Factors Affecting Social Networking Site Users' Information Privacy Concerns: A Facebook Case

Shakir Karim[*], Asif Aziz[**], Irfan Ahmed Usmani [***], Umair Uddin Shaikh[****], Safdar Rizvi[**]

[*]Department of Computer Science and Information Technology, Sir Syed University of Engineering & Technology, Karachi, Pakistan
[**] Computer Science Department, Bahria University Karachi Campus, Karachi, Pakistan
***Department of Telecommunication Engineering, Sir Syed University of Engineering & Technology
****School of Computer Science, Institute of Business Administration, Karachi, Pakistan

Abstract- Online social networking sites (SNS) have grown very fast for the last two decades. People share nothing with everything on these online social networks, and most users seem unaware of the privacy issues that these social networking sites can pose. Reviews of previous literature on information privacy stressed the importance of empirically evident factors affecting information privacy concerns. This paper aims to explore the factors of the information privacy concerns affecting the SNS. users. Three factors are identified, and a ten-item questionnaire is designed based on the previous literature. We selected users with more than three years of Facebook experience and executed a pilot test of 50 users confirming the reliability. We validated the identified factors as an enabler of information privacy concern for a population of 500 experienced Facebook users.

Index Terms- Social Networking Sites, Information Privacy, Information Privacy Concerns, Privacy Awareness, Facebook.

I. Introduction

Social Networking Sites (SNS.) are considered very convenient platforms to get in touch with friends, family, colleagues, and even people with similar interests. With the advent of Smart Phones, SNS. are gaining popularity each following day, and because of the appealing services they offer, people are becoming part of these SNS. at a very growing rate. However, the ever-increasing popularity of SNS. has also given rise to various forms of threats associated with profiling and data sharing over these platforms.

SNS. are web-based services that provide ways to their members to create and publish a profile regarding their identifications, share information with other members and allow them to navigate through the list of connections (of members) with which they are connected [1]. The SNS. users can perform these actions on a wherever and whenever basis. Examples of SNS. are Facebook, Twitter, LinkedIn, MySpace, Orkut, etc. Most SNS. users consider it necessary to spend a variable amount of time on these social networks. To stay in touch with their links and perform activities such as sharing status, posting photos, discussing events, products, and movies using these sites. These SNS. provides the user unrestricted access to social media but at the cost of Privacy [2].

The growing interest of people towards these sites has given rise to significant concerns about the Privacy of information. Though almost all SNS. provide some privacy policies about information usage, most SNS. users are unaware that their information can be exploited [3].

The current study focuses on Facebook due to its popularity among social media platforms globally, with over 2.80 billion active monthly users [4]. Still, with such growing popularity, it has a legacy of some privacy issues. On November 25, 2020, a South Korean company fined Facebook $6.06 million for sharing users' personal information without consent [5]. The Privacy International (the watchdog organization) has categorized Facebook as the second-lowest for "substantial and comprehensive privacy threats" due to its strict privacy-related flaws [6]. Frequently reported cases regarding malicious mischief on Facebook to include Manipulating user pictures, setting up fake user profiles, and publicizing information embarrassing for users to harass them [7-9]. A study of Facebook users' privacy awareness [10] has reported that despite more than 75 percent of participants' awareness of the privacy settings, only half incorporated those settings. Another similar study [11] has said that around 70 percent of users knew the Facebook privacy settings available, however, only 62 percent actually practiced those settings. Over time, the number of fields is observed to be grown in Facebook profiles. Additionally, default visibility settings changed to disclose more personal information to large audiences [3] between 2005 and 2014. Upgradation in privacy policy may confuse the user, affecting user behavior [12]. Facebook and other SNS. provide a significant level of indulgence and satisfaction to individuals. Research has reported continuous bargaining and tension between expected benefits and perceived privacy risks [13-15]. Ibrahim characterize online networks as a platform where social capital is generated, suggesting that using these platforms information can be traded [13]. Social Networking Sites are example of such online networks. The literature on information privacy [16] identified the gap in research regarding the factors affecting information privacy concerns. It seems essential to investigate the changing dimensions of privacy concerns for SNS. users separately.

This study aims to explore the factors affecting the information privacy concerns from the perspective of the SNS. users. Among many other SNS., for the current study, we have drawn our focus to Facebook as it is the most popular social networking site used by millions of people to socialize online all over the globe [4].

II. CONCEPTUAL BACKGROUND (PRIVACY AND SNS)

Various notions of Privacy have been highlighted in the research literature. Such as "Privacy as a human right" [16], "Privacy as a commodity" [17] with the perspective of a cost-benefit calculus at both societal and individual levels, "Privacy as a state" of limiting access to information [18], "a state of being apart from others" as defined by Weinstein [19] and "Privacy as Control" as reflected in the theories of general Privacy [20] [18]. Margulis [21, 22] has presented a control-centered definition of "general privacy," combining the views of Westin & Altman, as "Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability [21]".

