HOW DO USERS ENGAGE ON A PRIVACY-BASED SOCIAL NETWORKING APP?

Mehrdad Koohikamali, College of Business Administration, California State Polytechnic University, Pomona, 3801 W Temple Ave, Pomona, CA 91768, mkoohikamali@cpp.edu

Dan J. Kim, College of Business, University of North Texas, Dan.Kim@unt.edu

Aaron French, College of Business, Kennesaw State University, afrenc20@kennesaw.edu

ABSTRACT

On social networks, users have different ways to interact with each other and engage. If people's identity is hidden or they do not self-disclose their information, engagement becomes difficult. This study proposes a research model to investigate triple trade-off between anonymity, disclosure, and privacy on a new privacy-based social network application. We used a combination of survey method (at two stages) and actual mobile app data to test the proposed model. Results indicate a negative relationship between anonymity and privacy concern. Surprisingly while perception of engagement is increased with anonymity, actual engagement is negatively influenced by anonymity.

Keywords: Anonymity, Disclosure, Privacy, Engagement, Social Networking App.

INTRODUCTION

People spend more than one third of their wake time or more than 4 hours on mobile applications (apps) as of 2021 (Sydow, 2022). The highest percentage of time spent on mobile apps is for gaming, finance, and social networking applications (SNAs). Adoption and usage of SNAs is recognized in many studies and prior research investigates how users' intentional behaviors form and shift using popular SNAs. Self-disclosure, intention to adopt, and continuance intention variables are among the more explored variables in the previous research (Ku et al., 2013). Prior literature is grouped into two main categories: the first group of research focuses on the motivations and deterrents behind using social media and the second group of research investigates consequences of using social media. Recent research considers two-sided trade-offs when investigating how users utilize new technologies. Study shows trade-offs between desire for safety and requirement for privacy can motivate older adults to use health monitoring technologies (Ehrari et al., 2020).

When people deal with sensitive and personal information, they become more cautious and think about the consequences of disclosing such data. As a result, many use and have more than one social networks to protect their privacy, identity, and propriety (Stutzman et al., 2012). In addition, people adopt and migrate to new social networks specially to keep their perceived anonymity (Gerhart & Koohikamali, 2019) and more conveniently share content and feel safe. There are several positive consequences of anonymity such as free expression of ideas and privacy protection (Davenport, 2002). In the social media running context the positive influence of usage on engagement is proven, however engagement is lower when people have higher concerns for

privacy (Staddon et al., 2012). With the exception of separating real identity from a social media identity (Gross et al., 2005), people begin engaging and as a result may disclose personal information. This is counter intuitive to anonymity.

There are several gaps in the previous Information Systems (IS) research that this study plans to address. There is a gap about the triple trade-offs between anonymity, disclosure, and privacy (ADP) on SNAs and this study considers the triad when investigating usage behavior. The second gap is to focus on a new privacy-based SNA instead of popular application to see how actual engagement of user is formed and influenced by the triple trade-off. These gaps in the literature lead this research to tackle the following research questions: (1) how perceived anonymity and self-disclosure depth influence privacy concern in a social networking app context? (2) what is the influence of ADP on perceived and actual engagement? (3) what is the relationship between actual engagement and perceived engagement on a new SNA? Objectives of this research are two-fold: i) developing a research model to explain the trade-off between anonymity, disclosure, and privacy on a new SNA; ii) analyzing the relationship between ADP and engagement on a new SNA.

LITERATURE REVIEW

Social Networking and Engagement

The feeling that a technology has caught a user's interest is defined as engagement with the IT (Webster & Ahuja, 2006). Engagement with computer-mediated activities is a desirable human response and it is an important indicator of its success that grounds for re-use of the system (Bano & Zowghi, 2015). (O'Brien & Toms, 2008) study provide the conceptual framework for user engagement with technology. Engagement is defined as a "quality of user experience characterized by attributes of challenge, positive affect, durability, aesthetic and sensory appeal, attention, feedback, variety/novelty, interactivity, and perceived user control" (O'Brien & Toms, 2008). Initial mobile app engagement is generated after people use the app and acquire the initial experience (Dinner et al., 2015). Engagement on SNAs can be defined as a social interaction with other users by liking, commenting, or sharing information (Chu & Kim, 2011), engagement with a social networking app could have two aspects: first, engagement with individuals on the social network and second, engagement with the app and its functionalities. On SNAs, people build their engagement over a period of time (O'Brien & Toms, 2010).

There are four modes of SNA engagement: information seeking activity, connectivity, bricolage, and participation (Takahashi, 2010; Tian, 2015). First, the extent to which information users look up for specific/various types of information via a SNA is information seeking activity (Anderson et al., 2013; Takahashi, 2010). Second, the most important mode of SNA engagement is connectivity and it is defined as the ability to virtually connect to almost anyone on the SNA (Takahashi, 2010). Connectivity provide opportunities of interaction with people and information (Takahashi, 2010). Third, bricolage is the third mode of SNA engagement which it allows image creation and impression management (Takahashi, 2010).. Through bricolage SNA users are able to create/re-create their identity management (Deuze, 2006; Takahashi, 2010). Fourth, participation mode of SNA engagement is defined as online activities that people are involved in (Deuze, 2006; Literat, 2016). In this study, actual engagement is measured by participation and connectivity modes.

