Development of a Proposed Model for Online Social Media Users' Information Disclosure

Adebayo Afolabi Olajide, Joy Oluwabukola Olayiwola
University Library, Precious Cornerstone University, Ibadan, Nigeria
Federal Polytechnic, Computer Science Department, Ilaro, Nigeria

Abstract

Online social media keep evolving and adopted by users of various categories with diver types of information being provided as necessity for registration or for other purposes. There has been researches on how people behave in online environment. Several factors have been investigated as affecting online social media (OSM) users disclosure of information. This study tries to determine factors influencing information disclosure among OSM users and propose a model. The study employs descriptive method and survey design in gathering data to answer research questions. Level of significance effect for each factor was determined. Two theories were used as a basis to develop the proposed model. The results showed the effect of these factors on disclosure of information, recommendations and suggestions on how to protect users' online information on social media is also provided.

Keyword: Online Social Media, Online Social Media Users, Civil Servants, Information privacy, Information security

1. Introduction:

Information privacy and security is one major challenge of the modern-day internet or online platforms. Virtually all the online platforms are prone to one form of attack or the other. The online attacks are of diverse types. Online information attackers develop or invent different types of attacks. Attack against online users can be on the system used (hardware), the software, the platform (application), the backbone (internet or network), the users (direct physical) or information supplied on the platforms. All the attacks on internet users are targeted at a particular source or combination of sources. One of the most fertile sources of launching attack by the online attackers is availability of "personal information". Diverse types and large quantities of information are supplied by various users of online platforms. Users of online social media are asked to register through which they were asked to supply certain types of personal information. While some users may supplied just what is needed some others may supply more than necessary. Also in the course of using the online social networks, users send or post various types of information to colleagues, online administrators or update to the site, other pop-up request, various deceptive "promos" or lotteries and the likes. Other users in the context of trying to express emotion or socialising release some private and personal information which can be a possible cause of attack(s). There has been great concern to making these online social networks as safe as possible. It has been discovered that it takes more than one end to protect and safeguard the users. Various strategies has been employed to ensure online social network safety, these include privacy and security setting, awareness on how to use the platform, security education by the site administrators, technical securities that is expected of a would-be users, personal traits, computer efficacy among others. These and many more are some of the strategies that can be employed by users of online social networks in their bid to combat the incidence of privacy and security breaches. Privacy and security breaches can bring about a lot of damages or havoc to users in various ways. There is the need to study how users are coping with the various possible attacks on the social network sites.

Various theories have been propounded, adapted and adopted as models through which users of online social networks can overcome the various dangers. The issue of how to protect users from various online attacks has also been looked at from various dimensions such as the technical, administration of site, end-to-end encryption provided by the site administrators, users dimensions and technological methods. This research intends to study how users of online social networks in Ibadan metropolis ensure security and privacy of their information on social networks. The research also proposed a model that can be adopted in ensuring security and privacy of online users information on social networks. The following objectives and research

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

hypothesis were tested for in the course of the work.

Objectives of the study

- Examine the various factors influencing disclosure of private information by users of Online Social Networks in Ibadan.
- Develop a model to explain the influence of certain factors on disclosure of information by Online Social Network users in Ibadan.

The following set of hypotheses were tested for to establish the influence of the various factors of Information disclosure of users in OSM.

Hypothesis

H_{01} There is no significant relationship between Civil Servants' awareness of information privacy and security and disclosure of private information on Social Media (SM) in Ibadan metropolis.

H_{02} There is no significant relationship between Civil Servants perceived risk and disclosure of private information on Online Social Media (OSM) in Ibadan metropolis.

H_{03} There is no significant relationship between Civil Servants perceived benefit and disclosure of private information on OSM in Ibadan metropolis.

H_{04} There is no significant relationship between Civil Servants' computer self-efficacy and disclosure of private information on OSM in Ibadan metropolis.

H_{05} There is no significant relationship between Civil Servant trust and disclosure of private information on OSM in Ibadan metropolis.

H_{06} There is no significant difference between the Civil Servant demographic variables (gender, age, education qualification, type of work and level) and information disclosure of private information on OSM in Ibadan metropolis.

2. Literature review

Factors affecting disclosure of private information - One cannot help but marvel at the nature, amount, and detail of the personal information some users provide, and ponder how informed these online users are. People willingly disclose personal information and often times even intimate details of their lives ([1]; [2]). Despite pronounced privacy concerns, people still share intimate details of their lives in Online Social Media (OSM) environment ([3], [2]). Contrary results have been reported by other researchers ([4]; [5]). Disclosure of private information on online social network is something that is determined by certain factors. Some of the identified factors that affects information disclosure on OSM that have been reported were social capital ([6]), identity presentation ([7]); benefit for electronic commerce ([8]) and Trust ([9])

Trust is a factor that exposes OSM users to disclose their private information ([9]; [10]). Unfortunately, OSM users cannot control the behaviour of the other people they have shared the information with. Researchers have reported that trust positively influence users information disclosure ([11]; [12]). Trust in terms of the security mechanisms put in place by the OSM will determine the level of private information to be disclosed [13]. [14] reported that though the users did not trust the platforms owner since it is a private organisation, yet they will still prefer to use it and give out their personal information. Another factor discovered by the authors is perceived or derived benefits which affect how people share private information. On identity formation, [15] noted that people must reveal personal information in their OSM profiles in order to be effective. Habits have also been pointed to affect how information is shared on OSM [16]. [14] discovered that users of OSM rated identity formation in terms of access to relationship and value of being part of a social setting as some of the factors that lead them to disclose private information. Social interaction and identity is also another factor for revealing private information and is seen to strengthen ties and bonds in dyadic or group relationship ([17]; [14]).

On the issue of benefit, which is derivable in disclosing private information, this benefit can be described as risk versus reward. [10] confirmed that people are ready to forgo the safety of their private information if the perceived benefits are far more than the cost. Disclosure of information has been found to be related not only to benefits but also to the taste of the disclosure of the information [13]. [18] stated that the more users disclose information about themselves the more they may find gratifications and benefits from the systems.

Various benefits that are accruable from sharing private information has been documented in various literature to include: ability to maintain social ties [6]; the enhanced possibilities for reciprocation [5]; enjoyment ([5]; [9]); displaying social capital, to look important or popular [19]; time saving or convenience [8]; self-presentation [20]; providing selective information to present oneself in a positive light or to be seen in a certain way [21]; the opportunity to present only favorable information [22]. [9] identified perceived

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

ease of use and perceived usefulness which can also be categorized under the perceived benefits as affecting the disclosure of private information.