Given [23], the concept of Privacy "is in disarray" despite being researched for so many years. Xu et al. in [24] have identified "Information Privacy Concern" as a fundamental construct in Information Systems research that can be used as an alternate way to define the concept of "Information Privacy." Many scales have been developed to rationalize this concept, like "Concern for Information Privacy (C.F.I.P.)" established by [25], "Internet User Information Privacy Concern (I.U.I.P.C.)," a multidimensional scale developed by [26]. However, the literature on information privacy revealed the low utilization of the I.U.I.P.C. scale in the current research. It stressed the requirement of more specific "Information Privacy Concern" measurements in diverse contexts [27]. Such an acknowledgment calls upon the re-investigation of the privacy concern scale in light of the emerging technologies, current practices, and research as suggested by [28].

Specific Privacy concerns of SNS. users include unintended disclosure of personal information, damaged reputation due to rumors and gossip, unnecessary contact and harassment or nuisance, surveillance like structures due to historical information and backtracking functions, use of personal information by third parties (secondary use of data), and identity thefts & hacking [1].

Privacy concerns outlined above are confirmed by various studies and reported on Facebook. As part of this research, we have specifically focused on the issues related to Privacy on Facebook because of the vast and growing number of users and its popularity as one of the most used social networking sites in today's world [4].

A. Information Boundary Theory (I.B.T.)

Information boundary theory puts together the social aspects associated with information disclosure. It recognizes that each individual form physical or virtual informational space around her, with well-defined boundaries." Boundary Opening" can be seen as the motivation to disclose or reveal information. Subsequently, "Boundary Closing" can be seen as the motivation to retain or withhold information. This boundary opening and closing is governed by specific rules [29]. These rules are composed of dynamic psychological processes affected by the nature of the relationship, the expected use of disclosed information, and the benefits associated with disclosing information [29].

This view of I.B.T. is consistent with the SNS. user's perception of disclosing information over these sites, the relationship status with other users, and conditions that influenced this disclosure of information. These conditions "depend in part upon the status of the relationship between the sender and the audience (individual or institutional) receiving it [30]," which highlights the context-specific nature of these conditions. Hence, for SNS. users, privacy-related behavior can be seen as a result of a situational and context-specific cost-benefit analysis of information disclosure [31-33].

B. Communication Privacy Management (C.P.M.) Theory

In [29], Petronio highlights the usefulness of C.P.M. theory in understanding the tension between data subjects (e.g., Facebook users) and data recipients (e.g., connections in SNS., SNS. vendors and/or application providers) concerning Privacy. C.P.M. theory "not only gives the option of examining personal privacy boundaries around an individual's information. But also allows for the notion of multiple privacy boundaries or collectively held private information [29]". C.P.M. makes a convincing ground for "co-management of private information" guided by boundary coordination process through collective control of both data subjects and data recipients over disclosed or revealed information [34]. C.P.M. is a rule-based theory that includes three boundary coordination rules [29] (Petronio 2002): permeability, ownership, and linkage. These rules "illustrate the modes of change for the dialectic of privacy-disclosure as managed in a collective manner" [29]. In case of failing to comply with these rules, Boundary Turbulence occurs in a collective manner [29], which in turn increases the privacy concerns of individuals.

In light of these theories, we identified three factors, i.e., Privacy Awareness, Privacy Experience, and Sense of Information Ownership, as primary factors contributing towards the Social Network Sites Users' Information Privacy Concerns (SNS.U.I.P.C.).

III. RESEARCH METHOD

Research constructs for Social Network Sites Users' Information Privacy Concerns (SNS.U.I.P.C.) are measured using the instrument with a five-point Likert Scale (see Appendix 1). Items used for the instrument were mainly adapted from the previous research (see Appendix 1) as long as possible with slight modifications to align them with SNS. users' concerns. The instrument used in this paper were designed with the help of fellow researchers and enthusiastic Facebook users.

A pilot study was conducted among 50 participants, including undergraduate and graduate-level students, research scholars, and teachers from two different universities in Pakistan to assess the clarity and conciseness related to the instrument used and evaluate the measurement model. A sub-group of these respondents (n = 10) were also interviewed for their opinions and feedback on the survey. We have invested considerable effort and time to present each item as precisely as possible, in easily understandable wording, without any confusion, and in line with the theoretical meaning associated with each dimension of privacy concern in the literature.