Engagement is a dynamic construct that matures during a user's experience and use of a technology. Engagement with technology is a four-staged process: point of engagement, the period of sustained engagement, disengagement, and reengagement (O'Brien & Toms, 2008). Engagement with SNAs positively influences satisfaction (Imlawi & Gregg, 2014). In addition, self-disclosure behavior is positively related with engagement with SNAs. Engagement has a positive effect on future use of a system (Webster & Ahuja, 2006). Continued engagement is a post-adoption behavior (Bhattacherjee, 2001). The ubiquitous feature of smartphones makes them to be always available to increase user engagement and ultimately the continued use behavior (Kim et al., 2013; Koohikamali et al., 2020).

Anonymity, Self-Disclosure, and Privacy Concern

Anonymity on SNAs is known as an inability to identify content generator of a message (Hayne & Rice, 1997; Pinsonneault & Heppel, 1997). There are two types of anonymity on the internet: the technical anonymity and the social anonymity (Kiesler et al., 1984). In general, anonymity expected to lessen inhibition by reducing fear of social disapproval, censorship, and evaluation (Pinsonneault & Heppel, 1997). Representing the real identity and publicly posting personal information on SNAs could cause serious negative consequences to the user such as privacy invasion (Gross et al., 2005). As a result, many individuals seek anonymity and pretense different levels of identifiability on different SNAs (Gross et al., 2005). For example, on a professional SNA people may use their real names and instead they use fake names on a dating SNA to create a sense of anonymity to other users (Gross et al., 2005). The relationship between self-disclosure and privacy concern is weak if the provided information is not truthful, fake, or not personally identifiable. Thus, the role of perceived anonymity becomes crucial to better understand self-disclosure and social interactions.

Self-disclosure happens when a user shares information about him/her (Green et al., 2016; Koohikamali et al., 2017). Previous works have examined the relationship between self-disclosure behavior and its antecedents/consequences. Privacy concern is shown to be a significant predictor of users' decisions to disclose personal information (Zimmer et al., 2010). Recent research shows usage experiences positively influence self-disclosure (Trepte & Reinecke, 2013). Self-disclosed information are different in amount, honesty, intent, depth, and valence (Posey et al., 2010). Self-disclosure depth reflects intimacy in the communications (Posey et al., 2010). Depth of disclosed information is details of it (French & Read, 2013). On SNA, depth of self-disclosed information varies due to heterogeneity of audience and relationship differences (French & Read, 2013). Depth of information can range from very general (low depth) to very specific (high depth) (French & Read, 2013). According to the social penetration theory, the developmental process of interpersonal relationship is primarily based on self-disclosure (Altman & Taylor, 1973; Carpenter & Greene, 2015). People tend to share more information on SNAs with anonymous strangers compared to individuals who know them (Gross et al., 2005).

In the previous research, privacy concern is shown to be an important factor in usage of SNAs. Concerns for information privacy has been growing since 1960s (Dinev et al., 2015). Information privacy is the amount of information that an individual chooses to share with others (Westin, 2003). Personal information privacy is the optimal level of control over personal information (Malhotra et al., 2004). Privacy concern could determine the information sharing and relationship buildings on SNAs as two SNAs' post-adoption behaviors (Dwyer et al., 2007). Further, research shows privacy concerns on SNAs are cultivated by initial use experiences of users (Boyd &

Ellison, 2007). Privacy concerns could decrease the use of SNAs among users (Ku et al., 2013). Research demonstrates the inconsistencies between users' perception of privacy concern and their actual behavior (Jiang et al., 2013). To take advantage of SNA capabilities, users inevitably need to self-disclose and face privacy risks. Behaviors such as customization of messages, using pseudo-identities, and controlling flow of information are some means of protecting privacy. Thus, studying privacy concern on social networks should accompanied by consideration of users' disclosure behavior and their perception of anonymity.

THEORETICAL BACKGROUND AND MODEL DEVELOPMENT

Engagement with technologies enable organizations, developers, and businesses to build and maintain relationship with users and customers (Chu & Kim, 2011). Recent studies in the area of human-computer interaction (HCI) have moved beyond the use and usefulness of systems and there are new efforts is to understand and enhance actual engagement with a technology (Hassenzahl & Tractinsky, 2006). Engagement is a desirable response to a technology and it includes intrinsic interest (Imlawi & Gregg, 2014). SNAs permit users to engage in interactive and dynamic social interactions (Chu & Kim, 2011). Understanding privacy concerns in a new context, such as a new SNA, requires a thorough understanding of the type and amount of personal information a user choose to disclose. We argue, when a user tries a new SNA for the first type without giving access to his personal information and sharing a content the conceptualization of privacy concern in that context should differ from his/her information privacy concern on an old SNA with a huge number of shared contents. In addition, if a person chooses to use a built-up identity to disclose untruthful personal information the privacy concern is not the same as disclosing real identities. This study applies the contextual integrity of privacy as the theoretical underpinning to explain the situations in which users disclose different depths of their information on a SNA.

