

Winter 12-13-2018

# Anonymity, Privacy, and Disclosure (APD) Triad on Social Networking Applications

Mehrdad Koohikamali  
*University of Redlands*

Dan J. Kim  
*University of North Texas*

Aaron M. French  
*University of New Mexico*

Follow this and additional works at: <https://aisel.aisnet.org/wisp2018>

---

## Recommended Citation

Koohikamali, Mehrdad; Kim, Dan J.; and French, Aaron M., "Anonymity, Privacy, and Disclosure (APD) Triad on Social Networking Applications" (2018). *WISP 2018 Proceedings*. 14.  
<https://aisel.aisnet.org/wisp2018/14>

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2018 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

## **Anonymity, Privacy, and Disclosure (APD) Triad on Social Networking Applications**

**Mehrdad Koohikamali<sup>1</sup>**

School of Business, University of Redlands,  
Redlands, California, United States

**Dan J. Kim**

College of Business, University of North Texas,  
Denton, Texas, United States

**Aaron M. French**

School of Management, University of New Mexico,  
Albuquerque, New Mexico, United States

### **ABSTRACT**

While the average time people spend on their mobile apps continues to increase, the life cycle of using new social networking apps (SNA) remains relatively short, mostly due to privacy concern. For SNA users, it is important to know how the perception of anonymity and privacy concern determine the depth of disclosed information. For many SNA developers and practitioners, understanding the actual engagement of users on the platform is critical for measuring success of the app. Previous research has evaluated motivations/preventions of app usage and consequences of continuing usage. Despite efforts to understand the engagement with mobile devices and other users, there is little work in the Information Systems (IS) field to simultaneously investigate the triad of anonymity, privacy concern, and disclosure (APD) on continuous engagement with SNAs. Through the lens of contextual integrity of privacy, this research proposes a research model to investigate APD relationships with perceived and actual engagements with a new SNA. The research model is tested using a survey and actual usage data captured from users' log files provided by mobile app developers. Results demonstrate how privacy is significantly related with actual engagement while anonymity relationship with actual engagement is fully mediated by perceived engagement.

**Keywords:** Privacy, anonymity, disclosure, engagement, social network apps

---

<sup>1</sup> Corresponding author. [Mehrdad\\_Koohikamali@redlands.edu](mailto:Mehrdad_Koohikamali@redlands.edu) +1 909 748 8032

## INTRODUCTION

Free expression of any idea and individual privacy protection are two primary positive outcomes of perceived anonymity in communications (Kern 2013). On a specific social network site (SNS), protection of personal information privacy is possible by separating real personal identity from identity on the SNS (Gross et al. 2005). Maintaining anonymity on some SNSs is one of the motivations for people use them (Gross et al. 2005). Continuous user engagement is one of the indicators of information technology success in the context of use (Chu and Kim 2011). In the prior research the positive influence of SNS usage on activity engagement is demonstrated (Mahan et al. 2015). While, engagement with the SNSs is lower for people with higher privacy concerns (Staddon et al. 2012), using fake identities or not disclosing personal information could change perception of privacy concerns.

On mobile apps more personal information is accessible and users are more exposed to privacy violations (Papadopoulos et al. 2017). Most IS research is focused on privacy issues on SNSs, but the extent to which people engage with a new social networking app (SNA) is not clear with previous research focused on the triad of anonymity, privacy, and disclosure falling short. Furthermore, the relationship between perceived engagement and actual engagement is less considered in the IS literature. These two gaps in the literature guide the current research to tackle the following research questions: (1) how perceived anonymity and privacy concern influence self-disclosure depth in a new SNA context? (2) How APD influences the perceived and actual engagement? (3) How perceived engagement could predict the actual engagement on a new SNA? To address these questions, this study focuses on three objectives: i) develop a new research model to explain the ongoing engagement on a new SNA; ii) empirically test the proposed model using both an actual engagement data and survey data collected from users of a

new SNA; and iii) provide theoretical and practical implications of this study. In this research, we focus on SNAs, and draw the related literature focused on SNSs to build the research model.

## 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 and 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 and Zowghi 2015). O'Brien and Toms (2008) study provide the conceptual framework for user engagement with technology. They define engagement 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 and Toms 2008, pp.938). Social networking engagement can be defined as a social interaction with other users by liking, commenting, or sharing information (Chu and Kim 2011). Engagement with a social networking app can be viewed by two aspects: first, engagement with individuals on the social network and second, engagement with the app and its functionalities.