Perceived risks could also be influential of disclosure of private information ([5]). [13] stated that risks that are related to information disclosure are many and depends on the amount and type of information that is disclosed. OSM users are becoming more aware that information posted on SM can be abused by crooks, stalkers, bullies or even one's own friends [23]. [24] stated that risks will affect behaviour in OSM which also affects the disclosure of private information. Perceived risks was described as perceived damage by [9]

Perceived control has been reported to influence private information disclosure. [13] affirmed that the ability of individuals to control who sees or accesses their information affect how they disclose private information. [3] have reported that perceived control influences the perception of trust which invariably influences information disclosure. OSM like Facebook allow its users to change personal settings to control who can access or view the information in their profile [25]. When users discovered that their information is being collected without their consent, they frowned greatly at it [26]. Some studies have shown that setting of privacy, have helped them in the disclosure of private information ([27]; [19]; [28]). [29] reported that habit was the strongest predictor of information disclosure, followed by perceived control, then beliefs/trust that their information supplied will be safe. Perceived risks and trusting did not have significant effect on disclosure of private information. Lack of awareness on the part of the users that: marketers, platform administrators and other people may have access to some of their personal information ([9]; [30]; [31]. [9] identified that majority of OSM users are not concerned about privacy and security issues; this may affect their disclosure of information on the platforms. Contrary result was reported by [14] that users of OSM are aware of the exposure they face by disclosing their information on OSM but regarded it as nothing that will stop them from disclosing private information.

Social demographic factors which some authors defined as individual difference have been pointed to affect disclosure of private information: gender ([11]; [32]; [33]; [34]; Internet experiences [32] age ([2]; [35]) and cultural background [36]. Privacy concerns have been reported to rarely affect disclosure of private information ([37]; [38]).

3. Theoretical framework

This section provides the framework for this study. Two theoretical framework were reviewed: Social Exchange Theory (SET) and Social Cognitive Theory (SCT) that can be used to explain factors affecting information disclosure in online environment.

3.1. Social Exchange Theory (SET)

Social Exchange Theory goes back to ([39], [40], [41]). Social Exchange Theory states that humans weigh each relationship and interaction with another human on a reward cost scale without realizing it [41]. If the interaction was satisfactory, then that person or relationship is looked upon favourably. But if an interaction was unsatisfactory, then the relationship will be evaluated for its costs compared to its rewards or benefits. People try to predict the outcome of an interaction before it takes place. It asserts that people establish reciprocal relationships based on mutual interests [41].

The principles of the Social Exchange Theory defined one of the main factors governing interpersonal attraction, according to which people are attracted to or are interested in people similar to themselves and to those who offer meaningful resources (such as appearance, education, income, and health) that may be converted into possible rewards. The theory states that individuals engage in behaviour they find rewarding and avoid behaviour that have too high a cost. In other words, all social behaviour is based on each actor's subjective assessment of the cost-benefit of contributing to a social exchange. They communicate or exchange with each other contingent on reciprocal actions from the other communicating party [42]. The mutual reinforcement could be analyzed through a microeconomic framework, though many times the rewards are not monetary but social, such as opportunity, prestige, conformity, or acceptance [42].

Simple social exchange models assume that perceived benefit and perceived risk drive relationship decisions [43]. Both parties in a social exchange take responsibility for one another and depend on each other. The elements of relational life include:

3.1.1. Perceived risk: 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 [44] Its can be time, money, effort etc.

3.1.2. Perceived benefit: are the elements of a relationship that have positive value. It can be sense of acceptance, support, and companionship etc. As with everything dealing with the social exchange theory, it has as its outcome satisfaction and dependence of relationships. The social-exchange perspective argues that people calculate the overall worth of a particular relationship by subtracting its perceived risk from the perceived benefit it provides [45].

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

Worth = *perceived benefits – perceived risks*

If Worth is a positive number, it is a positive relationship. On the contrary, a negative number indicates a negative relationship. The worth of a relationship influences its outcome, or whether people will continue with a relationship or terminate it. Positive relationships are expected to endure, whereas negative relationships will probably terminate. In a mutually beneficial exchange, each party supplies the wants of the other party at lower risk to self than the value of the resources the other party provides. In such a model, mutual relationship satisfaction ensures relationship stability [46].

Outcome = *perceived benefits – perceived risks*

Homans based his theory on behaviourism to conclude that people pursue rewards to minimize costs. The satisfactions of the rewards that a party gains from an exchange relationship is judged relative to some standard, which may vary from party to party [46]. Hence [47] gave the reasons why people engage in a social exchange to have been posited as an expected gain in reputation and influence on others; an anticipated reciprocity on the part of others; altruism; and direct reward. Given that participation in the social media is not compensated, the first three reasons appear to have particular relevance to why people participate in social media.

3.2. Social Cognitive Theory (SCT)

A Social Cognitive Theory, [48] advanced a view of human functioning that accords a central role to cognitive, vicarious, self-regulatory, and self-reflective processes in human adaptation and change. People are viewed as self-organising, proactive, self-reflecting and self-regulating rather than as reactive organisms shaped and shepherded by environmental forces or driven by concealed inner impulses [49]. The theory states that when people observe a model performing a behaviour and the consequences of that behaviour, they remember the sequence of events and use this information to guide subsequent behaviour. Observing a model can also prompt the viewer to engage in behaviour they already learned.

The capacity to exercise self-influence by personal challenge through goal setting and evaluative reaction to one's own performances provides a major cognitive mechanism of motivation and self-directedness [50]. In [51] article, he claimed that Social Learning Theory shows a direct correlation between a person's perceived self-efficacy and behavioural change. Self-efficacy comes from four sources: "performance accomplishments, vicarious experience, verbal persuasion, and physiological states" [51]. Goal adoption enlists self-investment in the activity. Once people commit themselves to valued goals, they seek self-satisfaction from fulfilling them and intensify their efforts by discontent with substandard performances. The motivational effects do not stem from the goals themselves, but from the self-evaluation that is made conditional on their fulfilment [50].

From this theoretical perspective, human functioning is viewed as the product of a dynamic interplay of personal, behavioural, and environmental influences. For example, how people interpret the results of their own behaviour informs and alters their environments and the personal factors they possess which, in turn, inform and alter subsequent behaviour. This is the foundation of [48] conception of reciprocal determinism, the view that; personal factors in the form of cognition, affect, and biological events; behaviour and environmental influences create interactions that result in a triadic reciprocity. Bandura altered the label of his theory from social learning to social "cognitive" both to distance it from prevalent social learning theories of the day and to emphasize that cognition plays a critical role in people's capability to construct reality, self-regulate, encode information, and perform behaviour [49].

3.2.1. Self-efficacy: Social cognitive theory posits that learning most likely occurs if there is a close identification between the observer and the model and if the observer also has a good deal of self-efficacy. Self–efficacy is the extent to which an individual believes that they can master a particular skill. Self-efficacy beliefs function as an important set of proximal determinants of human motivation, affect, and action—which operate on action through motivational, cognitive, and affective intervening processes [52].