Contextual integrity recognizes the importance of social systems on people's reactions and the framework of contextual integrity accounts social determinants (Nissenbaum, 2004). Users in SNAs facing two distinct privacy issues: the apparent issue which is about the abandon of confiding personal information to profiles on SNAs and the insidious issue about how social media companies handle users' information (Nissenbaum, 2004). Nissenbaum continues that social network sites are a medium of interaction, transaction, informtion exchange, and communication. Nissenbaum argues that exnension of information on SNAs to a diverse variety of social contexts is inevitable. On social networks, there are different spheres for people (such as public vs. private) and users have different norms to disclose their information to each sphere (Grodzinsky & Tavani, 2010). Within different contexts individuals may have different roles that derive particular activities (Sar & Al-Saggaf, 2014). Activities within a context are oriented around values that are governed by behavior-guiding norms (Sar & Al-Saggaf, 2014).

Regarding the flow of information in social contexts, (Nissenbaum, 2004) demonstrates that paying attention to the complex norms explain how users of SNAs post information under certain context-relative information norms. On SNAs, individuals establish and manage the boundaries of various spheres (e.g. public vs. private) by applying different mechanisms such as anonymity, deception, dissimulation (Acquisti et al., 2015). Consequently, our study considers the influence of perception of self-anonymity and self-disclosure depth on how people experience uncertainty about being concerned about their privacy. To assess the relationships between perceived self-anonymity, self-disclosure depth, privacy concerns, and engagement with a SNA this study

proposes a research model (Figure 1) and present the following hypotheses. Perceived self-anonymity and self-disclosure depth are captured at the beginning stage of using a new SNA and other constructs are at the continued usage stage.

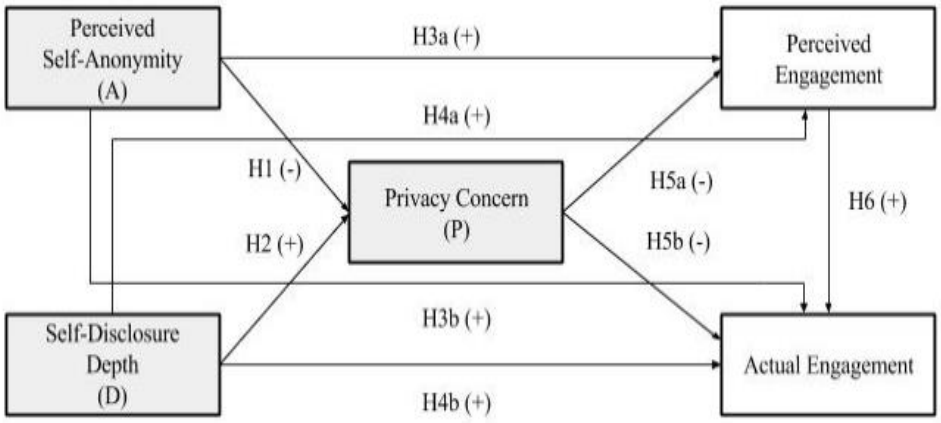

Figure 1. Proposed ADP model

One of the unique characteristics of online communications is the perceived anonymity for users (Cho & Kim, 2012). Anonymity ensures a user that his/her identity is not observable, identifiable, and linkable by other users (Pfitzmann & Köhntopp, 2001). Research shows the presence of anonymity in communication influences the type of content being shared. Individuals' perceptions of anonymity result in unregulated behavior and less concern about self-image (Sproull & Kiesler, 1986). Behaviors of anonymous individuals could become more extreme and impulsive (Sproull & Kiesler, 1986) and it may leads to privacy violations (Cho & Kim, 2012). On social networks, individuals who perceive to be anonymous may experience deindividuation (Jiang et al., 2013). As a result of deindividuation, users have less concern for self (Postmes & Spears, 1998). Individuals who perceive themselves unidentifiable on social networks have a greater sense of protection, and higher feel of immunity, and lesser concern for privacy (Jiang et al., 2013). Considering above discussion, this study suggests:

H1: Perceived self-anonymity negatively influences privacy concern.

Self-disclosure is defined as any information one user shares with others (Krasnova et al., 2010). Self-disclosed information differs in amount, honesty, depth, intent, and valence (Posey et al., 2010). The negative influence of privacy concern on self-disclosure intentions have been discussed broadly in the previous literature (Bansal et al., 2010). Privacy paradox argues that the actual behavior of users to disclose their information is not always the same as their intentions (Norberg et al., 2007). Users' sense of personal privacy deteriorate as they actually disclose their information (Norberg et al., 2007). People disclose personal information to gain benefits (Bansal et al., 2010). For example, on SNAs people self-disclose to foster their relationships (Posey et al., 2010). Self-disclosure depth is related to sharing of intimate and detailed personal information in communications (French & Read, 2013; Posey et al., 2010). When the personal informaiton is dislcosed, it may be misused and cause unwanted consequences (Bansal et al., 2010). Disclosing certain types of personal informaiton such as more intimate personal health information could cause greater undesirable outcomes (Bansal et al., 2010; Hui et al., 2007). This research argues when people initially use a new system and they disclose their intimate personal information, their

concern for privacy may increase due to higher vulnerabilities to future risks. Thus, this research proposes:

H2: Self-disclosure depth is positively related to privacy concern.

