioning and circumstances surrounding the occurrence of behavior (Doménech-Betoret et al., 2017). Every individual can identify goals he/she wants to accomplish, and things he/she would like to change, or achieve. However, most people realize that putting these plans into action is not quite so simple. Bandura (1977) found that an individual's self-efficacy plays a major role in how goals, tasks, and challenges are approached. A strong sense of efficacy enhances human well-being; for instance, self-efficacy beliefs could influence the amount of stress and anxiety that people experience as they engage in an activity, e.g., using a technology. It is found that people with a strong sense of self-efficacy develop a deeper interest in the activities in which they participate, form a stronger sense of commitment to their interests and activities, recover quickly from setbacks and disappointments, and view challenging problems as tasks to be mastered. However, people with a weak sense of self-efficacy avoid challenging tasks, believe that difficult tasks and situations are beyond their capabilities, focus on personal failings and negative outcomes, and quickly lose confidence in personal abilities. For this study, OSM privacy and security self-efficacy are included as a variable that could influence the disclosure of private information on OSM. Privacy and security self-efficacy, in this case, refers to the attitudes, abilities, and cognitive skills of OSM users and the confidence in the ability to exert control over their motivation to use OSM and their behaviors, while using OSM, which is a social environment. The conceptual model, shown in Figure 1 hypothesized that disclosure of private information on OSM could be influenced by privacy and security awareness, the perceived benefit associated with the use of OSM, the perceived risk associated with the use of OSM, trust in the security of OSM, and privacy and security self-efficacy of users.

Figure 1

The Research Framework


Privacy and Security awareness
Perceived Benefits
Perceived Risks
Trust in security of OSM
Privacy and security self-efficacy
Demographic variable (Gender)
H1
H2
H3
H4
H5
H6
Disclosure of Private Information on OSM

Note: OSM = online social media

Privacy And Security Awareness and Disclosure of Private Information on OSM

Awareness is defined as being well-informed about a particular situation or development (Correia & Compeau, 2017). In information privacy and security research, this can be a daunting task since being well-informed about a particular situation may include the need for an understanding of the technology, policies, regulations, and/or common practices used to obtain private data. Privacy and security awareness of OSM users means having knowledge of good security practices and knowing the importance of protecting personal information while using OSM (Koohang et al., 2018b; Koohang et al., 2021; Yerby, et al., 2019). It is the knowledge of OSM users about private information provided on OSM, and how OSM can store private information for a long period that increases the ability to collect, store, analyze and share private information without authorization from OSM users. Previous research has shown that increased security awareness encourages users to perform good security behavior (Tomy & Pardede, 2016; Yerby et al., 2019). The degree of understanding of users about the importance of information security and their responsibilities to act to and exercise sufficient levels of information security control is crucial when using OSM. Al Abri et al. (2009) found that privacy awareness influenced users' privacy risk concerns, while Kuo and Talley (2014) found a positive association between awareness and SNSs users' information privacy concerns. The studies of Benson et al. (2015) and Malik et al. (2016b) also found significant relationships between awareness of users and disclosure of private information on OSM. Several other studies have also shown, to some extent, that security awareness may affect a person's intent to practice good security behavior (Furnell et al. 2007; North et al., 2010). However, less is known about disclosure and the role of the Ibadan metropolis OSM users' awareness of privacy and security concerns, particularly when there is strong criticism regarding the use of individual data by social media sites for surveillance, targeted advertising, profiling, and so on. Hence, we assumed, in this study, that the awareness of OSM users about privacy and security on OSM could influence their disclosure of personal information on OSM; hence, the first hypothesis was proposed:

H1: There is a significant relationship between privacy and security awareness and disclosure of private information on OSM.

Perceived Benefits of OSM And Disclosure of Private Information on OSM

Perceived benefit is the elements of a relationship that have positive value. Several types of perceived benefits have been identified in prior literature as being associated with the use of social networking sites: the convenience of maintaining existing relationships, new relationship building, self-presentation, and enjoyment (Cheung et al., 2011; Krasnova et al., 2010; Ying et al., 2021). Various forms of benefits have also been confirmed to affect information disclosure; for example, social ties, reciprocation (Krasnova et al., 2010); enjoyment (Elmi et al., 2013; Krasnova et al., 2009) displaying social capital to look important or popular (Christofides et al., 2009) timesaving or convenience (Hui et al., 2006) among other benefits. Scholars have tried to understand why people go online and disclose such huge amounts of personal information with no obvious benefit (Krasnova et al., 2010). Some of the findings have shown the perceived benefit that users feel they are gaining through their information disclosure (Ellison et al., 2011; Li et al., 2016) is one of the reasons. Though benefits in this regard are quite difficult to quantify, there is a common view among researchers that OSM users are disclosing information online due to a perceived benefit (Cheung et al., 2015; Richey et al., 2018). For instance, social validation or self-expression may be perceived benefits, which may encourage a user to disclose private information on social media (Bazarova & Choi, 2014; Yerby et al., 2019). Cheung et al. (2015) examined the relative impacts of perceived cost, perceived benefits, and social influence on self-disclosure behaviors on social networking sites. The results indicate that perceived benefits exhibited the strongest effect on self-disclosure on social networking sites. Social media helps preserve current social ties and new connections and provides an opportunity for people to share their opinions, ideas, and common interests, and build up new relationships. Hence, it is assumed that the perception of benefits associated with the use of OSM could make users disclose personal information on the platform; hence, it was proposed that:

H2: There is a significant relationship between users' perceived benefits associated with the use of online OSM and the disclosure of private information on OSM.

Perceived Risks Associated with OSM Use and Disclosure of Private Information on OSM

Risk is an elusive concept based on the notion of uncertainty sometimes expressed in terms of the probability of an adverse event occurring. Risk refers to "uncertainty about and severity of the events and consequences (or outcomes) of an activity concerning something that humans value" (Aven &Renn, 2009, p. 2). Commonly used definitions of risk as "a situation involving exposure to danger" or "the possibility that something unpleasant or unwelcome will happen" are not very specific and need to be pinned down (Pearsall & Hanks, 1999, p. 1602). Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence (Mulisa & Getahun, 2018). It is more widely understood to be an event with a negative outcome, in other words, a threat. Risk is usually defined as the "probability of a particular event (or hazard) occurring and the consequent severity of the impact of that event" (Baldwin et al., 2012, p. 82). Risks related to information disclosure are many and depend on the amount and type of information that is disclosed (Beldad et al., 2011; Dwivedi et al., 2018; Koohang et al., 2021; Yerby, et al. (2019). Users of OSM are prone to many risks associated with Internet use. The perception of risks associated with OSM use could influence the disclosure of private information on OSM, which could make users cautious about accepting friend requests from strangers (Li et al., 2016). Kuo and Talley (2014) for instance, found a positive relationship between SNSs users' privacy concerns and their risk perceptions; therefore, we also assumed a relationship between perceived risk and disclosure of private information on OSM. Another hypothesis was proposed:

H3: There is a significant relationship between users' perception of risk associated with the use of OSM and the disclosure of private information on OSM.