According to Bandura, self-efficacy is the belief in one's capabilities to organize and execute the courses of action required to manage prospective situations [51]. Bandura and other researchers have found an individual's self-efficacy plays a major role in how goals, tasks, and challenges are approached. Individuals with high self-efficacy are more likely to believe they can master challenging problems and they can recover quickly from setbacks and disappointments. Individuals with low self-efficacy tend to be less confident and don't believe they can perform well, which leads them to avoid challenging tasks. Therefore, self-efficacy plays a central role in behaviour performance. Observers who have high level of self-efficacy are more likely to adopt observational learning behaviour.

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

4. Conceptual Framework

The conceptual framework for this study is derived from the Social Exchange Theory (SET) and Social Cognitive Theory (SCT). The constructs: perceived risk; perceived benefit; self-efficacy; awareness of information privacy and security; gender; academic qualification and trust will be used to build a research framework in this study.

Disclosure of private information on OSM and security awareness - [9] on factors that influence self-disclosure amount in social media (SM) did made use of security awareness and information disclosure. [30] research titled students and privacy in the networked environment used security awareness; and [31] networks security emerging security information, systems and technologies also used security awareness. [53] results of their survey showed that although most of the users were aware of the privacy settings, most of them do not change their privacy settings from default settings.

According to [54] there exists a positive association between awareness and SNSs users' information privacy concerns. Extant literature suggests that most users are willing to share online profiles/information given that privacy issues are adequately addressed [55]. Hence, we hypothesise that:

$H_{01:}$ There is no significant relationship between security awareness and information disclosure among OSM users.

Perceived risks and disclosure of private information on SM - perceived risk is a construct adopted from social exchange theory. It is the elements of relational life that have negative value to a person, such as the effort put into a relationship. It could be influential of disclosure of private information, [13] stated that risks that are related to information disclosure are many and depends on the amount and type of information that is disclosed. OSM user are becoming more aware that information posted on SM can be abused by crooks, stalkers, bullies or even one's own friends [23]. [9] described perceived risks as perceived damage. [56] in a study adopting SET to explain that individuals engage in relationships when the perceived costs associated with the relationship are less than the expected perceived benefits. It further explains that individuals participate in self-disclosure to foster relationships - reciprocation is the primary benefit of self-disclosure, whereas risk is the foundational cost of self-disclosure.

[57] in her research on understanding privacy decision -making using social exchange theory explore that disclosure is often a reasonable, and even rational, response to so many of the decisions that we face, even those with detrimental privacy consequences. It's similar to the impulse that makes smartphones users reach for smartphones to check to see who just texted, despite the fact that they are navigating a vehicle down a freeway at seventy miles per hour. The technology has been overlaid upon our existing social structures, but with none of the limitations inherent to our cognitive capacities. [53], showed that perceived risks and disclosure of private information on SM shows that users were cautious about accepting friend requests from strangers so as not to disclose their private information on SM to the public. [54] found out that there is a positive relationship existing between SNSs users' privacy concerns and their risk perceptions. Hence, we hypothesis that:

$H_{02:}$ There is no significant relationship between perceived risks and information disclosure among OSM users.

Perceived benefits and disclosure of private information on SM - Perceived benefit is a construct adopted from social exchange theory. It is the elements of a relationship that have positive value. Rewards can be sense of acceptance, support, and companionship etc. Rewards can consist of anything tangible or intangible that an individual considers valuable [44]. The various forms of benefits have been confirmed to affect information disclosure; for example social ties ([6]); the enhanced possibilities for reciprocation [5]; enjoyment ([5]; [9]; displaying social capital to look important or popular [19]; time saving or convenience [8]; self-presentation [20]; providing selective information to present oneself in a positive light or to be seen in a certain way [21]; the opportunity to present only favourable information [22]. Hence we hypothesis that:

$H_{03:}$ There is no significant relationship between perceived benefits and information disclosure among OSM users.

Computer self-efficacy (CSE) and disclosure of private information on SM - Self–efficacy is a construct derived from Social cognitive theory. It is seen as the extent to which an individual believes that they can master a particular skill. Self-efficacy beliefs function as an important set of proximal determinants of human motivation, affect, and action, to which operate on action through motivational, cognitive, and affective intervening processes. [52] posits that learning most likely occurs if there is a close identification between the observer and the model and if the observer also has a good deal of self-efficacy. CSE can be described as pertaining to individuals' judgment of their

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

capabilities to use computers under different situations. Research has shown that CSE significantly influences an individual's decision to use computers to achieve various tasks [58}. [59] investigated the role of user computer self-efficacy (CSE), cybersecurity countermeasures awareness, and cybersecurity skills toward computer misuse intention in organisations.

H_{04}: There is no significant relationship between computer self-efficacy and information disclosure among OSM users.

Trust and disclosure of private information on SM - [60] addressed trust as a firm belief in the competence of an agent to act dependably, securely, and reliably within a specified context. Trust is an important element that can determine the success of online social networks and other business websites. Social network providers and other service providers have to increase the users' confidence and push them to trust their services by providing a secure and easy system for users' personal information privacy protection. Users may also trust communications between their computers and the internet websites more than online social network providers in terms of leakage of personal information [61].

[54] find out that user's privacy concerns do not have a significant effect on their trust in the use of SNSs. Although previous literature demonstrates an association between privacy concerns and trust in e-commerce context [62]. These results may not prove suitable within the context of SNSs. Hence, it can be construed that OSM users may be left to think safeguarding privacy alone is not sufficiently adequate enough to trust OSM [54]; in lieu of their finding, they may anticipate other information practices to be in place such as security measures to increase their trust perceptions [63]. Hence we hypothesise that:

H_{05}: There is no significant relationship between trust and information disclosure among OSM users.

Demographic variables and disclosure of private information on SM - [64] refer to gender differences as an average group difference between male and female that are presumably based on sexually monomorphic (the same between the sexes biological adaptations).Gender have been used to affect information disclosure by [11] in their research titled internet social network communities: risk taking, trust, and privacy concerns. [32] made used of gender in predicting user concerns about online privacy in Hongkong. [33] research titled social networks, gender, and friending: An analysis of MySpace member profiles and also [34] study titled Grooming, gossip, Facebook and Myspace made used of gender as part of their social demographic factors.

[53] studied the effect of educational qualification on information disclosure. Their study titled personal information privacy settings of online social networks and their suitability for mobile internet devices made used of personal information which includes educational qualification with other information and privacy protection. Early study by [66] found that certain users' demographic factors influence internet users information privacy concerns (IUIPC) such as age, education and income level. [64] find out that gender does play a role in personal information disclosure with males more likely to disclose personal information than females in every category. The study revealed that gender, age, and education have significant influences on information disclosure and user's privacy settings and that on most sites over 50% of friend requests were readily accepted. Hence, we hypothesise that:

H_{06}: There is no significant relationship between demographic variables and information disclosure among OSM users.