On SNAs staying relatively anonymous to other users is not difficult because people could use made-up or fake names instead of their real names (Byrne, 2007). The inherent psychological comfort as a result of perceived anonymity increases the level of involvement in online environments (Bell, 2001). Using SNAs and creating content has become a means of managing identity (Livingstone, 2008). Online identify might be shaped in relation to other users of the social network and many may seek confidentiality when disclose their personal information(Livingstone, 2008). Furthermore, ways of enacting identity on SNAs vary significantly and many users refrain to self-portray and instead render the personal profile as a place-maker (Livingstone, 2008). A key aspect of user-generated content on online websites such as social networks is anonymity (Scott & Orlikowski, 2014). Anonymity is the lack of identification that decreases inhibition (Posey et al., 2010). Perception of anonymity allows users to feel comfortable when sharing personal information (Lea & Spears, 2001). Disinhibition occurs is caused by public and private self-awareness as two main subjective states (Pinsonneault & Heppel, 1997). Individuals with higher perceptions of anonymity would experience greater disinhibition and as a result of disinhibition individuals feel free to perform public behaviors (Bansal et al., 2010). Additionally, Scott and Orlikowski (2014) demonstrate the elective form of anonymity makes users to engage more with Trip Advisor, a famous social networking website, due to their perceptions of being unidentifiable. Findings of the study by Ayyagari et al. (2011) suggest individuals' engagement with a technology is accompanied by strain over unintended consequences. So, this study suggests:

H3a: Perceived anonymity positively influences perceived ongoing engagement with SNAs.

H3b: Perceived anonymity positively influences actual ongoing engagement with SNAs.

SNA users can engage in various ranges of activities. (Takahashi, 2010) investigates modes of SNA engagement. Findings of (Takahashi, 2010) suggests information seeking activity, connectivity, bricolage, and participation as four main modes of SNA engagement. Among modes of SNA engagement, connectivity and participation are related with the interaction among users which is the most important aspect of using SNAs. Connectivity and participation modes of engagement are accessible through content sharing. Research shows disclosure of personal information is a predictor of engagement on social networks (Liau et al., 2005). On social networks, to reduce uncertainties between users in communications self-disclosure is a necessary element (Imlawi & Gregg, 2014). People use disclosed information on SNAs to get general understanding of other users which eventually yields to greater engagement with SNAs (Joinson et al., 2011). Self-disclosure stimulates feedback on social networks, and it improves engagement. This research argues when users provide more in depth of their personal information on a SNA, they show greater level of interest to engage with it. Thus, this study hypothesizes:

H4a: Self-disclosure depth is positively related with perceived engagement with SNAs.

H4b: Self-disclosure depth is positively related with actual engagement with SNAs.

Effective engagement with a technology is the result of factors such as users' experiences during the usage and users' expectations and values (Vasalou et al., 2015). Through the perspective of engagement theory, initial engagement with a technology is based on users' motivations (O'Brien & Toms, 2008). The key feature of engagement with a technology is control (O'Brien & Toms, 2008). Privacy risks usually hinders engagement with a technology (Vasalou et al., 2015). Individuals with high privacy concern usually perceive themselves unable of sufficient control

over their personal information. (Staddon et al., 2012) discusses the effect of privacy concern on engagement. Their findings show low engagement with social networks is the result of high privacy concerns. People who perceive higher concerns for their privacy consistently spend less time on social networks (Staddon et al., 2012). It suggests privacy concern is an important gate to engagement of users with social networks. Privacy concerns influences people's choice of engaging with the network and sharing content (Stutzman et al., 2012). This research proposes:

H5a: Privacy concern is negatively related with perceived engagement with SNAs.

H5b: Privacy concern is negatively related with actual engagement with SNAs.

IS literature provides many studies that support actual behavior and perceived behavior are not necessarily interchangeable (Barnett et al., 2015; Belanger & Xu, 2015). Moreover, self-reporting in complex situations is challenging (Barnett et al., 2015). It is arguable that engagement with a SNA constitutes many aspects that are not easily discernible for users. Consistent with prior research, this study investigates if actual engagement with a SNA predicts perceived engagement. Therefore, this research hypothesizes:

H6: Perceived engagement positively influences the actual engagement with SNAs.