Trust in Security of OSM and Disclosure of Private Information on OSM

Trust may be defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (Mayer et al., 1995, p. 712). Trust is a key component of the social exchange theory by Homans (1958) which is related to the amount of control that an individual has in a relationship (Heath & Bryant, 2013). Mayer et al. (1995) defined trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 712). It is the degree to which online users believe their personal information is protected (Gefen et al., 2003). Trusting beliefs include four elements, i.e., benevolence, honesty, competence, and predictability (Salo & Karjaluoto, 2007). Trust is closely associated with users' willingness to disclose personal information in online settings and could be built based on users' positive experiences (Nuñez-Gonzalez, et al., 2015). The presence of trust is critical to the success of online interaction (Alzaidi & Agag, 2022) as engaging in online social exchanges creates a pattern of trust that facilitates the development of close relationships. Several studies (e.g., Koohang et al., 2018b; Koohang et al., 2021), of interpersonal exchange situations, have confirmed that trust is a precondition for self-disclosure because it reduces the perceived risks involved in revealing private information. Studies, (e.g., Dhagarra et al. 2020; James et al., 2017) express that trust and privacy concerns are direct predictors of users' behavior to accept and use OSM and disclose information. Gurung and Raja (2016) and Krasnova et al. (2010) found that trust helps to mitigate any concerns that platform users may have, ultimately leading to greater disclosure. When users believe that the OSM platform has sufficient safeguards, they may be more comfortable and have a stronger intention to share information with others on that platform (Wu & Sukoco, 2010). Thus, we proposed that:

H4: There is a significant relationship between the trust of users in the security of OSM and the disclosure of private information.

OSM Privacy and Security Self-Efficacy and Disclosure of Private Information on OSM

Self-efficacy has been a popular and important construct in information system research and a key concept in social cognitive theory that has been found relevant in many information technology research settings. Just like computer self-efficacy, OSM privacy and security self-efficacy reflect users' beliefs in their abilities to organize and execute the courses of action needed to have control over the type of information they disclose and share on OSM; that is users' capabilities to protect private information from unauthorized disclosure, modification, loss, destruction, and usage. Bandura (1997) has shown that observing others' performance and receiving feedback from others contribute to perceived self-efficacy within a domain, which is related to performance across a host of contexts due to elevated judgments of one's abilities. Foregrounding on Bandura's (1977, 1997) self-efficacy theory to conceptualize self-efficacy in the domain of online social media in the form of online social media privacy and security self-efficacy, we define OSM privacy and security self-efficacy as a user's beliefs about his or her capabilities to perform desired functions specifically in the online social media environment. We apply OSM privacy and security self-efficacy to examine the degree to which this variable influences the disclosure of private information on OSM. Some studies have reported various findings concerning the influence of self-efficacy on disclosure. For instance, Youn (2009) developed a conceptual framework for understanding young adolescents' privacy concerns and found that privacy and security self-efficacy are one of the factors that determine the levels of online privacy concerns. Weinberger and Zhitomirsky-Geffet (2017) also found that factors, such as users' concern for personal information protection on the Internet and users' privacy self-efficacy were among the strongest predictive factors of online privacy literacy and disclosure. It is, then assumed that users who are more confident and have high self-efficacy will be able to control and monitor the information they disclose on OSM; hence, the level of OSM privacy and security self-efficacy of the users could influence their disclosure of private information; hence, it was proposed that:

H5: There is a significant relationship between privacy and security self-efficacy of users and disclosure of private information on OSM.

Demographic Variable (Gender) and Disclosure of Private Information on OSM

Previous research studies (e.g., Alnjadat et al., 2019; Aparicio-Martínez et al., 2020; Karatsoli and Nathanail, 2020) widely reported gender differences in social media usage. According to the report published by the Statista Research Department on September 28, 2021, 78 percent of adult women and 65 percent of adult men used social networking sites in the United States as of February 2019. Gender has also been found to influence information disclosure on OSM by some studies, e.g., Aljohani et al. (2016), Li et al., (2015), Yao and Zhang (2008), Thelwall (2008), and Zukowski and Brown (2007). For instance, Aljohani et al. (2016) found that gender plays a role in personal information disclosure with males more likely to disclose personal information than females. Zukowski and Brown (2007) also found that certain user demographic factors, such as age, education, and income level influenced Internet users' information privacy concerns, while other factors such as gender and Internet experience had no influence. In this study, we assumed that the gender of OSM users could influence information disclosure; thus, another hypothesis was proposed:

H6: There is a significant difference between the gender of civil servants and the disclosure of private information on OSM.

METHODOLOGY

The study adopted the descriptive survey research design. The location of the study is the Ibadan metropolis. Ibadan is the capital and most populous city of Oyo State, in Nigeria. It is the third-largest city by population in Nigeria after Lagos and Kano, with a total population of 3,649,000 as of 2021, and over 6 million people within its metropolitan area. Ibadan is ranked the second fastest growing city on the African continent according to the UN Human settlements research program (Oluwole, 2022). The Ibadan metropolis was selected because of its familiarity with the researcher. Also, the selection of all the local government areas under the Ibadan metropolis is established on the fact that all of them cut across all the residential zones in the metropolis and they all spatially converge at the center of the city. The population of the study comprised civil servants in the Ibadan metropolis, Nigeria. The selection of the civil servants is premised on the fact that most are literate and users of OSM. The population of civil servants in the Ibadan metropolis, who use online social media, is unknown; therefore, convenience and accidental sampling techniques were used to select the respondents. Using the formula provided by Rose et al. (2015), $n = 3pq/d^{2,}$ where n = sample size of an unknown population since the researcher does not know the population of civil servants to be used in the Ibadan metropolis; p = 0.5; q = 1 – p (which is also 0.5); and d = 0.05, which is the error margin set for the study. This error margin covers the probability of error in the study and in the selection showing that to an extent, the study is 95% error-free and has an error probability of 5%.

Thus, applying the formula,

$$n = \frac{3 \times 0.5 \times 0.5}{0.05^2}$$

$$= \frac{0.75}{0.0025} = 300$$

Thus, by this formula, 300 civil servants were selected by convenience sampling technique across the five local government areas in the Ibadan metropolis. A questionnaire was used for data collection. The questionnaire was designed to ensure that information and data obtained are relevant to the objectives and research question. The questionnaire is divided into six sections. Section A collected data on the users' demographics, section B collected data on the types of social media the respondents were using, while section C collected data on the types of personal information made available by the respondents on OSM. Section D collected data about the respondent's perceptions of exposure to privacy and security threats on OSM; section E collected data about users' level of awareness of information privacy and security on OSM; section F collected data about methods and strategies used by OSM users; section G collected data about factors influencing disclosure of private information, while section H collected data about disclosure of private information. The items were measured on four Likert scales, ranging from Strongly disagree as 1 to Strongly Agree as 4. The instrument was structured by the constructs embedded in the aims, objectives, and research questions to ensure the validity of the research instruments. In addition, the instrument was given to two researchers for suggestions and modifications. Comments and suggestions provided were incorporated in the final copy of the questionnaire.

A pilot study was also carried out to ensure that the instrument is reliable. The instrument was administered to 20 individuals from Ido local government, which is not in the Ibadan metropolis. The internal consistency was determined by the use of Cronbach's alpha. The results, as shown in Table 1 show that the constructs are reliable as all coefficients are above 0.70, which is considered a good threshold for construct reliability (George & Mallery, 2003).

Table 1

Cronbach's Alpha Coefficients for Internal Consistency Reliability for the Scales

Variables	Cronbach's alpha reliability coefficients	No. of items
Privacy and security awareness	0.759	3
Perceived benefits	0 .751	4
Perceived risks	0.898	7
Trust in the security of OSM	0.825	4
Privacy and security self-efficacy	0.878	3
Disclosure of private information	0.871	7

Note. OSM = online social media.