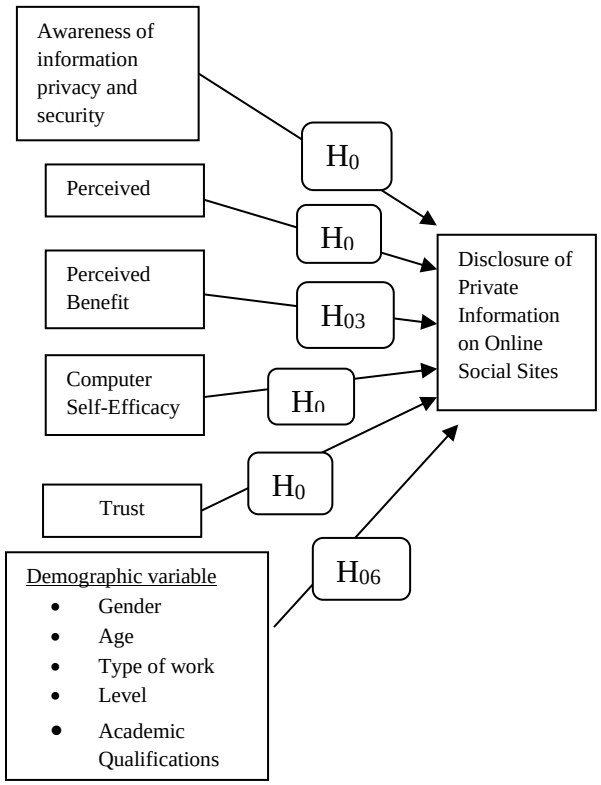

Figure 1. Conceptual framework

The conceptual framework is presented in Figure 1. The framework shows that disclosure of private

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

information on SM could be influenced by perceived risk, perceived benefit, CSE, awareness of information privacy and security, trust and demographic variables.

5. Methodology

In a bid to develop a proposed model for factors affecting information privacy and security practice among online social media users in Ibadan metropolis, literature review of various factors affecting information privacy and security practices among users of online sociFigal networks was carried out. Also, two theoretical models that have been earlier proposed as affecting disclosure of information were also reviewed. A conceptual model was developed by the researcher from the previous theoretical models. The independent variables were for tested to determine their level of significance on the dependent variable. The conceptual model was based on the previous models of information privacy and security practices and the various factors that affect disclosure of information. A questionnaire was administered to gather data on information privacy and security practices to be able to test for the level of significance of the various factors in the conceptual model. A sample of 255 respondents that are Civil Servants' residents within Ibadan metropolis covering the 13 local governments that make up Ibadan metropolis was drawn covering various demography of users. In the course of administering the questionnaire, the researcher visits different locations like government offices, private offices, shopping malls, parks, to ensure a wide spread of the respondents for this research.

6. Analysis of Findings

Descriptive Analyses of Variables - We present information about the socio-demography variables of the respondents (sex, age, highest educational level, type of work, and level of work) of the respondents, factors influencing disclosure of private information.

The information provided here was analysed using frequency count and percentage (see the various socio-demographic variables of the respondents in Table 1). The Table 1 revealed that 156 (61.2%) were males while 99 (38.8%) were females; 2 (0.8%) were less than 20, 9 (3.5%) were between 20-25 years, 44 (17.3%) were between 26-30 years, 43 (16.9) were between 31-35 years, 50 (19.6%) were between 36-40 years, 45 (17.6%) were between 41-45 years,34 (13.3%) were between 46-50 years and 28 (11.0%) were above 50 years and above. Results also showed that 14 (5.5%) have SSCE/O' Level, 41 (16.1%) OND/NCE, 135 (52.9%) HND/ Bachelor, 56 (22.0%) have Masters, while 9 (3.5%) are PhD holders.

Table 1. Sociology-Demographic Variables of the Respondents

All	Demographic Char	Frequency	Percentage
Sex	Male	156	61.2
	Female	99	38.8
	Total	**255**	**100.0**
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
	Total	**255**	**100.0**
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
	Total	**255**	**100.0**
Type of Work	Local govt. staff	99	38.8
	NECO staff	44	17.2
	Administrator	40	15.7
	Teacher	19	7.5
	Auditor	18	7.1
	Speech Therapist	2	0.8
	IT	4	1.6
	Librarian	7	2.7
	Medical Officer	15	5.9
	Security	7	2.7
	Total	**255**	**100.0**
Level of 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
	16 – above	3	1.2
	Total	**255**	**100.0**

Our findings demonstrated that 99 (38.8%) were local government staff, 44 (17.2%) were National Examination Council (NECO) staff, 40 (15.7%) were administrator, 19 (7.5%) were teacher, 18 (7.1%) were auditor, 2 (0.8%) were speech therapist, 4 (1.6%) were IT, 7 (2.7) were librarian, 15 (5.9%) were medical officer, while 7 (2.7%) were security. Lastly, results showed that 8 (3.1%) are on level 1-3, 54 (21.2%) are on

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

level 4-6, 113 (44.3%) are on level7-9, 61 (23.9%) are on level 10-12,16 (6.3) are on level 13-15 while 3 (12.0%) are on level 16 above. From the findings above, it suffices to state that majority of the respondents were males, between the age of 36 and 40, HND/ Bachelor holder local government staff and were on level 7 – 9.

What factors influence disclosure of private information by users of OSM in Ibadan metropolis?

This research question examines factors influencing disclosure of private information by users of SM in Ibadan metropolis, this section was divided into five parts which were perceived benefits, perceived risks, trust, computer self-efficacy and awareness. A Likert scale was used to measure the variables; "Strongly Disagree", "Disagree", "Agree" and "Strongly Disagree", which was later merged as "Strongly Disagree + Disagree = Disagree" and "Strongly Agree + Agree = Agree". The findings were as presented in Table 2.

Table 2. Factors influencing disclosure of Civil Servants private information by users of OSM

No	**Factors influencing disclosure**	**Agree (%)**	**Disagree (%)**	**Mean**	**St. D**
	Perceived benefits				
i.	Feel important sharing personal information	138 (54.1)	117 (45.9)	1.46	.499
ii.	Derived joy sharing and getting information	209 (82.0)	46 (18.0)	1.18	.385
iii.	Get information	225 (88.2)	30 (11.8)	1.12	.323
iv.	Know more people	226 (88.6)	29 (11.4)	1.11	.318
	Perceived risk				
v.	Don't care about risk of sharing information	122 (47.8)	133 (52.2)	1.52	.501
vi.	Afraid SM will sell my information	173 (67.8)	82 (32.2)	1.32	.468
vii.	Adequate protection of information supplied	179 (70.2)	76 (29.8)	1.30	.458
viii.	Place for various vices and evil to take place	190 (74.5)	65 (25.5)	1.25	.437
ix.	Personal information get to untrusted hands	197 (77.3)	58 (22.7)	1.23	.420
x.	Information can get to wrong hands	209 (82.0)	46 (18.0)	1.18	.385
xi.	Hackers were danger to personal information	212 (83.1)	43 (16.9)	1.17	.375
	TRUST				
xii.	Not share information with third party	145 (56.9)	110 (43.1)	1.43	.496
xiii.	Friends not use information to abuse	149 (58.4)	106 (41.6)	1.42	.494
xiv.	Good security to protect my information	151 (59.2)	104 (40.8)	1.41	.492
xv.	Everybody plays according to rules	154 (60.4)	101 (39.6)	1.40	.490
	COMPUTER SELF EFFICACY				
xvi.	Privacy setting to control information	196 (76.9)	59 (23.1)	1.23	.423
xvii.	Change default security and privacy setting	211 (82.7)	44 (17.3)	1.17	.379
xviii.	Operate computer devices very well	226 (88.6)	29 (11.4)	1.11	.318
	AWARENESS				

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

xix.	Controlling privacy settings	211 (82.7)	44 (17.3)	1.17	.379
xx.	Privacy setting	213 (83.5)	42 (16.5)	1.16	.372
xxi.	Sharing personal information	225 (88.2)	30 (11.8)	1.12	.323

Note: St.D represent standard deviation.