RESEARCH METHODOLOGY

Through the lens of contextual integrity of privacy this study proposes a research model to explain the ongoing engagement with a new SNA. This research model attempts to examine the effect of initial perceived self-anonymity and self-disclosure depth on ongoing privacy concern and ongoing engagement with the SNA. A survey method is used to test the research model in two-stages: after using a SNA for the first time and after three weeks during the ongoing usage period. To test and verify the proposed research model, Sociabile app (a new SNA) was introduced to respondents, and they were asked to install the app to experience it for the first time (phase1, n1=196). Sociabile (social + mobile) was a new privacy-based SNA, which was available on iTunes and Google Play, and it is used for the current study. After 3-weeks respondents of the first phase were asked to participate in another survey about their ongoing usage experience of Sociabile during this period (phase 2, n2=119). Pre-validated measures are used to operationalize perceived anonymity (H.-G. Chen et al., 2008), perceived engagement with the SNA (Ellison et al., 2007; O'Brien & Toms, 2010), and privacy concern (H.-G. Chen et al., 2008). Self-disclosure depth is self-developed and defined as the ratio of number of specific fields user has filled over total fields. Measurement items are provided in the Appendix.

RESULTS

Following the two-step analytical approach suggested by (Hair et al., 2006), this study first evaluated the measurement model reliability and validity and then assessed the structural model. The partial least squares (PLS) was used to test the research model, because PLS employs a component-based approach for estimation that minimizes residual distributions (Chudnov, 2008), and is best suited for testing complex relationships by avoiding inadmissible solutions and factor indeterminacy (R. Chen et al., 2011). Assessment of the measurement model was a three-step analysis process including evaluating reliability of the measurement model, evaluating convergent validity, and ensuring discriminant validity. Results of the structural model analysis based on the proposed hypothesis is shown in Figure 2, including explained variance of dependent or dependent

variables, estimated path coefficients, and t-values. The PLS results indicate the structural model explains 10% of the variance in ongoing privacy concern, 29% of the variance in perceived engagement with a SNA, and 50% of the variance in actual engagement with a SNA. Analyzing significance of path coefficients reveal all paths are statistically significant except the relationship between privacy concerns and the perceived engagement, self-anonymity and actual engagement, and self-disclosure depth and privacy concern. Opposed to our hypothesized positive relationship between initial self-disclosure depth and ongoing perceived engagement and actual engagement (H4a, H4b), path coefficients were negative, failing to support H4a and H4b. Another initial interesting finding was about the positive effect of perceived self-anonymity on perceived engagement but lack of statistical support for actual engagement. Finally, previous literature has discussed the negative relationship between users' privacy concerns and engagement with a SNA, as users are more worried about the control over their personal information. Findings did not show a significant relationship between privacy concern and perceived engagement with a SNA, while the relationship was significant for actual engagement. One possible explanation is that on a privacy-based SNA that was introduced to users, people's perception regarding the protection of their information privacy is high and subsequently privacy concern. While privacy concern does not negatively influence their perception of engagement with the SNA, intuitively people with high privacy concerns are more worried about possible risks and exhibit lower actual engagement.

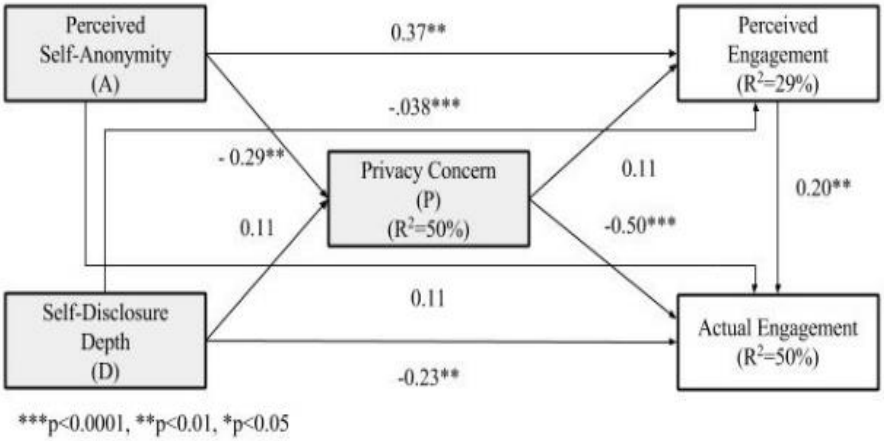

Figure 2. Structural model analysis

CONCLUSION

The most significant contributions of this study are divided into theoretical and practical perspectives. Although the relationship between privacy concern and self-disclosure is well-studied in the previous Information System (IS) literature, the lack of an integrated model to examine the relationship between anonymity, disclosure depth, privacy concern and how they influence engagement with a social networking app is the main motivation for this study. Theoretically, this study investigates a research model explaining engagement with a SNA during the continued use stage. This research is one of the few studies in the IS to investigate engagement to the SNA over a period of continued use and as a dependent variable through the lens of contextual integrity of privacy. Findings of this research can be extended in the future to better understand antecedents and consequences of engagement with a SNA. Second, the proposed research model is not merely based on perception of usage behavior and instead this research

examined the role of actual engagement with a new SNA. Including both perception and actual engagement is beyond the technology acceptance, and it extends the current mainstream body of IS research. This study could be useful in future studies examining success of a new system by incorporating engagement perceptions of users. Third, integration of perceived self-anonymity, self-disclosure depth, and privacy concern helped to shed light on the perplexities of information management on internet and specifically on online social networks. Results open up a new stream of research focusing on different types of information users disclose on various social networks. Practical contributions of this study can be discussed from the view of three groups. First, developers of new SNAs may consider users' initial perceptions of using social network apps to improve functionalities in the future versions. Second, practitioners may apply results of this study to increase users' engagement with a technology it. Third, users may apply the integration of self-anonymity and self-disclosure depth to evaluate the potential risks to their personal information privacy.