Three hundred copies of the questionnaire were administered, while two hundred and fifty-five (255) were returned, completed, and usable for data analysis, which represents an 85.0% response rate. The data was collected primarily by the researchers with the help of a research assistant. The research assistant was well briefed and orientated on the content of the questionnaire and what is expected of the respondents. The respondents were appealed to complete the questionnaire immediately; where this was not possible, the researchers and the assistant arranged how and when to collect the questionnaire. The purpose of the study was well explained to the respondents to make them understand the purpose of the study and were properly informed that their participation was voluntary, and that the questionnaire would be used for research purposes only. Their informed consent was sought before allowing them to fill out the questionnaire; hence, only respondents that were willing to participate in the study were involved. The anonymity and confidentiality of information provided were ensured as the responses could not be traced to an individual. Data were analyzed quantitatively using descriptive analysis (frequency and percentage), while inferential statistics (Pearson correlation) was used to test the hypotheses at a 0.05 level of significance.

RESULTS

Demographic Information of the Respondents

The frequency counts and percentages of the respondents' demographics are presented in Table2.

Table 2

Demographic Variables of the Respondents

Variables	Measurement	Frequency (*N*=255)	Percentage
Sex	Male	156	61.2
	Female	99	38.8
Age	Less than 20	2	0.8
	20 – 25	9	3.5
	26 – 30	44	17.3
	31 – 35	43	16.9
	36 – 40	50	19.6
	41- 45	45	17.6
	46 – 50	34	13.3
	Above 50	28	11.0

Variables	Measurement	Frequency (*N*=255)	Percentage
Highest Educational Qualification	SSCE/ O' level	14	5.5
	OND / NCE	41	16.1
	HND/Bachelor	135	52.9
	Masters	56	22.0
	PhD	9	3.5
Place of Work	Local government	87	34.1
	State government	134	52.6
	Federal government	34	13.3
Level at Work	1 – 3	8	3.1
	4 – 6	54	21.2
	7 – 9	113	44.3
	10 – 12	61	23.9
	13 – 15	16	6.3
	Above 16	3	1.2

Note. SSCE = Secondary School Certificate, O' level = Ordinary level certificate, OND = Ordinary National Diploma, NCE = National Certificate of Education, HND= Higher National Diploma, PhD = Doctor of Philosophy

About 61.0% of the respondents were males, while about 39.0% were females. Most were within the age range 36-40 ((19.6%) Most had a first degree/Higher level Diploma certificates. Most were also state civil government employees (52.6%), with a majority on grade levels 7-9 (44.3%).

Types of OSM used by OSM users in the Ibadan metropolis

Table 3 shows that WhatsApp (91.8%), Facebook (74.5%), Facebook Messenger (58.8%), YouTube (48.6%), Yahoo messenger (44.3%) and Google+ (41.6%) were the most frequently used OSM. The table shows that WhatsApp had the highest mean (2.63), while Tumblr had the lowest (1.11).

Table 3

Types of Online Social Media Used

Types of OSM	Frequently Used (freq/%)	Occasionally Used (freq/%)	Never Used (freq/%)	*M*	*SD*
WhatsApp	234 (91.8)	13 (5.1)	8 (3.1)	2.63	0.680
Facebook	190 (74.5)	49 (19.2)	16 (6.3)	2.62	0.646
Facebook Messenger	150 (58.8)	64 (25.1)	41 (16.1)	2.61	0.672
YouTube	124 (48.6)	72 (28.2)	59 (23.1)	2.55	0.702
Google+	68 (26.7)	84 (32.9)	103 (40.4)	2.51	0.731
Yahoo Messenger	113 (44.3)	62 (24.3)	80 (31.4)	2.44	0.755
iTunes	36 (14.1)	52(20.4)	167 (65.5)	2.43	0.755
Twitter	78 (30.6)	79 (31.0)	98 (38.4)	2.36	0.755
Imo	51 (20.0)	87 (34.1)	117 (45.9)	2.34	0.831
Instagram	98 (38.4)	74 (29.0)	83 (32.5)	2.26	0.771
WeChat	59 (23.1)	50 (19.6)	146 (57.3)	2.14	0.809
Skype	43 (16.9)	77 (30.2)	135 (52.9)	2.08	0.829
LinkedIn	41 (16.1)	62 (24.3)	152 (59.6)	1.87	0.862

Types of OSM	Frequently Used (freq/%)	Occasionally Used (freq/%)	Never Used (freq/%)	*M*	*SD*
Bloggers	31 (12.2)	54 (21.2)	170 (66.7)	1.75	0.809
Pinterest	27 (10.6)	45 (17.6)	183 (71.8)	1.57	0.754
Flickr	23 (9.0)	50 (19.6)	182 (71.4)	1.32	0.586
Tumblr	29 (11.4)	37 (14.5)	189 (74.1)	1.11	0.405

Note. OSM = online social media.

Types of Personal Information Civil Servants Make Available on OSM

Table 4 shows the responses of the civil servants concerning personal information they make available on OSM. Information about gender was mostly disclosed (83.9%), while “emotions” were the least disclosed (33.3%).

Table 4

Type of Personal Information made Available on OSM

Personal information disclosed on OSM	Yes (frequency/%)	No (frequency/%)
Gender	214 (83.9)	41 (16.1)
Religion	209 (82.0)	45 (17.6)
Phone number(s)	210 (82.4)	45 (17.6)
Pictures	202 (79.2)	53 (20.8)
Email addresses/other social networks sites	199 (78.0)	56 (22.0)
Friend list	188 (73.7)	67 (26.3)
Home town	184 (72.2)	71 (27.8)
Date of birth	180 (70.6)	75 (29.4)
Videos	171 (67.1)	84 (32.9)
Favorites	162 (63.5)	93 (36.5)
Relationship status	164 (64.3)	91 (35.7)
Type or place of work	158 (62.0)	97 (38.0)
Hobbies/interest	154 (60.4)	101 (39.6)
Educational Qualifications	148 (58.0)	107 (42.0)
Groups you are following	145 (56.9)	110 (43.1)
Picture and Post Tags	143 (56.1)	112 (43.9)
Current contact address	136 (53.3)	119 (46.7)
Current postal address	120 (47.1)	135 (52.9)
Calendar/schedules	111 (43.5)	144 (56.5)
List of Jobs	102 (40.0)	153 (60.0)
Emotions	85 (33.3)	170 (66.7)

Note. OSM = online social media.

Information Privacy and Security Threats OSM Users are Exposed to

The various information privacy and security threats social media users are exposed to are presented in Table 5. Exposure to Viruses/worms/Trojans was the most ranked (62.7%,), while "posts of malicious content" was the least (51.0%).

Table 5

Privacy and Security Threats on Social Media

Threats	High (frequency/%)	Low (frequency/%)
Malware	160 (62.7)	95 (37.3)
Spams	156 (61.2)	99 (38.8)
Loss of personal data	149 (58.4)	106 (41.6)
Phishing	140 (54.9)	115 (45.1)
Negative post	140 (54.9)	115 (45.1)
Abuse of information posted	135 (52.9)	120 (47.1)
Unintended disclosure of information	134 (52.5)	121 (47.5)
Cross-site profile cloning	133 (52.2)	122 (47.8)
Identity theft/profile cloning	129 (50.6)	126 (49.4)
Posts of malicious content	130 (51.0)	125 (49.0)

Methods or Strategies OSM Users adopt to Protect their Privacy and Security

As shown in Table 6, among the technical/hardware strategies used by the civil servants, "using personal devices to log in" was rated highest (94.4%), while "updating of antivirus" was the highest among the software strategies (94.9%). The users also rated "follow-up change in the privacy policy" highest (94.1%) among the options provided for platform strategies. The responses of the civil servants are all above average (above 50%), which indicates that they were aware of measures that could protect their privacy and security on OSM.