A. Survey Design

We are collecting data from students, research scholars, and teachers from the major universities in Pakistan. An increasing number of teaching and learning methodologies today make use of Facebook. "Facebook has quickly become a basic tool for and a mirror of social interaction, personal identity and network building among students [35]". Therefore, students and teachers naturally become part of our interest population. We are only collecting data from the users who have used Facebook for more than three years. The recruitment material presented some lines of background information about the survey and its intended use, deliberately not disclosing too many details. We have planned to survey around 500 participants using Facebook for more than three years.

B. *Data Analysis Strategy*

The planned data analysis is divided into two main tasks. Task 1 is about identifying the factor structure for SNS.U.I.P.C., and Task 2 is about establishing the nomological validity of SNS.U.I.P.C.

For Task 1, we have decided to establish the proper factor structure of SNS.U.I.P.C. since this construct has been developed using the existing items found in previous literature with slight modifications. Following the procedure presented by [26], to establish privacy measurement, firstly, we have performed an exploratory factor analysis (E.F.A.) of the identified factors of SNS.U.I.P.C., to be followed by confirmatory factor analysis (C.F.A.), once the data gathering phase will be completed. We have conducted E.F.A. using the Principal Component Analysis (P.C.A.) technique with VARIMAX rotation on the pilot data. All items loaded cleanly on their respective constructs with no cross-loadings. Convergent Validity Assessments were performed by examining the reliability measures, that is, Cronbach Alpha for each factor and found to be more than 0.70 for all constructs, as shown in Table 1, which satisfies Nunnally's criteria for convergent validity [36].

For Task 2, we have decided to test the construct of SNS.U.I.P.C. for nomological validity after completing C.F.A. from Task1, following the [28].

IV. CONCLUSION & FUTURE WORK

This study aims to answer the rising need to understand SNS. users' information privacy concerns. Privacy issues in such context become very important where large amounts of data and personal information get shared between the data subjects and data recipients, negotiating the boundaries of personal information disclosure. Yet, few studies have been conducted for identifying privacy concerns for SNS. users. This study is intended to examine SNS. users' information privacy concerns by extending the literature already present for Internet users' privacy concerns to this new dynamic face of social networking sites.

Future research concentrates on implementing machine learning-based algorithms to have a deeper analysis of the concerns regarding information privacy.

APPENDIX

Privacy Experience (PExp) – Smith et al. 1996

PExp1	Personal Information misuse of any of my contacts on Facebook makes me more concerned about my own Privacy on Facebook.
PExp2	Any incident of online Information Privacy misuse, even other than Facebook, makes me concerned about my own Privacy on Facebook.

Privacy Awareness (PAware) – Xu et al. 2008

PAware1	I am fully aware of the policy issues and practices adopted by Facebook regarding personal information usage.
PAware2	I am well aware of the measures taken by Facebook to ensure my Privacy.
PAware3	I keep myself updated about privacy issues on Facebook.
PAware4	I feel that because of my Facebook presence, others know more about me than I am comfortable with.

Sense of Information Ownership (S.I.O.) – Smith et al. 1996, Xu et al. 2008

SIO1	I believe that my personal information on Facebook is readily available to others more than I would want it to be.
SIO2	I am concerned that F.B. may share my personal information with other entities, without my permission.
SIO3	I feel that Facebook use makes my personal information available to others which, if used unwantedly, will invade my Privacy.
SIO4	I am concerned that my personal information available on Facebook may be used by Facebook for other purposes.

REFERENCES

[1] Boyd, D.M. and Ellison, N.B., 2007. Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1), pp.210-230.

[2] Srinivasan, D., 2019. The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. Berkeley Bus. LJ, 16, p.39.

[3] Acquisti, A., Brandimarte, L. and Loewenstein, G., 2015. Privacy and human behavior in the age of information. Science, 347(6221), pp.509-514.

[4] Facebook (2021) Company information. https://newsroom.fb.com/company-info/.

[5] South Korean watchdog fines Facebook $6.1 million for sharing user info without consent. 2020: https://tribune.com.pk/story/2273518/south-korean-watchdog-fines-facebook-61-million-for-sharing-user-info-without-consent.

[6] A race to the bottom: Privacy ranking of internet service companies, 2007; Privacy International: http://www.privacyinternational.org/issues/internet/interimrankings.pdf

[7] Kessler, T.R., 2007. Internet ‘joke’lands UNH student in trouble. citizen.com.

[8] Maher, M., 2007. You've got messages: modern technology recruiting through text-messaging and the intrusiveness of facebook. Tex. Rev. Ent. & Sports L., 8, p.125.

[9] Unsafe Internet habits can lead stalkers to your door. Retrieved: 22 Sep.2007. http://www.dailynebraskan.com/home/index.cfm?event=displayArticlePrinterFriendly&uStoryid=7926276f-6141-430a-b417-32b71c7da93a.

[10] Govani, T. and Pashley, H., 2005. Student awareness of the privacy implications when using Facebook. Unpublished paper presented at the "Privacy poster fair" at the Carnegie Mellon university school of library and information science, 9, pp.1-17.