Overall, this study has examined the phenomena of engagement with a new SNA and triangle of anonymity, disclosure, and privacy concern (ADP) as it is not studied in the previous IS literature. This study proposes a new research model explaining engagement with a new SNA in the ongoing use stage. In addition, actual engagement with a new SNA as a post-adoption behavior is included and measured in this research to deepen understanding post-adoption of SNA. Privacy concern is not studied in accordance with perceived self-anonymity and self-disclosure depth. This model identifies self-anonymity, self-disclosure depth as predictor of privacy concern at later stage. As demonstrated by preliminary analysis, privacy concern is not related with perceived engagement, but it is related with actual engagement with a new privacy-based SNA. Finally, interestingly self-disclosure depth has a negative effect on engagement.

REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Altman, I., & Taylor, D. (1973). Social penetration theory. *New York: Holt, Rinehart &Winston*.

Anderson, A. a, Delborne, J., & Kleinman, D. L. (2013). Information beyond the forum: Motivations, strategies, and impacts of citizen participants seeking information during a consensus conference. *Public Understanding of Science (Bristol, England)*, *22*(8), 955–970.

Ayyagari, R., Grover, V., & Purvis, R. (2011). Technostress: Technological Antecedents and Implications. *MIS Quarterly*, *35*(4), 831–858.

Bano, M., & Zowghi, D. (2015). A systematic review on the relationship between user involvement and system success. *Information and Software Technology*, *58*, 148--169.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150.

Barnett, T., Pearson, A. W., Pearson, R., & Kellermanns, F. W. (2015). Five-factor model

personality traits as predictors of perceived and actual usage of technology. *European Journal of Information Systems*, *24*(4), 374–390. https://doi.org/10.1057/ejis.2014.10

Belanger, F., & Xu, H. (2015). Editorial The role of information systems research in shaping the future of information privacy. *Information Systems Journal*, 573–578.

Bell, M. (2001). Online role-play: Anonymity, engagement and risk. *Educational Media International*, *38*(4), 251–260.

Bhattacherjee, A. (2001). Understanding information systems continuance: an expectation-confirmation model. *MIS Quarterly*, *25*(3), 351–370.

Boyd, D. M., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210–230.

Byrne, D. N. (2007). Public discourse, community concerns, and civic engagement: Exploring black social networking traditions on BlackPlanet. com. *Journal of Computer-Mediated Communication*, *13*(1), 319–340.

Carpenter, A., & Greene, K. (2015). Social Penetration Theory. In *The International Encyclopedia of Interpersonal Communication* (pp. 1–4).

Chen, H.-G., Chen, C. C., Lo, L., & Yang, S. C. (2008). Online privacy control via anonymity and pseudonym: Cross-cultural implications. *Behaviour & Information Technology*, *27*(3), 229–242.

Chen, R., Wang, J., Herath, T., & Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems*, *52*(1), 73–81.

Cho, D., & Kim, S. (2012). Empirical Analysis of Online Anonymity and User Behaviors: The Impact of Real Name Policy. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3041–3050. https://doi.org/10.1109/HICSS.2012.241

Chu, S.-C., & Kim, Y. (2011). Determinants of consumer engagement in electronic word-of-mouth (eWOM) in social networking sites. *International Journal of Advertising*, *30*(1), 47–75.

Chudnov, D. (2008). Updates on pulsing content, unconferences, and coding. *Computers in Libraries*, *28*(8), 31–33. https://doi.org/Editorial

Davenport, D. (2002). Anonymity on the Internet: Why the Price May Be Too High. *Communications of the ACM*, *45*(4), 33–35. https://doi.org/10.1145/505248.505267

Deuze, M. (2006). Participation, remediation, bricolage: considering principal components of a digital culture. *The Information Society*, *22*(2), 63–75.

Dinev, T., McConnell, A. R., & Smith, H. J. (2015). Research Commentary—Informing Privacy

Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the "APCO" Box. *Information Systems Research*, *26*(4), 639–655.

Dinner, I., Van Heerde, H. J., & Neslin, S. (2015). *Creating Customer Engagement Via Mobile Apps: How App Usage Drives Purchase Behavior*.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas Conference on Information Systems*, 339.

Ehrari, H., Ulrich, F., & Andersen, H. B. (2020). Concerns and trade-offs in information technology acceptance: the balance between the requirement for privacy and the desire for safety. *Communications of the Association for Information Systems*, *47*, 227–247.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4), 1143–1168.