Table 6

Strategies Used for Privacy and Security Protection on OSM

Methods or strategies used	Used (frequency/%)	Not used (frequency/%)
Technical/hardware		
Use office devices to log in	162 (63.5)	93 (36.5)
Share my external devices with other	167 (65.5)	88 (34.5)
Use any available devices to log in	190 (74.5)	65 (25.5)
Use only my devices to log in	247 (94.4)	13 (5.1)
Software		
Use of firewall	205 (80.4)	50 (19.6)

Methods or strategies used	Used (frequency/%)	Not used (frequency/%)
Do security update	224 (87.8)	31 (12.2)
Check sites before use	228 (89.4)	27 (10.6)
Update from time to time	233 (91.4)	22 (8.6)
Install antivirus	237 (92.9)	18 (7.1)
Update antivirus	242 (94.9)	13 (5.1)
Platform		
Changed my security settings to privacy	229 (89.8)	26(10.2)
Read and follow the security policy	233 (91.4)	22 (8.6)
Aware of who can see my post	237 (92.9)	18 (7.1)
Follow-up change in the privacy policy	240 (94.1)	15 (5.9)
Attitude		
Share my password	136 (53.3)	119 (46.7)
Keep very important data like bank details	163 (63.9)	92 (36.1)
Post details of my movement	164 (64.3)	91 (25.7)
Use one password for many SNSs logins	172 (67.5)	83 (32.5)
Click posted on my wall	198 (77.6)	57 (22.4)
Click links sent by my known friends	211 (82.7)	44 (17.3)
Change my password	212 (83.1)	43 (16.9)
Careful of where I provide personal details	217 (83.1)	38 (14.9)
Use a very strong password	224 (87.8)	31 (12.2)
Cautious of whom I add as friend	245 (96.1)	10 (3.9)
Always trust all the discussions	247 (96.9)	8 (3.1)
Careful of what I share with friends online	248 (97.3)	7 (2.7)

Note. OSM = online social media.

Factors Influencing Disclosure of Private Information on OSM

The results of the test of the hypotheses reveal the factors that influence the disclosure of private information on OSM. The hypotheses were tested in null forms, assuming that no significant relationship exists between the concerned variables. The pre-set level of significance is 5%. When the *p*-value (the significance of the test) exceeded the pre-set level, the null hypothesis was not rejected. When the *p*-value was less than or equal to 0.05, the null hypothesis was rejected and the alternative hypothesis, which states that a significant relationship exists between the variables under consideration, was accepted.

Table 7

Pearson Correlation Results of the Test of Hypotheses 1 to 5

Independent Variables		Disclosure of private information (Dependent variable)
Privacy and security awareness	Pearson Correlation	0.388^{**}
	Sig. (2-tailed)	0.000
	N	255
Perceived benefits	Pearson Correlation	0.366^{**}

Independent Variables		Disclosure of private information (Dependent variable)
	Sig. (2-tailed)	0.000
	N	255
Perceived risks	Pearson Correlation	0.298**
	Sig. (2-tailed)	0.000
	N	255
Trust in the security of OSM	Pearson Correlation	0.408**
	Sig. (2-tailed)	0.000
	N	255
Privacy and security self-efficacy	Pearson Correlation	0.327**
	Sig. (2-tailed)	0.000
	N	255

Note. OSM = online social media. Sig. = Significant.
**Correlation is significant at the 0.01 level (2-tailed).

The results of the Pearson correlation in Table 7 show that all the variables (privacy and security awareness, perceived benefits associated with use of OSM, perceived risks associated with use of OSM, trust in security of OSM, and privacy and security self-efficacy of users) have positive and significant relationships (*p* < .05) with disclosure of private information on OSM. However, the strength of the correlation is weak (0.388; 0.366, 0.298, and 0.327 respectively), except for trust which is moderate (0.408). Hence, the null hypotheses are rejected.

In addition, Table 8 shows the results of the Mann-Whitney test for hypothesis 6. The results show no significant relationship *(p* = .946 < .05) between the gender of the civil servants and their disclosure of private information on OSM; hence null hypothesis 6 was not rejected.

Table 8

Mann-Whitney Test Results for Hypothesis 6

	Disclosure of private information
z	-0.068
Asymp. Sig. (2-tailed)	0.946
Mann-Whitney U	
a. Grouping Variable: Gender	

Note. Asymp. Sig. (2-tailed) = Asymptotic 2-sided significance.

DISCUSSION

The most frequently used social media by civil servants in the Ibadan metropolis were WhatsApp, Facebook, Facebook Messenger, YouTube, Yahoo messenger, and Google+, respectively. This finding is in agreement with the findings of Alabi (2018) who found that the most frequently used social media among IT workers in the University of Ibadan were Whatsapp, Facebook, Google+, YouTube, Instagram, Yahoo Messenger, and Twitter respectively. The finding is also in conformity with those of Alsobayel (2016), Barry and Pearson (2015), and Thomas and Laseinde (2015). The high usage of WhatsApp, Facebook, Facebook Messenger, Yahoo Messenger, YouTube, and Google+ can allude to the fact that most of them are now available and usable with hand-held ICT devices, such as phones and personal digital assistants (PDA). Also, the synchronous attributes of some of these platforms could influence their use among this category of users. Other synchronous platforms like Instagram were not highly used because of the demography of the users which is civil servants who may not be too impressed with the posting of pictures.

Most of the respondents provided various types of personal information on social media except emotions (sexual orientation, tune-on or tune-off), a list of jobs completed, and a calendar/schedule. This finding contradicts that of Aldhafferi et al. (2013) which found that users consider contact information, such as current address, physical address, phone number, and email address, as requiring more privacy protection than other pieces of personal information. Also, items such as favorite TV shows, books, and movies were not as important in terms of the need for privacy protection. Thus, the findings of this study indicate that contact information does not need privacy protection like other pieces of personal information to expect emotions that seem to be more private to them than any other personal information. Personal information that was provided highly may be considered less privacy and security threatened by the users.

The privacy threats the civil servants were exposed to are viruses, worms, trojans, posts of malicious content, disclosure of personal data, and negative posts; while the security threats are phishing, spam, malware, third-party application, and physical threats. These are related to the findings of previous studies, such as Abdulhamid et al. (2011), Franchi et al. (2014), Salleh et al. (2012), and Wang et al. (2013). The findings, however, show that the civil servants were aware of information privacy and security on OSM. This is contrary to the findings of Tuunkainen et al. (2009) who found that active users of Facebook disclosed a vast amount of private information because they were not aware of the visibility of their information to people that they did not necessarily know. Also, Slusky and Partow-Navid (2012) found that information security awareness was lower than the knowledge level of information security among their respondents. It could be that the level of education and the maturity of our respondents concerning age, contributed to their high level of privacy and security while using social media. Also, the increased sensitization of Nigeria’s mass media on the need for users to take caution while disclosing private information on social media may have contributed to our findings. The news of various vices in Nigeria in recent times is also another pointer to the fact that users are supposed to be careful and find out how to mitigate privacy and security breaches online.