There are four modes of social networking engagement: information seeking activity, connectivity, bricolage, and participation (Takahashi 2010; Tian 2015). In this study, actual engagement is measured by participation and connectivity modes. The most important mode of social networking engagement is connectivity, which is defined as the ability to virtually connect to almost anyone on the network (Takahashi 2010). Participation mode of social networking engagement is defined as online activities that people are involved in (Deuze 2006; Literat 2016). Continued engagement is a post-adoption behavior (Bhattacharjee 2001). The ubiquitous

nature of smartphones provides the ability to always be available to increase user engagement and ultimately the continued use behavior (Kim et al., 2007; Kim et al., 2013).

### **Anonymity, Self-Disclosure, and Privacy Concern**

Anonymity on social networks is known as an inability to identify content generator of a message (Hayne and Rice 1997; Pinsonneault and 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 is expected to lessen inhibition by reducing fear of social disapproval, censorship, and evaluation (Pinsonneault and Heppel 1997). Representing the real identity and publicly posting of personal information on social networks such as 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 social networks (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 research has 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 and 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), whereas depth of disclosed information reflects the details of it (French and

Read 2013). On social networks, depth of self-disclosed information varies due to heterogeneity of audience and relationship differences (French and Read 2013). Depth of information can range from very general (low depth) to very specific (high depth) (French and Read 2013).

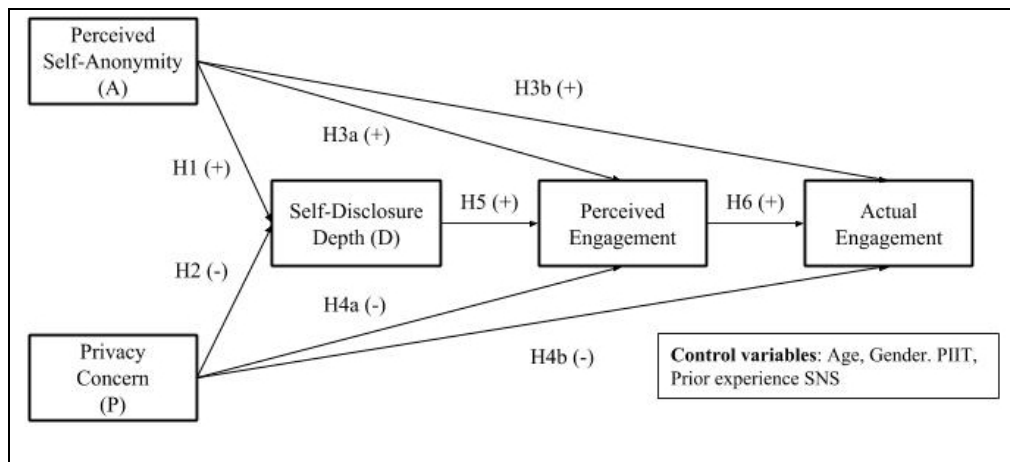
Finally, previous research identifies privacy concern as an important factor in social network use. Concerns for information privacy has been growing since 1960s (Dinev et al. 2015). Information privacy is the amount of information that an individual chooses to share with others (Westin 2003). Personal information privacy is the optimal level of control over personal information (Malhotra et al. 2004). Privacy concern could determine post-adoption behaviors such as the information sharing and relationship buildings on SNSs (Dwyer et al. 2007) and similarly on SNAs. Research demonstrates the inconsistencies between users' perception of privacy concern and their actual behavior (Jiang et al. 2013). Thus, studying privacy concern on social networks should be accompanied by the consideration of users' disclosure behavior and their perception of anonymity.

## **THEORETICAL BACKGROUND AND MODEL DEVELOPMENT**

This study applies the contextual integrity of privacy as the theoretical underpinning to explain the situations in which users disclose different depths of 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, pp.190). Users in SNSs facing two distinct privacy issues: the apparent issue which is about the abandon of confiding personal information to profiles on SNSs and the insidious issue about how social media companies handle users' information (Nissenbaum 2004, pp.221). Nissenbaum continues that social networks are a medium of interaction, transaction, information exchange, and communication. Nissenbaum argues that extensions of information on social networks to a

diverse variety of social contexts is inevitable. Correspondingly, SNAs creates a medium of interaction between users and exchange of information between them.