The Table 2 indicates perceived benefits in the following order: 226(88.6%) know more people, 225(88.2%) get information, 209(82.0%) derived joy sharing and getting information and 138(54.1%) respondents feel important sharing personal information.

Perceived risk construct shows that 173(67.8%) respondents were afraid that SM will sell their information, 212(83.1%) respondents agreed that hackers were a danger to personal information and 209(82.0%) also agreed that information can get to wrong hands. While 133(52.2%) disagreed that they don't care about risk of sharing information. 197(77.3%) agreed that personal information get to untrusted hands, 179(70.2%) agreed that SM provide adequate protection of information supplied by users and 190(74.5%) agreed that SM is a place for various vices and evil to take place.

Trust construct shows that154(60.4%) agree that everybody plays according to SM rules, 151(59.2%) respondents agree SM has a good security to protect my information, also 149(58.4%) respondents do agree that friends do not use information to abuse, meanwhile 145(56.9%) respondents agree that SM does not share information with third party. Computer self-efficacy construct indicate that 226(8.6%) majority agreed that they can operate computer devices very well, 211(82.7%) respondents agreed that they can change default security and privacy setting, 196(76.9%) respondents also do agree that can use the privacy setting to control information.

Awareness construct shows that 213(83.5%) knows privacy setting, 225(88.2%) knows about the risk in sharing personal information and 211(82.7%) know how to control privacy settings. From the findings, all the users agree to the various factors that were responsible for disclosure of private information. All the major

constructs were rated highly as affecting disclosure of information with the exception of trust that is a bit low.

6.1. Test of Hypothesis

H_{01}: There is no significant relationship between awareness of privacy and security on SM and information disclosure in Ibadan metropolis.

The Table 3 shows 0.05 significant level, the result (r=0.388**, p=0.000) indicates that there is a significant relationship between awareness of privacy and security on SM and information disclosure in Ibadan metropolis. As a result, the alternative hypothesis was accepted.

While Table 4 with 0.01 significant level, the result (r=0.298**, p=0.000) indicates that there is a significant relationship between perceived risk and disclosure of private information among Civil Servants using OSM in Ibadan metropolis. As a result, the alternative hypothesis was accepted.

Table 3. Correlation Analysis of Civil Servant's Awareness of Privacy and Security on SM and Information Disclosure

		Awareness	**Disclosure**
Awareness	Pearson Correlation	1	.388**
	Sig. (2-tailed)		.000
	N	255	255
**. Correlation is significant at the 0.01 level (2-tailed).			

H_{02}: There is no significant relationship between perceived risk and disclosure of private information on OSM users in Ibadan metropolis.

Table 4. Correlation analysis of Civil Servant's perceived risk and disclosure of private information on OSM users in Ibadan metropolis

		Risk	**Disclosure**
Perceived Risk	Pearson Correlation	1	.298**
	Sig. (2-tailed)		.000
	N	255	255
**. Correlation is significant at the 0.01 level (2-tailed).			

H_{03}: There is no significant relationship between perceived benefit and disclosure of private information on OSM users in Ibadan metropolis.

Table 5: Correlation Analysis of Civil Servant's Perceived Benefit and Disclosure of Information on OSM

		Benefit	**Disclosure**
Perceived Benefit	Pearson Correlation	1	.366**
	Sig. (2-tailed)		.000

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

	N	255	255
**. Correlation is significant at the 0.01 level (2-tailed).			

The Table 5 0.01 significant level, the result (r=0.366**, p=0.000) indicates that there is a significant relationship between Civil Servant's perceived benefit and disclosure of private information on OSM in Ibadan metropolis. As a result, the alternative hypothesis was accepted.

H_{04}: There is no significant relationship between Civil Servants *computer self-efficacy and disclosure of private information on OSM users in Ibadan metropolis.*

The Table 6 shows 0.01 significant level, the result (r=0.327**, p=0.000) indicates that there is a significant relationship between computer self-efficacy and disclosure of private information on SM in Ibadan metropolis. As a result, the alternative hypothesis was accepted.

Table 6. Correlation Analysis of Civil Servant's Computer Self-Efficacy and Disclosure of Private Information on OSM

		CSE	**Disclosure**
CSE	Pearson Correlation	1	.327**
	Sig. (2-tailed)		.000
	N	255	255
**. Correlation is significant at the 0.01 level (2-tailed).			

H_{05}: There is no significant relationship between Civil Servants *trust and disclosure of private information on OSM users in Ibadan metropolis.*

Table 7. Correlation Analysis of Civil Servant's Trust and Disclosure of Private Information on OSM

		Trust	**Disclosure**
Trust	Pearson Correlation	1	.408**
	Sig. (2-tailed)		.000
	N	255	255
**. Correlation is significant at the 0.01 level (2-tailed).			

The Table 7 shows 0.05 significant level, the result (r=0.408**, p=0.000) indicates that there is a significant relationship between trust and disclosure of private information on SM in Ibadan metropolis. As a result, the alternative hypothesis was accepted.

H_{06}: There is no significant difference between the demographic variables (gender, age, education qualification, type of work and level) and information disclosure of private information on SM in Ibadan metropolis.

The Mann-Whitney test was employed to test the effect of each of the demographic variables of Civil Servants' disclosure of private information on OSM in Ibadan Metropolis. Table 8 presents significant difference in information disclosure of private information on OSM in Ibadan metropolis with respect to the gender of the respondent (Z=-.068, p=0.946). The null hypothesis is accepted. Table 9 shows that there is a significant difference in information disclosure of private information on OSM in Ibadan metropolis with respect to the age of the respondent (Z=-.619, p=.536). The null hypothesis is accepted. The Table 10 shows that there is a significant difference in information disclosure of private information on OSM in Ibadan metropolis with respect to the highest education qualification of the respondent (Z=-1.006, p=0.314). The null hypothesis is accepted.