It was discovered from the findings that the majority of the respondents used hardware, software, platform, and attitude strategies to protect their information on OSM. This means that the civil servants made use of different methods or techniques to protect or secure their private information on social media indicating that they are highly aware of the methods and strategies to protect their personal information. It has been established that using stronger authentication and access control and having a strong password can protect personal information. The strength of authentication is different from one site to another site. To provide a strong defense, the use of additional authentication factors, such as e-mail verification through CAPTCHAs, as well as the use of spam filters are advised to be used. Senthil et al. (2016) explained that in taking over the privacy concern of OSM by the users, a strongly enforced set of well-defined policies like using a strong password, awareness of changing passwords often, awareness of information disclosure, the purpose of antivirus or related software, and proprietary software, among others must be put in place. Most of the civil servants reported using their devices to avoid privacy and security breaches because most of them could afford the devices. Their use of software can be connected with the fact that their awareness of privacy and security threats is high and therefore try to find means of avoiding the breaches. The commonest and easiest means to secure OSM accounts is through the use of available free software which most of them indicated they used. There was reported low use of sharing of passwords, which means that they shared their passwords, maybe with their children or other co-workers in the office as some within the demography may not be able to operate the devices very well on their own.

OSM users' awareness is a vital issue in protecting users against risks and threats on social media. The test of hypotheses revealed that privacy and security awareness positively and significantly influenced the disclosure of private information by civil servants, even though the magnitude of the correlation is low. This shows that the civil servants were aware of privacy and security on social media. This could be because most of the civil servants are well educated. The level of their education with age and experience is expected to influence their awareness of privacy and security on online platforms. Our results support the findings of Benson et al. (2015), Koohang et al. (2021), Salleh et al. (2012), and Tomy and Pardede (2016). For instance, Benson et al. explored the antecedents of information disclosure of social media users. The results show that both user awareness and security notices had a positive statistical effect on the civil servants' information disclosure. Yerby, et al. (2019) found that social media awareness was a significant predictor of risk and that users must be trained on how to avoid identity theft and secure their personal information. Awareness must include educating users about the threats, risks, and methods to be safer (Van der Walt et al., 2018). Users that perceive themselves to be aware of the threats and policies of OSM would modify their behaviors when interacting with the social media platforms (Yerby et al.). However, the results of Alkeinay and Norwawi (2014) contradict this finding.

The results from the second hypothesis show a positive correlation and significant relationship between perceived benefit and disclosure of private information on OSM. This finding is related to the results of some previous studies such as Kuo and Talley (2014), Li et al. (2016), Mulisa and Getahun (2018), Salleh et al. (2012), and Ying et al., (2021), which found that users' perceived benefits increased the willingness to disclose private information on social networks. This means that the perceived benefits of using OSM influenced the civil servants to disclose private information, not minding the risks attached to it. The perception of the value of the benefits associated with OSM use may have a greater influence on the civil servants' judgment on whether to disclose personal information or not. This could far outweigh the experienced or expected risks that they could be exposed to. If the encountered or experienced risks are very small compared to exposed risks, it may still be an indicator that, in the face of the exposed risks, they can weather it successfully, so they may not see reasons why they should not disclose their information online.

It was also found that a low but positive correlation and significant relationship existed between perceived risk and disclosure of private information. The finding conforms with that of Li et al. (2016), Mulisa and Getahun (2018), Koohang et al., (2021), and Ying et al., (2021) which found that risks influenced behavior on OSM which also influenced the disclosure of private information. Li et al. for instance, found that perceived risks decreased users' willingness to disclose private information on social network sites. The desire of the users to be part of new online communities seems to negate the awareness of risk and threats of over-disclosure of information on OSM. However, the findings contradict that of Koehorst (2013) who reported that perceived risks did not have a significant influence on the disclosure of private information in their study. The civil servants, in this study, are literate and experienced; hence, this could have influenced their understanding of risks associated with the use of OSM and thus made them cautious of how they disclose private information on OSM.

Researchers have reported that trust in the security of OSM positively influences users' information disclosure (Alzaidi & Agag, 2022). Trust is the backbone for creating relationships on social media sites (Wang et al., 2021). The results from the fourth hypothesis show that there is a significant relationship between trust and disclosure of private information on OSM which is contrary to the findings of Kuo and Talley (2014) which found that users' privacy concerns did not have a significant effect on their trust in the use of SNSs. Koehorst (2013) also reported that trust did not have a significant effect on the disclosure of private information. Trust in terms of the security mechanisms put in place by the OSM will determine the level of private information to be disclosed (Beldad et al., 2011; Koohang et al., 2018; Koohang et al., 2021). However, the findings of this study are in line with Taddei and Contena (2013) who stated that users with a high level of trust were more comfortable with intimate topics and so they disclose more personal information. Ghamari and Mellbin (2015) reported that, though the users did not trust the owner of the platform since it is a private organization, they will still prefer to use it and give out their personal information. The findings of this study reveal that the respondents trust social media security to protect their information from a third party. The knowledge of computer security as a result of self-efficacy, together with the fact that the civil servants are in a good position to manage information, might have increased their trust level in OSM, which invariably made them disclose private information online.

The results from the fifth hypothesis show a significant relationship between OSM privacy and security self-efficacy and disclosure of private information. Hocevar et al. (2014) explained that users with higher social media self-efficacy found the information shared via social media to be more trustworthy than those with lower social media self-efficacy. The self-efficacious social media users also relied more both on the opinions of others and on social media specifically when evaluating or verifying information found online, suggesting that they might be more prone to seek out and be influenced by the opinions and suggestions from others. Users who assess themselves as being highly efficacious may tend to look for positive outcomes from social media use, while those exhibiting low self-efficacy may likely expect unfavorable outcomes in the disclosure of private information. The civil servants' knowledge about setting security features, updating, reading security terms, or installing anti-virus and other related means of circumventing risks could make them disclose information on OSM. Having the knowledge or having someone at home or in the office that can help them, coupled with their awareness about risks and threats online, may have provoked a conscious effort on their part to learn about OSM to be safe while using it. The benefits of using the online platforms might have been a catalyst for them to be computer efficacious which they now employ to ensure that it does not hinder them from disclosing information online. This means that the majority of the respondents were computer literate and they were aware of the privacy and security setting of the computer devices, therefore they can make use of the settings to either disclose or not disclose their personal information.

The analysis of the sixth hypothesis shows that there is no significant difference between the disclosure of private information by male and female civil servants. This contradicts the findings of Li et al. (2015) which found that males and females had significantly differentiated privacy disclosure patterns in dimensions related to the breadth and depth of disclosure of information on social network sites. It was also a deviation from the findings of Aljohani et al. (2016) and Karatsoli and Nathanail (2020), whose results indicated that the gender of their respondents played a role in personal information disclosure on social media.

CONCLUSION AND RECOMMENDATIONS

This study concluded that the civil servants in the Ibadan metropolis made use of various OSM and were exposed to various privacy and security threats such as viruses, worms, Trojans, phishing, spam, and malware. The civil servants used various controls and strategies available on the Internet to minimize their exposure to privacy and security threats. Privacy and security awareness, the perception of benefits associated with the use of OSM, the perception of risks associated with the use of OSM, trust in the security of OSM, and the civil servants’ privacy and security self-efficacy are the factors that influenced the disclosure of private information by them. Our results imply that OSM users require more cognitive awareness regarding their genres of disclosure and the effect of their disclosures on their private lives, because since the Internet and OSM provide an incredible array of interpersonal-communication options, users may be unaware of the hidden dangers lurking behind online friendships. With the increased use of social media and the enormous amount of private information shared on OSM, we recommend that it is expedient for OSM users to be aware of the risks involved in disclosing private information on the platforms as the lack of knowledge on information privacy and security has exposed many users of SM to serious threats. Efforts should be made by designers and developers of OSM to compel users to read privacy policies before creating online profiles, so they would know the dangers involved in disclosing private information and thereby help them exercise caution while disclosing personal information on OSM. OSM developers should also ensure to build effective security measures to safeguard users’ private information from hackers, spammers, and identity fraudsters. OSM users need to be increasingly made aware of the inherent risks involved when they disclose their personal information through these platforms and know that such information could be used unethically by some other individuals to perpetrate crimes.