Regarding the flow of information in social contexts, Nissenbaum (2010) demonstrates that paying attention to the complex norms explain how users of social networks 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 perceived self-anonymity and privacy concern on self-disclosure depth. 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 privacy concern 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 and Kim 2012). Anonymity ensures a user that his/her identity is not observable, identifiable, and linkable by other users (Pfitzmann and Köhntopp 2001). Behaviors of

anonymous individuals could become more extreme and impulsive (Sproull and Kiesler 1986) and it may lead to privacy violations (Cho and Kim 2012). On social networks, individuals who perceive to be anonymous may experience deindividuation (Jiang et al. 2013) resulting in users have less concern for self (Postmes and Spears 1998). Individuals who perceive themselves as unidentifiable on social networks have a greater sense of protection, and higher feel of immunity, and lesser concern for privacy (Jiang et al. 2013), resulting in disclosing more information. Considering the above discussion, this study suggests:

***H1: Perceived self-anonymity positively influences self-disclosure depth.***

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 previous literature (Bansal et al. 2010). Self-disclosure depth is related to sharing of intimate and detailed personal information in communications (French and Read 2013; Posey et al. 2010). When the personal information is disclosed, it may be misused and cause unwanted consequences (Bansal et al. 2010). Disclosing certain types of personal information such as more intimate personal health information could cause greater undesirable outcomes (Bansal et al. 2010; Hui et al. 2007). This research argues privacy concerns decreases level of details people are willing to disclose. Thus, this research proposes:

***H2: Privacy concern is negatively related with self-disclosure depth.***

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). The inherent psychological comfort as a result of perceived anonymity increases the level of involvement in



online environments (Bell 2001). On social networks creating content has become a means of managing identity (Livingstone 2008). Online identity 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 and Orlikowski 2014). Perception of anonymity allows users to feel comfortable when sharing personal information (Lea and Spears 2001). 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). So, this study suggests:

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

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

Effective engagement with a technology is the result of factors such as users' experiences during 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 and Toms 2008). The key feature of engagement with a technology is control (O'Brien and Toms 2008). Privacy risks usually hinders engagement with a technology (Vasalou et al. 2015). Individuals with high privacy concern usually perceive themselves unable to sufficiently control their personal information. A study by 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). Hence, this research proposes:

*H4a: Privacy concern is negatively related with perceived engagement with SNAs.*

*H4b: Privacy concern is negatively related with actual engagement with SNAs.*

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 and Gregg 2014). People use disclosed information on social networks to get general understanding of other users which eventually yields to greater engagement with the network (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:

*H5: Self-disclosure depth is positively related with perceived engagement with SNAs.*

IS literature provides many studies that support the argument that actual behavior and perceived behavior are not necessarily interchangeable (Belanger and Xu 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 perceived engagement with a SNA predicts actual engagement. Therefore, this research hypothesizes:

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

## RESEARCH METHODOLOGY

Through the lens of framework of contextual integrity of privacy this study suggests a research model to explain the ongoing engagement with a new 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, a new app called Sociabile (a new privacy-based 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 was used for the current study. After 3-weeks, respondents of the first phase were asked to participate in a second survey about their ongoing usage experience of Sociabile during this period (phase 2, n2=119). Pre-validated measures are used to operationalize perceived anonymity (Chen et al. 2008), perceived engagement with the SNA (Ellison et al. 2007; O'Brien and Toms 2010), and privacy concern (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 use profile fields. Actual engagement was the sum of all possible connectivity and participation engagement features. Measurement items are provided in Appendix A. Subject demographics are displayed in Table 1.