French, A. M., & Read, A. (2013). My mom's on Facebook: An evaluation of information sharing depth in social networking. *Behaviour and Information Technology*, *32*(10), 1049–1059.

Gerhart, N., & Koohikamali, M. (2019). Social Network Migration and Anonymity Expectations: What Anonymous Social Network Apps Offer. *Computers in Human Behavior*, *95*, 101–113.

Green, T., Wilhelmsen, T., Wilmots, E., Dodd, B., & Quinn, S. (2016). Social anxiety, attributes of online communication and self-disclosure across private and public Facebook communication. *Computers in Human Behavior*, *58*, 206–213.

Grodzinsky, F. S., & Tavani, H. T. (2010). Applying the "contextual integrity" model of privacy to personal blogs in the blogosphere. *International Journal of Internet Research Ethics*, *3*(1), 38–47.

Gross, R., Acquisti, A., & Iii, H. J. H. (2005). Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, 71–80.

Hair, J. F., Tatham, R. L., Anderson, R. E., & Black, W. (2006). *Multivariate data analysis* (Vol. 6). Pearson Prentice Hall Upper Saddle River, NJ.

Hassenzahl, M., & Tractinsky, N. (2006). User experience-a research agenda. *Behaviour & Information Technology*, *25*(2), 91–97.

Hayne, S. C., & Rice, R. E. (1997). Attribution Accuracy When Using Anonymity in Group Support Systems. *International Journal of Human-Computer Studies*, *47*, 429–452.

Hui, K.-L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: an exploratory

field experiment. *MIS Quarterly*, 19–33.

Imlawi, J., & Gregg, D. (2014). Engagement in online social networks: The impact of self-disclosure and humor. *International Journal of Human-Computer Interaction*, *30*(2), 106–125.

Jiang, Z., Heng, C. S., & Choi, B. C. F. (2013). Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions. *Information Systems Research*, *24*(3), 579–595.

Joinson, A. N., Houghton, D. J., Vasalou, A., & Marder, B. L. (2011). Digital Crowding: Privacy, Self-Disclosure and Technology. In *Privacy Online. Digital Crowding: Privacy, Self-Disclosure, and Technology* (pp. 33–45). Springer Berlin Heidelberg.

Junglas, I., Abraham, C., & Watson, R. (2008). Task-technology fit for mobile locatable information systems. *Decision Support Systems*, *45*(4), 1046–1057.

Junglas, I., Johnson, N., & Spitzmüller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, *17*(4), 387–402.

Kiesler, S., Siegel, J., & McGuire, T. W. (1984). Social psychological aspects of computer-mediated communication. *The American Psychologist*, *39*(10), 1123–1134.

Kim, Y. H., Kim, D. J., & Wachter, K. (2013). A study of mobile user engagement (MoEN): Engagement motivations, perceived value, satisfaction, and continued engagement intention. *Decision Support Systems*, *56*, 361–370.

Koohikamali, M., Mousavi, R., Peak, D. A., & Prybutok, V. R. (2020). Benefit Expectations and Continued Usage of Location-Based Applications for Location Intelligence. *Journal of Applied Business and Economics*, *22*(9). https://doi.org/10.33423/jabe.v22i9.3676

Koohikamali, M., Peak, D., & Prybutok, V. (2017). Beyond Self-Disclosure: Disclosure of Information about Others in Social Network Sites. *Computers in Human Behavior*, *69*, 29–42.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: why we disclose. *Journal of Information Technology*, *25*(2), 109–125.

Ku, Y.-C., Chen, R., & Zhang, H. (2013). Why do users continue using social networking sites? An exploratory study of members in the United States and Taiwan. *Information & Management*, *50*(7), 571–581.

Lea, M., & Spears, R. (2001). Knowing Me , Knowing You : Anonymity Effects on Social Identity Processes Within Groups. *Personality and Social Psychology Bulletin*, *27*(5), 526–537.

Liau, A. K., Khoo, A., & Hwaang, P. (2005). Factors influencing adolescents engagement in risky Internet behavior. *CyberPsychology & Behavior*, *8*(6), 513–520.

Literat, I. (2016). Interrogating participation across disciplinary boundaries: Lessons from political philosophy, cultural studies, art, and education. *New Media & Society*, *18*(8), 1461444816639036-. https://doi.org/10.1177/1461444816639036

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393–411.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash L. Rev.*, *79*, 101–139. https://doi.org/10.1109/SP.2006.32

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

O'Brien, H. L., & Toms, E. G. (2008). What is user engagement? A conceptual framework for defining user engagement with technology. *Journal of the American Society for Information Science and Technology*, *59*(6), 938–955.

O'Brien, H. L., & Toms, E. G. (2010). The development and evaluation of a survey to measure user engagement. *Journal of the American Society for Information Science and Technology*, *61*(1), 50–69.

Pfitzmann, A., & Köhntopp, M. (2001). Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. *Designing Privacy Enhancing Technologies*, *2009*, 1–9.