[11] Jones, H. and Soltren, J.H., 2005. Facebook: Threats to privacy. Project MAC: MIT Project on Mathematics and Computing, 1(01), p.2005.

[12] Wijoyo, H., Limakrisna, N. and Suryanti, S., 2021. The effect of renewal privacy policy whatsapp to customer behavior. *Insight Management Journal*, 1(2), pp.26-31.

[13] Ibrahim, Y., 2008. The new risk communities: Social networking sites and risk. *International Journal of Media & Cultural Politics*, 4(2), pp.245-253.

[14] Tufekci, Z., 2008. Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), pp.20-36.

[15] Tyma, A.W., 2007. Rules of interchange: Privacy in online social communities–A rhetorical critique of MySpace. com. *Journal of the Communication, Speech & Theatre Association of North Dakota*, 20, p.31.

[16] Smith, H.J., Dinev, T. and Xu, H., 2011. Information privacy research: an interdisciplinary review. *MIS quarterly*, pp.989-1015.

[17] Bennett, C.J., 1995. The political economy of privacy: a review of the literature. Hackensack, NJ: Center for Social and Legal Research.

[18] Westin, A.F., 1968. Washington and Lee Law Review Privacy And Freedom. Lee L. Rev, 166(1).

[19] Weinstein, W.L., 2017. The private and the free: A conceptual inquiry. *In Privacy & Personality* (pp. 27-55). Routledge.

[20] Altman, I., 1975. The environment and social behavior: privacy, personal space, territory, and crowding.

[21] Margulis, S.T., 1977. Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), pp.5-21.

[22] Margulis, S.T., 1977. Privacy as a behavioral phenomenon. *Journal of Social Issues Ann Arbor*, Mich, 33(3), pp.1-195.

[23] Solove, D.J., 2005. A taxonomy of privacy. U. Pa. l. Rev., 154, p.477.

[24] Xu, H., Dinev, T., Smith, J. and Hart, P., 2011. Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, 12(12), p.1.

[25] Smith, H.J., Milberg, S.J. and Burke, S.J., 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly*, pp.167-196.

[26] Malhotra, N.K., Kim, S.S. and Agarwal, J., 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research*, 15(4), pp.336-355.

[27] Bélanger, F. and Crossler, R.E., 2011. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly*, pp.1017-1041.

[28] Stewart, K.A. and Segars, A.H., 2002. An empirical examination of the concern for information privacy instrument. *Information systems research*, 13(1), pp.36-49.

[29] Petronio, S., 2002. Boundaries of privacy: Dialectics of disclosure. Suny Press.

[30] Stanton, J.M. and Stam, K.R., 2003. Information technology, privacy, and power within organizations: A view from boundary theory and social exchange perspectives. Surveillance & Society, 1(2), pp.152-190.

[31] Acquisti, A. and Grossklags, J., 2005. Privacy and rationality in individual decision making. IEEE security & privacy, 3(1), pp.26-33.

[32] Culnan, M.J. and Armstrong, P.K., 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization science, 10(1), pp.104-115.

[33] Dinev, T. and Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. Information systems research, 17(1), pp.61-80.

[34] Petronio, S., 2010. Communication privacy management theory: What do we know about family privacy regulation?. Journal of family theory & review, 2(3), pp.175-196.

[35] Debatin, B., Lovejoy, J.P., Horn, A.K. and Hughes, B.N., 2009. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of computer-mediated communication, 15(1), pp.83-108.

[36] Nunnally, J.C. and Bernstein, I.H., 1978. Psychometric Theory McGraw-Hill New York. The role of university in the development of entrepreneurial vocations: a Spanish study, pp.387-405.

AUTHORS

First Author – Shakir Karim Buksh, MS in Computer Science, Sir Syed University of Engineering and Technology, Karachi, Pakistan. email: skbux@ssuet.edu.pk.

Second Author – Asif Aziz, PhD, Bahria University Karachi Campus, Karachi, Pakistan. email: asifaziz.bukc@bahria.edu.pk.

Third Author – Irfan Ahmed Usmani, M.Sc. in Communication Technology, Sir Syed University of Engineering and Technology, Karachi, Pakistan. email: iausmani@ssuet.edu.pk

Fourth Author – Umair Uddin Shaikh, Institute of Business Administration, Karachi, Pakistan. email: ushaikh@iba.edu.pk

Fifth Author – Safdar Rizvi, PhD, Bahria University Karachi Campus, Karachi, Pakistan. email: safdar.bukc@bahria.edu.pk.

Correspondence Author – Shakir Karim Buksh, MS in Computer Science, Sir Syed University of Engineering and Technology, Karachi, Pakistan. email: skbux@ssuet.edu.pk.