**Table 1.** Demographic information

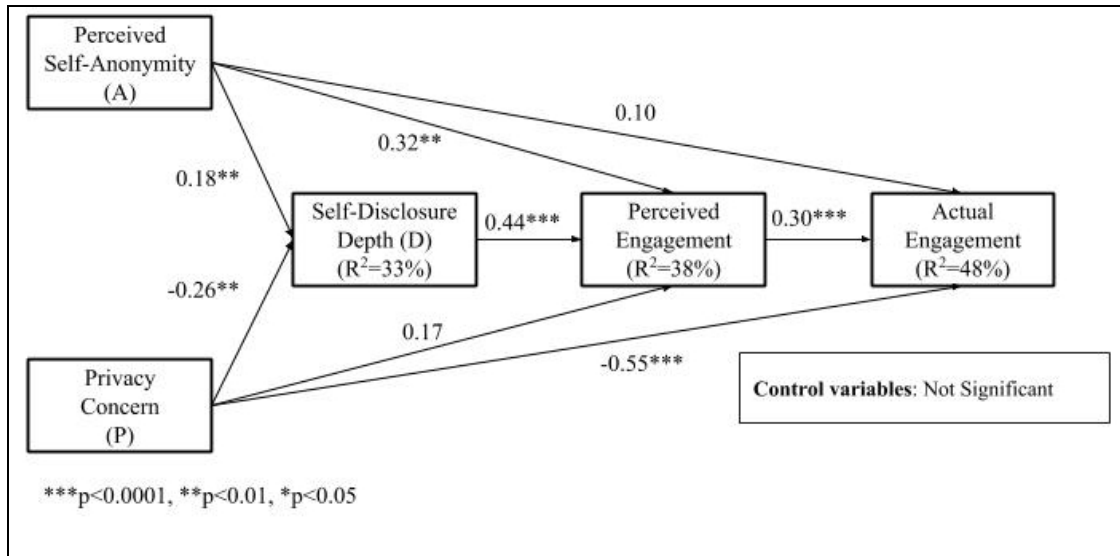
<b>Gender</b>	Male (55%), Female (45%)				
<b>Age</b>	Min=18, Max=41, Average=23				
<b>Disposable Income (\$/ year)</b>	<5k	5k=< <10k	10k=< <15k	15k=< <20k	>=20k
<b>Academic Standing</b>	48%	21%	21%	1%	9%
	Freshman	Sophomore	Junior	Senior	Graduate
	4%	14%	65%	17%	0%

## DATA ANALYSIS AND RESULTS

Following the two-step analytical approach suggested by Hair et al. (2006), this study first evaluated the measurement model for reliability and validity followed by an assessment of 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 (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 variable, estimated path coefficients, and t-values.

The PLS results indicate the structural model explains 33 percent of the variance in ongoing self-disclosure depth, 38 percent of the variance in perceived engagement with a SNA, and 48 percent 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 and perceived self-anonymity and actual engagement. 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 the 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. On the other hand, the relationship between perceived self-anonymity and actual engagement was insignificant, while it was significant for perceived engagement. This can be explained by the notion of self-disclosure that user do not perceive they stay anonymous on a SNA after revealing some personal information. This is an interesting finding, demonstrating how privacy concern relationship with perceived engagement is fully mediated by the self-disclosure depth. In addition, perceived self-anonymity relationship with actual engagement is fully mediated by perceived engagement.



**Figure 2.** Structural model analysis

**CONTRIBUTIONS**

The most significant contributions of this study can be divided into theoretical and practical segments. Although the relationship between privacy concern and self-disclosure is well-studied in previous IS literature, the lack of an integrated model to simultaneously examine the relationship between anonymity, self-disclosure depth, privacy concern in a new SNA and how they influence engagement is the main motivation for this study. This is an important contribution because it demonstrates the need for inclusion of all three aspects when information privacy is being investigated. 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 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 over time. 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 introduce 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.

### CONCLUSION

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 of perceived self-anonymity and self-disclosure depth. This model identifies self-anonymity and privacy concern as predictor of self-disclosure depth at later stage. As demonstrated, privacy concern is not related with perceived engagement, but rather related with actual engagement with a new privacy-based SNA. Finally, perceived anonymity is not related with actual engagement, but it related with perceived engagement.