Table 8. Significant Difference of Civil Servant's Demographic Variable (gender) and Information disclosure of OSM

	Gender
Z	-.068
Asymp. Sig. (2-tailed)	.946
Mann-Whitney U a. Grouping Variable: Gender	

Table 9: Civil Servant's Demographic Variable (age) and Information Disclosure of OSM

	Age
Z	-.619
Asymp. Sig. (2-tailed)	.536
Mann-Whitney U a. Grouping Variable: age	

Table 10. Civil Servant's Demographic Variable and SM Information Disclosure

	HEQ
Z	-1.006
Asymp. Sig. (2-tailed)	.314
Mann-Whitney U Grouping variable: HEQ	

Note: HEQ means highest educational qualification

Table 11. Mann-Whitney Test Significant Difference in Information Disclosure

	Level
Z	-.783
Asymp. Sig. (2-tailed)	.433
Mann-Whitney U a. Grouping Variable: level in the place of work	

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

Table 11 shows that there is a significant difference in information disclosure of private information on OSM in Ibadan metropolis with respect to the work level of the respondent (Z=-.783, p=0.433). The null hypothesis is accepted.

6.2. Summary of values

The Table 12 shows a summary of the values of the hypotheses test, their significant values and decisions on the null hypotheses.

Table 12. Summary of Hypotheses Test

Variables	Correlation coefficient	Significant values	Decision
Awareness of privacy and security on SM and information disclosure	0.388**	0.000	Reject
Perceived risk and disclosure of private information on SM	0.298**	0.000	Reject
Perceived benefit and disclosure of private information on SM	0.366**	0.000	Reject
Computer self-efficacy and disclosure of private information on SM	0.327**	0.000	Reject
Trust and disclosure of private information on SM	0.408**	0.000	Reject
Information disclosure of private information on SM with respect to the gender.	-0.068	0.946	Accept
Information disclosure of private information on SM with respect to the age	-0.619	0.536	Accept
Information disclosure of private information on SM with respect to the highest education qualification	-1.006	0.314	Accept
Information disclosure of private information on SM with respect to the work level	-0.783	0.433	Accept

6. Discussion

What factor influence disclosure of private information by OSM users in Ibadan metropolis? From the result of this research question, it was found that perceived risk, perceived benefit, computer self-efficacy, trust and awareness can highly influence disclosure of private information this is in agreement with the results of [4] and [5]. [14] stated that users of OSM were aware of the exposure they face by disclosing their information on OSM but regarded it as nothing that will stop them from disclosing private information. Also, trust is a factor that exposes OSM users to disclose their private information [9]. Some studies have shown that setting of privacy, have helped them in the disclosure of private information ([38]; [27]; [19]; [28]).

The findings of this hypothesis showed that there is a relationship between perceived risk and disclosure of private information signifying that the respondents were fully aware of the risk in disclosing their personal information.

H_{02}: There is no significant relationship between perceived risk and disclosure of private information on OSM in Ibadan metropolis.

The findings of this study contradict that of [29] who reported perceived risks did not have significant effect on disclosure of private information. [13] stated that perceived risks that were related to information disclosure were many and depends on the amount and type of information that is disclosed. [54] found that there is a positive relationship existing between OSM users' privacy concerns and their risk perceptions which support the findings of this research. The desire to be part of these new online communities seems to negate the awareness of risk and threats of over-disclosure of information on these platforms.

H_{03}: There is no significant relationship between perceived benefit and disclosure of private information on OSM users in Ibadan metropolis.

The H_{03} showed that there is a relationship between perceived benefit and disclosure of private information on OSM meaning that the benefits of sharing personal information instigates the respondents to share their information not minding the risk attached to it which support [66]. They found that perceived benefits by users of OSM is moderately related to information disclosure, users felt that by providing their real identity, it will increase their chances of being properly identified and easily meet old/new friends and family members. [9] identified the following which can also be categorized under the perceived benefits as perceived ease of use and perceived usefulness as also affecting the disclosure of private information. The various forms of benefits have been confirmed to affect information disclosure; for example, social ties [5].

The benefits attributable to use of online social networks sites may overshadow the risks associated with it vis-a-vis the rational nature of human beings. Also the value of the benefit may far outweigh the experienced or expected risks that they have been 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

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

successfully, so they may not see reasons why they should not disclose their information online.

H_{04}: There is no significant relationship between computer self-efficacy and disclosure of private information on SM in Ibadan metropolis.

We found out that *H_{04}* have relationship between computer self-efficacy and disclosure of private information which means that 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 their personal information. [67], findings indicates that individuals who assess themselves as being highly efficacious tend to look for positive outcomes from social media use, while those exhibiting low CSE were likely to expect unfavorable outcomes in disclosure of private information. The knowledge of computer in the area of setting of security features, updating, reading of security terms or installing anti-virus and other related means of circumventing risk will affect disclosure of information.

H_{05}: There is no significant relationship between trust and disclosure of private information on SM in Ibadan metropolis.

There is a significant relationship between trust and disclosure of private information on SM meaning that the respondents trust social media security in order to protect their information from third party. However, they feel free to disclose their personal information which is contrary to [54], found that users' privacy concerns do not have a significant effect on their trust in the use of SNSs. [29] reported that trusting did not have significant effect on 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 [13]. [3] stated that users with high level of trust were more comfortable with intimate topics and so they disclose more personal information. [14] reported that though the users did not trust the platforms owner since it is a private organisation, yet they will still prefer to use it and give out their personal information. Researchers have reported that trust positively influence users' information disclosure [11], [12].

H_{06}: There is no significant difference between the demographic variables (gender, age, education qualification, type of work and level) and information disclosure of private information on SM in Ibadan metropolis.

The null hypothesis was accepted which state that there is no significant difference between demographic variables and disclosure of private information contrary to some researchers. There is no difference between the male and female perspective of disclosure of private information meaning both genders do share their private information irrespective of their awareness about information disclosure, which contracts [65]. Their results indicated that gender does play a role in personal information disclosure with males more likely to disclose personal information than females in every category. From the result of the findings, all the age groups do share their personal information on social media. However, no particular age group is restricted to disclosing private information on SM. Educational qualification and level of work were not barriers to disclosing personal information on SM. Social demographic factors which some authors defined as individual difference have been pointed to affect disclosure of private information: gender ([11]; [32]; [33]; [34]); internet experiences [32] age [35]).

7. The Resultant Model

The resultant model is the diagram showing the research framework with the results of the hypotheses.