LIMITATIONS AND SUGGESTIONS FOR FURTHER STUDIES

The study was restricted to civil servants in the Ibadan metropolis, which is a relatively small fraction of OSM users in Nigeria. Another limitation is the use of non-probabilistic techniques (convenience and accidental) for sample selection because of unavailable data on the population of civil servants who are OSM users. As a result, the extent to which the findings of this research can be generalized to the wider population is limited. However, it does provide insights into OSM users’ perceptions and responses about the disclosure of private information on OSM, which can contribute to developing understanding in this area, and which is the focus of this paper.

Future studies could investigate the disclosure of private information on OSM by other populations. This study could also be extended to other parts of Oyo State or other regions in the country. Future research may also use a qualitative approach to collect data on this subject, while some other variables could also be explored.

REFERENCES

Abdulhamid, S. M., Ahmad, S. Waziri, V. O., & Jibril, F. N. (2011). Privacy and national security issues in social networks: The challenges. *International Journal of Computer, The Internet and Management, 19*(3), 14–20.

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy Enhancing Technologies, 1–22. https://doi.org/10.1007/11957454_3

Alabi, O. O. (2018). *Use of social media by information technology workers in University of Ibadan, Oyo State.* [Unpublished master’s thesis]. University of Ibadan, Ibadan.

Al Abri, D., McGill, T., & Dixon, M. (2009). Examining the impact of e-privacy risk concerns on citizens’ intentions to use e-government services: *An Oman perspective. Journal of Information Privacy & Security, 5*(2), 3–26. https://doi.org/10.1080/15536548.2009.10855861

Aldhafferi, N., Watson, C., & Sajeev, A. S. (2013). Personal information privacy settings of online social networks and their suitability for mobile internet devices. *International Journal of Security, Privacy and Trust Management, 2*(2), 1–17. https://doi.org/10.5121/ijsptm.2013.2201.

Aljohani, M., Nisbet, A., & Blincoe, K. (2016). A survey of social media users' privacy settings and information disclosure. In M. Johnstone (Ed.), *Australian Information Security Management Conference* (pp. 67–75). Research Online Institutional Repository. https://doi.org/10.4225/75/58a693deee893

Alkeinay, N. Y., & Norwawi, N. M. (2014). User oriented privacy model for social networks. *Procedia of Social and Behavioral Sciences*, *129*(2014), 191–197. https://doi.org/10.1016/j.sbspro.2014.03.666

Alnjadat, R., Hmaidi, M. M., Samha, T. E, Kilani, M. M., & Hasswan, A. M. (2019). Gender variations in social media usage and academic performance among the students of University of Sharjah. *Journal of Taibah University Medical Sciences*, *14*(4),390–394. https://doi.org/10.1016/j.jtumed.2019.05.002.

Alsobayel, H. (2016). Use of social media for professional development by health care professionals: A cross-sectional web-based survey. *JMIR Medical Education*, *2*(2), 1–8. https://doi.org/10.2196/mededu.6232

Altshuler, Y., Elovici, Y., Cremers, A. B., Aharony, N., & Pentland, A. (2013). *Security and privacy in social networks*. Springer. https://doi.org/10.1007/978-1-4614-4139-7

Alzaidi, M. S., & Agag, G. (2022). The role of trust and privacy concerns in using social media for e-retail services: The moderating role of COVID-19. *Journal of Retailing and Consumer Services*, *68*, 1-13. https://doi.org/10.1016/j.jretconser.2022.103042

Aparicio-Martínez, P., Ruiz-Rubio, M., Perea-Moreno, A. -J., Martinez-Jiménez, M. P., Pagliari, C., Redel-Macías, M. D., & Vaquero-Abellán, M. (2020). Gender differences in the addiction to social networks in the southern Spanish university students. *Telematics and Informatics*, *46*(2020), 1-12, https://doi.org/10.1016/j.tele.2019.101304

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research*, *12*(1), 1–11. https://doi.org/10.1080/13669870802488883

Baddeley, M. (2011). A behavioural analysis of online privacy and security. *Cambridge Working Papers in Economics (CWPE),1147*, 1-26.

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, *84*(2), 191–215. https://doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1997). *Self-efficacy: The exercise of control*. Freeman and Company.

Barry, A. R., & Pearson, G. J. (2015). Professional use of social media by pharmacists. *Canadian Journal of Hospital and Pharmacy*, *68*(22), 22–27. https://doi.org/10.4212/cjhp.v68i1.1421

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication*, *64*, 635–657. https://doi.org/10.1111/jcom.12106

Beard, V. A. (2005). Individual determinants of participation in community development in Indonesia. *Environment and Planning C: Politics and Space*, *23*(1), 21–39. https://doi.org/10.1068/c36m

Beldad, A., De Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. *The Information Society*, *27*(4), 220–232. https://doi.org/10.1080/01972243.2011.583802

Benson, V., Saridakis, G., & Tennakoon, H. (2015). Information disclosure of social media users: Does control over personal information, user awareness and security notices matter? *Information Technology & People*, *28*(3), 426–441. https://doi.org/10.1108/ITP-10-2014-0232

Beye, M. Jeckmans, A. J. P., Erkin, Z., Hartel, P., Lagendijk, R. L., & Tang, Q. (2012). *Privacy in online social networks*. In A. Abraham (ed.). *Computational social networks*. Springer. https://doi.org/10.1007/978-1-4471-4051-1_4

Blau, P. M. (1964). *Exchange and power in social life*. Wiley.

Cheung, C., Lee, Z. W. Y., & Chan, T. K. H. (2015). Self-disclosure in social networking sites: The role of perceived cost, perceived benefits, and social influence. *Internet Research*, *25*(2), 279–299. https://doi.org/10.1108/IntR-09-2013-0192

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Were they two sides of the same coin or different processes? *Cyberpsychology and Behavior*, *12*(3), 341–345. https://doi.org/10.1089/cpb.2008.0226

Cong, L. (2007). Online chatter's self-marketing in cyberspace. *CyperPsychology and Behavior, 10*(1), 131–132. https://doi.org/10.1089/cpb.2006.9982

Conger, S., Pratt, J. H. & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401–417. https://doi.org/10.1111/j.1365-2575.2012.00402.x

Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): A review of the use, definition, and measurement of IPA. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 4021–4030). ScholarSpace. https://doi.org/10.24251/HICSS.2017.486

Debatin, B., Lovejoy, J. P., Horn, A. M. A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: An Indian perspective. *International Journal of Medical Informatics*, *141*, 1-13. https://doi.org/10.1016/j.ijmedinf.2020.104164

Doménech-Betoret, F., Abellán-Roselló, L., & Gómez-Artiga, A. (2017). Self-Efficacy, satisfaction, and academic achievement: The mediator role of students' expectancy-value beliefs. *Frontiers in Psychology, 8*, 1–12. https://doi.org/10.3389/fpsyg.2017.01193

Dwivedi, Y. K., Kelly, G., Jansen, M., Rana, N. P., Slade, E. L., & Clement, M. (2018). Social media: The good, the bad, and the ugly. *Information Systems Frontiers, 20*, 419–423. https://doi.org/10.1007/s10796-018-9848-5

Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer users* [Doctoral dissertation, Nova Southeastern University]. Nova Southeastern University ProQuest Dissertations Publishing. https://nsuworks.nova.edu/gscis_etd/947

Ellison, N. B., Vitak, J., Steinfield, C., Gray, R. & Lampe, C. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In S. Trepte, & L. Reinecke (Eds), *Privacy online* (pp. 19–32). Springer. https://doi.org/10.1007/978-3-642-21521-6_3

Elmi, A. H., Iahad, N. A., & Ahmed, A. A. (2013). Factors influence self-disclosure amount in social networking sites (SNSs). *Journal of Information Systems Research and Innovation*, *2*, 43–50. https://doi.org/10.1016/j.cose.2007.03.001

Franchi, E., Poggi, A., & Tomaiuolo, M. (2014). Information attacks on online social networks. *Journal of Information Technology Research 7*(3), 54–71. https://doi.org/10.4018/jitr.2014070104

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal internet users. *Computers & Security, 26*, 410-417. https://doi.org/10.1016/j.cose.2007.03.001

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51–90. https://doi.org/10.2307/30036519.