Pinsonneault, A., & Heppel, N. (1997). Anonymity in Group Support Systems Research: A New Conceptualization, Measure, and Contingency Framework. *Journal of Management Information Systems*, *14*(3), 89–108.

Posey, C., Lowry, P. B., Roberts, T. L., & Ellis, T. S. (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*, *19*(2), 181–195.

Postmes, T., & Spears, R. (1998). Deindividuation and antinormative behavior: A meta-analysis. *Psychological Bulletin*, *123*(3), 238.

Sar, R. K., & Al-Saggaf, Y. (2014). Contextual integrity's decision heuristic and the tracking by social network sites. *Ethics and Information Technology*, *16*(1), 15–26.

Scott, S. V, & Orlikowski, W. J. (2014). Entanglements in practice: performing anonymity through social media. *Mis Quarterly*, *38*(3), 873–893.

Sproull, L., & Kiesler, S. (1986). Reducing Social Context Cues: Electronic Mail in Organizational Communication. *Management Science*, *32*(11), 1492–1512.

Staddon, J., Huffaker, D., Brown, L., & Sedley, A. (2012). Are privacy concerns a turn-off?: engagement and privacy in social networks. *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 10.

Stutzman, F., Gross, R., & Acquisti, A. (2012). Silent Listeners: The Evolution of Privacy and Disclosure on Facebook. *Journal of Privacy and Confidentiality*, *4*(2), 7–41.

Sydow, L. (2022). *Consumers in Three Countries Now Spend More than 5 Hours a Day in Apps*. https://www.data.ai/en/insights/market-data/consumers-in-five-countries-now-spend-more-than-5-hours-a-day-in-apps/

Takahashi, T. (2010). MySpace or Mixi? Japanese engagement with SNS (social networking sites) in the global age. *New Media & Society*, *12*(3), 453–475.

Tian, X. (2015). Network domains in social networking sites: expectations, meanings, and social capital. *Information, Communication & Society*, *4462*(December 2015), 1–15. https://doi.org/10.1080/1369118X.2015.1050051

Trepte, S., & Reinecke, L. (2013). The reciprocal effects of social network site use and the disposition for self-disclosure: A longitudinal study. *Computers in Human Behavior*, *29*(3), 1102–1112. https://doi.org/10.1016/j.chb.2012.10.002

Vasalou, A., Oostveen, A. M., Bowers, C., & Beale, R. (2015). Understanding engagement with the privacy domain through design research. *Journal of the Association for Information Science and Technology*, *66*(6), 1263–1273.

Webster, J., & Ahuja, J. S. (2006). Enhancing the design of web navigation systems: the influence of user disorientation on engagement and performance. *MIS Quarterly*, *30*(3), 661–678.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.

Zhou, Z., Jin, X.-L., Fang, Y., & Vogel, D. (2015). Toward a theory of perceived benefits, affective commitment, and continuance intention in social virtual worlds: cultural values (indulgence and individualism) matter. *European Journal of Information Systems*, *24*(3), 247–261.

Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., & Grover, V. (2010). Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure. *Decision Support Systems*, *48*(2), 395–406.

APPENDIX. MEASUREMENT OF PRINCIPAL CONSTRUCTS

Construct	Item	Measurement Item	Reference
Privacy Concern	PC1	I am concerned that I am asked to provide my personal information on this app.	(Junglas, Abraham, et al., 2008; Junglas, Johnson, et al., 2008; Zhou et al., 2015)
	PC2	I am concerned [if/that] this app stores too much of my personal information.	
	PC3	I am concerned that there is the possibility of unauthorized access to databases that contain my information on this app.	
	PC4	I am concerned that unauthorized people can access my personal information on this app.	
	PC5	I am concerned that this app does not have thorough procedures to prevent errors in my personal information.	
	PC6	I am concerned that there are not enough features to double-check the accuracy of my personal information on this app.	
	PC7	I am concerned that this app uses my personal information for other purposes without getting my authorization.	
	PC8	I am concerned that this app shares my information without my consent.	
Self-Disclosure Depth	DD	Numbers of specific personal information disclosed (email, physical appearance, current workplace, etc.)/total number of disclosed personal information	Self-developed
Perceived Anonymity	ANON1	It is easy for me to hide my identity on this app.	(Ayyagari et al., 2011)
	ANON2	I can remain anonymous when using this app.	
	ANON3	It is easy for me to hide my usage of this app.	
	ANON4	It is difficult for others to identify my use of this app.	
Perceived Engagement with SNA	ENG1	I am engaged with it.	(Kim et al., 2013; O'Brien & Toms, 2008)
	ENG2	I recommend my engagement to someone else.	
	ENG3	I am really drawn into it.	
	ENG4	During my experience with it I let myself go.	
	ENG5	When I use it, I lose track of time.	
Actual Engagement	Connectivity	Number of friends they have connected to.	(Deuze, 2006)
		Number of friend requests sent to others.	
	Participation	Number of time capsules sent.	
		Number of My Mind messages posted.	
		Number of comments on posts by others.	