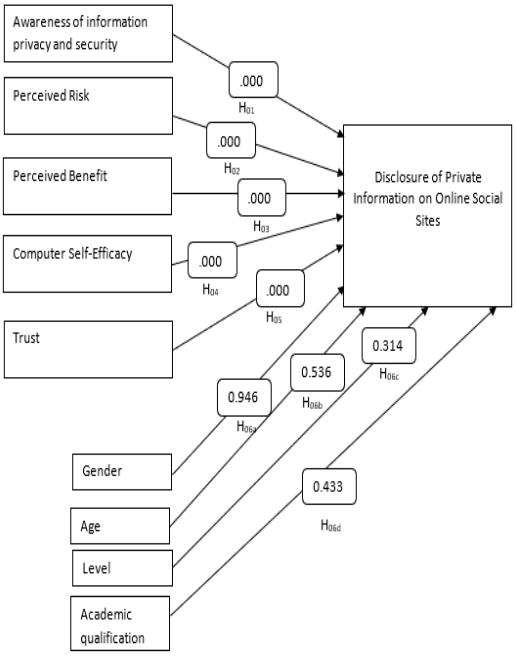

Figure 2. Resultant Model

The arrows in Figure 2 shows illustrates the relationship between the variables of the study.

8. Conclusion

Our research study has been able to establish the influence of awareness, perceived risk, perceived benefit, computer self-efficacy, trust on disclosure of private information, while there is no significance difference between the demographic characteristics and their disclosure of private information on SM. A new model of factors that can affect information privacy and security among OSN users in Ibadan metropolis was also developed. The study was also able to combine and amend both social cognitive theory and social exchange theory to explain the outcome of users of OSNs in terms of their information privacy and security disclosure.

9. Reference

[1] European Commission. (2010). European Textbook on Ethics in Research. Luxembourg: Publications Office of the European Union.

[2] Taddicken, M. (2014). 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, Vol. 19, No 2, pp. 248- 273.

[3] Taddei, S. and Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? Computers in Human Behavior, Vol. 29, pp 821–826. DOI:10.1016/j.chb.2012.11.022

[4] Stutzman, F., Vitak, J., Ellison, N. B., Gray, R., Lampe, C. (2012). Privacy in interactions: Exploring disclosure and social capital in Facebook. In Breslin, J. (Ed.), Proceedings of the 8th International AAAI Conference on Weblogs and Social Media. Palo Alto, CA: AAAI Press. 330–337.

[5] Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: why we disclose. Journal of Information Technology. 25 (2), 109-125.

[6] Ellison, N.B., Steinfeld, C., and Lampe, C. (2007). The benefits of facebook friends: exploring the relationship between college students' use of online social networks and capital. Journal of Computer-Mediated Communication Vol. 12 No 4. http://jcmc.indiana.edu/vo112/issue4/ellison.html. (Access Date: 20 December 2021).

[7] Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. International Digital and Media Arts Journal. http://www.units.muohio.edu/codeconference/papers/papers/stutzman_track5.pdf. (Access Date : 19 December 2021).

[8] Hui, K. L., Tan, B. C., and Goh, C. Y. (2006). Online information disclosure: Motivators and measurements. ACM Transactions on Internet Technology (TOIT), Vol. 6 No 4, pp. 415-441.

[9] Elmi, A. H., Iahad, N. A. and Ahmed, A.A. (2012). Factors influence self-disclosure amount in social networking sites (SMs). Journal of Information Systems Research and Innovation, 2(Dec. special issue) pp. 43-50. https://pdfs.semanticscholar.org/37d8/bc81b2b92499d89316580fedd4e8a6da020c. pdf. (Access Date: 12 August 2021).

[10] Beldad, A., De Jong, M., and Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Computers in Human Behavior, Vol. 26 No 5, pp. 857-869.

[11] Fogel, J. and Nehmad, E. (2009). Internet social network communities: risk taking, trust, and privacy concerns. Computer in Human Behaviour, Vol, 25, pp. 152-160.

[12] Mesch, G. S. (2012). Is online trust and trust in social institutions associated with online disclosure of identifiable information online. Computers in Human Behavior, 28 (4), 1471-1477. DOI: 10.1016/j.chb.2012.03.010.

[13] Beldad, A., De Jong, M., and Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviors on the internet. The Information Society, Vol. 27 No 4, pp. 220-232.

[14] Ghamari, N. and Mellbin, L. (2015). Disclosing personal information to social networking site providers: the role of trust, risk and perceived benefits. Master thesis submitted to the Department of Business Studies, Upsala University. 62. http://www.diva-portal.org/smash/get/diva2:824050/FULL TE XT01.pdf. (Access Date: 15 August 2021).

[15] Van Dijk, J. (2012). The Network Society. SAGE Publications Limited.

[16] Lankton, N. K., McKnight, D., and 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. https://www.researchgate.net/publication/313535146_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. (Access Date: 17 August 2021).

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

[18] Walther, J. B. (2011). Introduction to privacy online.In Trepte, S., Reinecke, L. (Eds.), Privacy online: Perspectives on privacy and self-disclosure in the social web (3–7). Berlin, Germany: Springer.

[19] Christofides, E., Muise, A. and Desmarais, S. (2009). Information disclosure and control on Facebook: Were they two sides of the same coin or different processes? Cyberpsychology and Behavior, Vol. 12 No 3, pp 341–345. DOI: 10.1089/cpb.2008.0226.

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

[20] Boyd, D. (2009). Why youth love social network sites: The role of networked publics in teenage social life. http://paper s.ssrn.com/sol3/papers.cfm?abstract_id=1518924. (Access Date: 9 November 2021).

[21] De Souza, Z., and Dick, G. N. (2009). Disclosure of information by children in social networking—Not just a case of "you show me yours and I'll show you mine". International Journal of Information Management, 29 (4), 255-261.

[22] Gibbs, J. L., Ellison, N. B. & Heino, R. D. (2006). Self-Presentation in Online Personals: The Role of Anticipated Future Interaction, Self-Disclosure, andPerceived Success in Internet Dating Communication Research 33(2):152-177, DOI: 10.1177/0093650 205285368.

[23] Staksrud, E. and Livingstone, S. (2009). Children and online risk. Information Communication and Society 12(3). DOI: 10.1080/13691180802635455.

[24] Kim, D. J., Ferrin, D. L. and Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: the role of trust, perceived risk, and their antecedents. Decision Support Systems, Vol. 44, pp. 544-564.

[25] Waters, S., and Ackerman, J. (2011). Exploring privacy management on Facebook: motivations and perceived consequences of voluntary disclosure. Journal of Computer-Mediated Communication, Vol. 17 No 1, pp. 101-115.

[26] Cespedes, F. V. and Smith, H. J. (2012). Database marketing: new rules for policy and practice. Sloan Management http://sloanreview.mit.edu/article/database-marketing-new-rules-for-policy-and-practice/. (Access Date: 16 August 2021).

[27] Boyd, D. and Marwick, A. (2011). "Social steganography: Privacy in network publics". Paper presented at Annual Conference of the International Communication Association. http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf. (Access Date: 14 August 2021).

[28] Litt, E. (2013). Understanding social network site users' privacy tool use. Computers in Human Behavior, Vol. 29, pp. 1649–1656. DOI:10.1016/j.chb.2013.01.049.

[29] 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. Master Thesis Report Communication Studies submitted to the department of Communication Studies University of Twente, Enschede. 40.