George, D., & Mallery, P. (2003). *SPSS for windows step by step: A simple guide and reference. 11.0 update* (4th ed.). Allyn & Bacon.

Ghamari, N., & Mellbin, L. (2015). Disclosing personal information to social networking site providers: The role of trust, risk and perceived benefits [Master's thesis, Uppsala University]. Diva Portal. http://urn.kb.se/resolve?urn=urn%3Anbn%3Ase%3Auu%3Adiva-255927

Gurung, A., & Raja, M. K. (2016). Online privacy and security concerns of consumer. *Information & Computer Security, 24*(4), 348–371. https://doi.org/10.1108/ICS-05-2015-0020

Hocevar, K. P., Flanagin, A. J., & Metzger, M. J. (2014). Social media self-efficacy and information evaluation online. *Computers in Human Behavior, 39*, 254–262. https://doi.org/10.1016/j.chb.2014.07.020

Homans, G. C. (1958). Social behavior as exchange. *American Journal of Sociology, 63,* 597-606. https://doi.org/10.1086/222355

Hugl, U. (2011). Reviewing person's value of privacy of online social networking. *Internet Research, 21*(4), 384–407. https://doi.org/10.1108/10662241111158290

Hui, K. L., Tan, B. C., & Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology*, *6*(4), 415–441. https://doi.org/10.1145/1183463.1183467

James, T. L., Wallace, L., Warkentin, M., Kim, B. C., & Collignon, S. E. (2017). Exposing others' information on online social networks (OSNs): Perceived shared risk, its determinants, and its influence on OSN privacy control use. *Information & Management, 54*(7), 851–865. https://doi.org/10.1016/j.im.2017.01.001

Joinson, A. N., & Paine, C. B. (2007). Self-disclosure, privacy and the internet. In A. N. Joinson, K. Y. A. McKenna, T. Postmes, & U. D. Reips (Eds.), *Oxford handbook of internet psychology* (pp. 237–252). Oxford University Press.

Karatsoli, M., & Nathanail, E. (2020). Examining gender differences of social media use for activity planning and travel choices. *European Transport Research Review, 12*, 44, 1–9. https://doi.org/10.1186/s12544-020-00436-4

Koehorst, R. H. G. (2013). Personal information disclosure on online social networks: An empirical study on the predictors of adolescences' disclosure of personal information on Facebook benefits [Master's thesis, University of Twente]. University of Twente Student Theses Repository. https://purl.utwente.nl/essays/63797

Koohang, A., Paliszkiewicz, J., & Goluchowski, J. (2018a). Social media privacy concerns: Trusting beliefs and risk beliefs. *Industrial Management & Data Systems, 118*(6), 1209–1228. https://doi.org/10.1108/IMDS-12-2017-0558

Koohang, A., Floyd, K., Rigole, N., & Paliszkiewicz, J. (2018b). Security policy and data protection awareness of mobile devices in relation to employees' trusting beliefs. *Online Journal of Applied Knowledge Management, 6*(2), 7–22. *https://doi.org/10.36965/OJAKM.2018.6(2)7-22*

Koohang, A., Floyd, K., Yerby, J. & Paliszkiewicz, J. (2021). Social media privacy concerns, security concerns, trust, and awareness: Empirical validation of an instrument. Issues in Information Systems, *22*(2), 133–145. https://doi.org/10.48009/2_iis_2021_136-149.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology, 25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Kuo, K., & Talley, P. C. (2014). An Empirical Investigation of the Privacy Concerns of Social Network Site Users in Taiwan. *Computing and Information Technology, 5*(2), 1–19.

Lankton, N. K., McKnight, D., & Thatcher, J. B. (2012). The moderating effects of privacy restrictiveness and experience on trusting beliefs and habit: An empirical test of intention to continue using a social networking website. *IEEE transactions on Engineering Management, 59*(4), 654–665. https://doi.org/10.1109/TEM.2011.2179048

Li, K., Lin, Z. & Wang, X. (2015). An empirical analysis of user's privacy disclosure behaviors on social networks sites. *Information and Management, 52*(7), 882–891. https://doi.org/10.1016/j.im.2015.07.006

Li, K., Wang, X., Li, K. & Che, J. (2016). Information privacy disclosure on social network sites: An empirical investigation from social exchange perspective. *Nankai Business Review International, 7*(3), 282–300. https://doi.org/10.1108/NBRI-02-2015-0005

Liu, Y., Tse, W.K., Kwok, P.Y. & Chiu, Y.H. (2022). Impact of social media behavior on privacy information security based on analytic hierarchy process. *Information, 13*, 280, 1–14. https://doi.org/10.3390/ info13060280

Lowry, P.B., Cao, J. & Everard, A. (2011). Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems, 27*(4), 163–200. https://doi.org/10.2753/MIS0742-1222270406

Magolis, D., & Briggs, A. (2016). A phenomenological investigation of social networking privacy awareness through a media literacy lens. *The National Association for Media Literacy Education's Journal of Media Literacy Education, 8*(2), 22–34. https://doi.org/10.23860/jmle-8-2-1

Malik, A., Hiekkanen, K., Dhir, A., & Nieminen, M. (2016a). Impact of privacy, trust and user activity on intentions to share Facebook photos. Journal of Information, *Communication and Ethics in Society, 14(*4), 364–382. https://doi.org/10.1108/JICES-06-2015-0022

Malik, A., Hiekkanen, K., Dhir, A., & Nieminen, M. (2016b). Privacy and trust in Facebook photo sharing: Age and gender differences. *Program, 50*(4), 462–480. https://doi.org/10.1108/PROG-02-2016-0012

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734. https://doi.org/10.2307/258792

McGuinness, D., & Simon, A. (2018). Information disclosure, privacy behaviors, and attitudes regarding employer surveillance of social networking sites. *International Federation of Library Associations and Institutions, 44*(3), 203–222. https://doi.org/10.1177/0340035218785389

Mulisa, F., & Getahun, D. A. (2018). Perceived benefits and risks of social media: Ethiopian secondary school students' perspectives. *Journal of Technology in Behavioral Science*, *3*(4), 294–300. https://doi.org/10.1007/s41347-018-0062-6

North, M., Perryman, D., Burns, S., & North, S. (2010). A comparative study of information security and ethics awareness in diverse university environments. *Consortium for Computing Sciences in Colleges*, *25*(5), 223–230.

Nuñez-Gonzalez, J. D., Graña, M., & Apolloni, B. (2015). Reputation features for trust prediction in social networks. *Neurocomputing*, *166*(1), 1–7. https://doi.org/10.1016/j.neucom.2014.10.099

Oluwole V. (2022, June 15). Top 10 fastest growing cities in Africa 2022. Business Insider Africa. Retrieved September 20, 2022, from https://africa.businessinsider.com/local/lifestyle/top-10-fastest-growing-cities-in-africa-2022/b97e271

Ostendorf, S., Müller, S. M., & Brand, M. (2020). Neglecting long-term risks: Self-disclosure on social media and its relation to individual decision-making tendencies and problematic social-networks-use. *Frontiers in Psychology, 11*, 1–17. https://doi.org/10.3389/fpsyg.2020.543388

Pearsall, J., & Hanks, P. (Eds) (1999). *The new oxford dictionary of English*. Oxford University Press.

Potter, W. J. (2014). *Media literacy* (7th ed.) Sage. https://doi.org/10.1111/soc4.12041

Richey, M., Gonibeed, A., & Ravishankar, M. N. (2018). The perils and promises of self-disclosure on social media. *Information Systems Frontiers*, *20*(3), 425–437. https://doi.org/10.1007/s10796-017-9806-7

Rideout, V. J., Foehr, U. G., & Roberts, D. F. (2010). *Generation M2: Media in the lives of 8- to 18-year-olds*. Kaiser Family Foundation. https://files.eric.ed.gov/fulltext/ED527859.pdf

Rose, S., Spinks, N., & Canhoto, A. I. (2015). *Management research: Applying the principles*. Routledge. https://doi.org/10.4324/9781315819198

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S., AAhlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social networks sites using protection motivation theory, trust and risk. *Journal of Internet social Networking and Virtual Communities,* 1–11. https://doi.org/10.5171/2012.281869

Salo, J., & Karjaluoto, H. (2007). A conceptual model of trust in the online environment. *Online Information Review, 31*(5), 604–621. https://doi.org/10.1108/14684520710832324

Senthil, K. N., Saravanakumar, K., & Deepa, K. (2016). On privacy and security in social media - A comprehensive study. *Procedia Computer Science*, *78*, 114–119. https://doi.org/10.1016/j.procs.2016.02.019

Serenko, N., & Fan L. (2013). Patients' perceptions of privacy and their outcomes in healthcare. *International Journal of Behavioral and Healthcare Research*, *4*(2), 101–122. https://doi.org/10.1504/IJBHR.2013.057359

Slusky L., & Partow-Navid, P. (2012). Students' information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3–26. https://doi.org/10.1080/15536548.2012.10845664

Stein, L., & Sinha, N. (2002). New global media and communication policy: The role of the state in the twenty-first century. In L. Lievrouw, & S. Livingstone (Eds.), *Handbook of new media: Social shaping and consequences of ICTs* (pp. 410–431). *Sage Publications.* https://www.doi.org/10.4135/9781848608245.n30

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *Journal of the International Digital Media and Arts Association*, *3*(1), 10–18.

Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., & Lampe, C. (2012). Privacy in interactions: Exploring disclosure and social capital in Facebook. *Proceedings of the 8th International AAAI Conference on Weblogs and Social Media, 6*(1), 330-337. https://doi.org/10.1609/icwsm.v6i1.14268

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, *29*, 821–826. https://doi.org/10.1016/j.chb.2012.11.022

Taddicken, M. (2013). The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tan, X., Qin, L., Kim, Y., & Hsu, J. (2012). Impact of privacy concern in social networking web sites. *Internet Research, 22*(2), 211–233. https://doi.org/10.1108/10662241211214575

Thelwall, M. (2008). Social networks, gender, and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology 59*(8), 1321–1330. https://doi.org/10.1002/asi.20835

Thomas, K. A., & Laseinde, A. A. (2015). Training needs assessment on the use of social media among extension agents in Oyo State, Nigeria. *Journal of Agricultural Informatics, 6*(1), 100–111. https://doi.org/10.17700/jai.2015.6.1.144

Tomy, S., & Pardede, E. (2016). Controlling privacy disclosure of third-party applications in online social networks. *International Journal of Web Information Systems*, *12*(2), 215–241. https://doi.org/10.1108/IJWIS-12-2015-0045

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society, 28,* 20–36. https://doi.org/10.1177/0270467607311484

Tuunkainen, V. K., Pitkänen, O., & Hovi, M. (2009). Users' awareness of privacy on online social networking sites - Case Facebook company. In *Proceeding of the 22nd Bled eConference, eEnablement: Facilitating an Open, Effective and Representative eSociety* (pp. 14–17). AIS Electronic Library. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1000&context=bled2009

Van Dijk, J. (2012). *The network society* (3rd Ed.). SAGE Publications.

Van der Walt, E., Eloff, J. H., & Grobler, J. (2018). Cyber-security: Identity deception detection on social media platforms. *Computers & Security*, *78*, 76–89. https://doi.org/10.1016/j.cose.2018.05.015

Warner, M., & Wang, V. (2019). Self-censorship in social networking sites (SNSs) – privacy concerns, privacy awareness, perceived vulnerability and information management. *Journal of Information, Communication and Ethics in Society, 17*(4), 375–394. https://doi.org/10.1108/JICES-07-2018-0060

Weinberger, M., & Zhitomirsky-Geffet, M. (2017). Factors affecting users' online privacy literacy among students in Israel. *Online Information Review, 41*(5), 655–671. https://doi.org/10.1108/OIR-05-2016-0127.

Wang, T., Ulmer, J. R., & Kannan, K. (2013). The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organisational Computing and Electronic Commerce, 23(*3), 200–223. https://doi.org/10.1080/10919392.2013.807712

Wang, X., Wang, Y., Lin, X., & Abdullat, A. (2021). The dual concept of consumer value in social media brand community: A trust transfer perspective. *International Journal of Information Management, 59,* 1-12.

https://doi.org/10.1016/j.ijinfomgt.2021.102319

West, R., & Turner, L. (2007). *Introducing communication theory*. McGraw Hill.

Westin, A. F. (1967). Special report: Legal safeguards to insure privacy in a computer society. *Communications of the ACM, 10*(9), 533–537. https://doi.org/10.1145/363566.363579

Wu, W.-Y., & Sukoco, B.M. (2010). Why should I share? Examining consumers' motives and trust on knowledge sharing. *Journal of Computer Information Systems, 50*(4), 11–19.

Yao, M. Z., & Zhang, J. (2008). Predicting user concerns about online privacy in Hongkong. *Cyberpsychology and Behavior, 11*(6), 779–781. https://doi.org/10.1089/cpb.2007.0252

Yerby, J., Koohang, A., & Paliszkiewicz, J. (2019). Social media privacy concerns and risk beliefs. *Online Journal of Applied Knowledge Management*, *7*(1), 1-13. https://doi.org/10.36965/OJAKM.2019.7(1)1–13.

Ying, F., Dartey, S., Ahakwa, I., Odai, L. A., Bright, D. & Amoabeng, S. M. (2021). Ascertaining the perceived risks and benefits of social media usage on the behavioural intent of employees: study of the banking sectors in ga-west municipality: Mediating role of user satisfaction. *International Research Journal of Advanced Engineering and Science*, *6*(1), 109–116.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, *43*(3), 389–418. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zhang, J. (2015). Voluntary information disclosure on social media. *Decision Support Systems*, *73*, 28–36. https://doi.org/10.1016/j.dss.2015.02.018

Zhang, S., Kwok, Ron C-W., Lowry. P. B., & Liu, Z. (2019). Does more accessibility lead to more disclosure? Exploring the influence of information accessibility on self-disclosure in online social networks. *Information Technology & People, 32*(3), 754–780. https://doi.org/10.1108/ITP-04-2017-0134

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. In *Proceedings of the 2007 Annual Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries (SAICSIT),* (pp. 197-204). Association for Computing Machinery. https://doi.org/10.1145/1292491.1292514