[30] Zorica, M. B., Biskupic, I. O., Ivanjko, T. and Spiranec, S. (2011). Students and Privacy in the Networked Environment. Mipro, 2011 Proceedings Of The 34th International Convention, 23-27 May 2011. 1090-1094.

[31] Nagy, J. and Pecho, P. S. (2009). Networks security. emerging security information, systems and technologies. Securware '09. Third International Conference on, 18-23 June 2009. 321-325.

[32] Yao, M. Z., and Zhang, J. (2008). Predicting user concerns about online privacy in Hongkong. Cyberpsychology and Behaviour, Vol. 11 No 6, pp 779–781.

[33] Thelwall, M. (2008). Social networks, gender, and friending: An analysis of MySpace member profiles. Journal of the American Society for Information Science and Technology, Vol. 59 No. 8, pp 1321–1330.

[34] Tufekci, Z. (2008). Grooming, gossip, facebook and myspace. Information Communication and Society, Vol. 11 No 4, pp 544 – 564.

[35] Rideout, V. J., Foehr, U. G. and Roberts, D. F. (2010). Generation M2: Media in the lives of 8- to 18-year-olds. Menlo Park, CA: Kaiser Family Foundation.

[36] Cong, L. (2007). Online chatters' self-marketing in cyberspace. CyperPsychology and Behavior, Vol. 10 No 1, pp. 131–132.

[37] Tan, X., Qin, L., Kim, Y. and Hsu, J. (2012). Impact of privacy concern in social networking web sites. Internet Research, Vol. 22 No 2 pp.211-233.

[38] Boyd, D. and Hargittai, E. (2010). Facebook privacy settings: Who cweres? First Monday, Vol. 15 No 8, pp 13-20. http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/ 3086/2589. (Access Date: 1 August 2021).

[39] Rusbult, C. E. (1983). Commitment and satisfaction in romantic associations: A test of the investment model. Journal of Experimental Social Psychology, 16, 172-186.

[40] Thibaut, J.W. and Kelley, H.H. (1959). The social psychology of groups. John Wiley and Sons, New York.

[41] Homans, G.C. (1958). Social behaviour as exchange. American Journal of Sociology. Vol, 63 pp. 597-606.

[42] Emerson, R.M. (1976). Social exchange theory. Annual Review of Sociology. Vol. 7, pp 335-362. htttp://annualreviewo fsociology/vol7.html. (Access Date: 29 October 2021).

[43] Encyclopedia of Public Relations (2013). Social exchange theory. thousand oaks: sage publications. http://www.credoreference.com/entry/sagepr/social_exchange_theory. (Access Date: 31 October 2021).

[44] West, R. and Turner, L. (2007). Introducing Communication Theory. McGraw Hill.186–7.17.

[45] Lambe, C. J., Wittmann, C. M. and Spekman, R. E. (2001). Social Exchange Theory and Research on Business-to-Business Relational Exchange. Journal of Business-to-Business Marketing. Vol. 8 No (3): 1–36. DOI:10.1300/J033v08n03_01.

 | DOI: 10.20533/ijisr.2042.4639.2021.0114

[46] Monge, P. R. and Contractor, N. (2003). Theories of communication networks. Oxford University Press.

[47] Chibucos, (2004). Social Exchange Theory. Chapter 5. http://www.sagepub.com. (Access Date: 13 October 2021).

[48] Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Englewood Cliffs, NJ: Prentice- Hall, Inc.

[49] Pajares, F. (2002). Overview of social cognitive theory and self-efficacy. https://www.uky.edu/~eushe2/Pajares/eff.html. (Access Date: 12 June 2021).

[50] Bandura, A. (1991). Social Cognitive Theory of Moral Thought and Action. In W. M. Kurtines and J. L. Gewirtz, (Ed), Handbook of Moral Behaviour and Development. 1, 45-103.

[51] Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. (PDF). Psychological Review. Vol. 84 No 2 pp 191–215. DOI:10.1037/0033295x.84.2.191.

[52] Bandura, A. (1989). Human agency in social cognitive theory. American Psychologist. Vol. 44 No 9 pp. 1175–1184. DOI:10.1037/0003066X.44.9.1175.

[53] Aldhafferi, N., Watson, C. and 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 (IJSPTM).2(2). DOI:10.5121.ijsptm.2013.2201.

[54] Kuo, K. and 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.

[55] Stutzman, F., Capra, R., & Thompson, J. (2011). Factors mediating disclosure in social network sites. Computers in Human Behavior, Vol. 27 No 1, 590-598.

[56] Posey, Clay; Benjamin Lowry, Paul; Roberts, Tom L.; Ellis, Selwyn (2010). Proposing the online community self-disclosure model: The case of working professionals in France and the UK who use online communities. European Journal of Information Systems, Vol. 19 No 2 pp 181–195. DOI:10.1057/ejis.2010.15.

[57] King, J. (2015). Understanding Privacy Decision – Making Using Social Exchange Theory. Vancouver, British Columbia, Canada. https://networkedprivacy2015.files.wordpress.com/2015/02/jenking_cscw_privacy_set_2015.pdf. (Access Date: 30 July 2021).

[58] Compeau, D., and Higgins, C. (1995). Computer self-efficacy: development of a measure and initial test. MIS Quarterly Vol. 19 No 2. pp.189-211.

[59] Choi, M., Levy, Y., and Hovav, A. (2012). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse. Retrieved from http://aisel.aisnet.org/wisp2012/29. (Access Date: 30 July 2021).

[60] Grandison and M. Sloman. (2000). A survey of trust in internet applications. IEEE Communication. Surveys Tuts., Fourth Quarter. http://www.comsoc.org/pubs/surveys/. (Access Date: 17 August 2018).

[61] Cutillo, L. A., Molva, R. and Strufe, T. (2009). Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, IEEE. Vol. 47, pp 94-101.

[62] Van Dyke, T. P., Midha, V., and Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in e-commerce. Electronic Markets, Vol. 17 No 1, pp. 68-81.

[63] Shin, D.H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers, Vol. 22 No 5, pp. 428-438.

[64] UNESCO, (2003). UNESCO's Gender Mainstreaming Implementation Framework. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/BSP/GENDER/PDF/1.%20Baseline%20Definitions%20of%20key%20gender-related%20concepts.pdf. (Access Date: 1 August 2021).

[65] Brown, I. and Zukowski, T. (2007). "Examining the influence of demographic factors on internet users' information privacy concerns". Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries. Port Elizabeth, South Africa. 197–204.

[66] Aljohani, M., Nisbet, A. and Blincoe, K. (2016). A survey of social media users' privacy settings and information disclosure. http://kblincoe.github.io/publications/2016_SEAU_Social_Media.pdf. (Access Date: 23 August 2021).

[67] Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. AAhlan, A. R. and Aditiawarman, U. (2012). Examining information disclosure behaviour on social networks sites using protection motivation theory, trust and risk. Journal of Internet social Networking and Virtual Communities. 2012(2012); 11 pages. DOI:10.5171/2012.281869.