## REFERENCES

- Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and Human Behavior in the Age of Information," *Science* (347:6221), pp. 509–514.
- Bano, M., and Zowghi, D. 2015. "A Systematic Review on the Relationship between User Involvement and System Success," *Information and Software Technology* (58), pp. 148–169. (<https://doi.org/10.1016/j.infsof.2014.06.011>).
- Bansal, G., Zahedi, F., and 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), pp. 138–150.
- Belanger, F., and Xu, H. 2015. "Editorial The Role of Information Systems Research in Shaping the Future of Information Privacy," *Information Systems Journal*, pp. 573–578. (<https://doi.org/10.1111/isj.12092>).
- Bell, M. 2001. "Online Role-Play: Anonymity, Engagement and Risk," *Educational Media International* (38:4), pp. 251–260.
- Bhattacharjee, A. 2001. "Understanding Information Systems Continuance: An Expectation-Confirmation Model," *MIS Quarterly* (25:3), pp. 351–370.
- Chen, H.-G., Chen, C. C., Lo, L., and Yang, S. C. 2008. "Online Privacy Control via Anonymity and Pseudonym: Cross-Cultural Implications," *Behaviour & Information Technology* (27:3), pp. 229–242.
- Chen, R., Wang, J., Herath, T., and Rao, H. R. 2011. "An Investigation of Email Processing from a Risky Decision Making Perspective," *Decision Support Systems* (52:1), pp. 73–81.
- Cho, D., and 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*, pp. 3041–3050. (<https://doi.org/10.1109/HICSS.2012.241>).
- Chu, S.-C., and Kim, Y. 2011. "Determinants of Consumer Engagement in Electronic Word-of-Mouth (EWOM) in Social Networking Sites," *International Journal of Advertising* (30:1), pp. 47–75.
- Chudnov, D. 2008. "Updates on Pulsing Content, Unconferences, and Coding," *Computers in Libraries* (28:8), pp. 31–33. (<https://doi.org/Editorial>).
- Deuze, M. 2006. "Participation, Remediation, Bricolage: Considering Principal Components of a Digital Culture," *The Information Society* (22:2), pp. 63–75. (<https://doi.org/10.1080/01972240600567170>).
- Dinev, T., McConnell, A. R., and 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), pp. 639–655.
- Dwyer, C., Hiltz, S., and Passerini, K. 2007. "Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace," in *Americas Conference on Information Systems*, p. 339.
- Ellison, N. B., Steinfield, C., and 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), pp. 1143–1168.
- French, A. M., and Read, A. 2013. "My Mom's on Facebook: An Evaluation of Information Sharing Depth in Social Networking," *Behaviour and Information Technology* (32:10), pp. 1049–1059. (<https://doi.org/10.1080/0144929X.2013.816775>).
- Green, T., Wilhelmsen, T., Wilmots, E., Dodd, B., and Quinn, S. 2016. "Social Anxiety, Attributes of Online Communication and Self-Disclosure across Private and Public Facebook Communication," *Computers in Human Behavior* (58), pp. 206–213.
- Gross, R., Acquisti, A., and Iii, H. J. H. 2005. "Information Revelation and Privacy in Online Social Networks," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, ACM, pp. 71–80.
- Hair, J. F., Tatham, R. L., Anderson, R. E., and Black, W. 2006. *Multivariate Data Analysis*, (Vol. 6), Pearson Prentice Hall Upper Saddle River, NJ.

- Hayne, S. C., and Rice, R. E. 1997. "Attribution Accuracy When Using Anonymity in Group Support Systems," *International Journal of Human-Computer Studies* (47), pp. 429–452. (<https://doi.org/10.1006/ijhc.1997.0134>).
- Hui, K.-L., Teo, H. H., and Lee, S.-Y. T. 2007. "The Value of Privacy Assurance: An Exploratory Field Experiment," *MIS Quarterly*, pp. 19–33.
- Imlawi, J., and Gregg, D. 2014. "Engagement in Online Social Networks: The Impact of Self-Disclosure and Humor," *International Journal of Human-Computer Interaction* (30:2), pp. 106–125.
- Jiang, Z. (Jack), Heng, C. S., and Choi, B. C. F. 2013. "Research Note —Privacy Concerns and Privacy-Protective Behavior in Synchronous Online Social Interactions," *Information Systems Research* (24:3), pp. 579–595. (<https://doi.org/10.1287/isre.1120.0441>).
- Joinson, A. N., Houghton, D. J., Vasalou, A., and Marder, B. L. 2011. "Digital Crowding: Privacy, Self-Disclosure and Technology.," in *Privacy Online. Digital Crowding: Privacy, Self-Disclosure, and Technology*, Springer Berlin Heidelberg, pp. 33–45. ([https://doi.org/10.1007/978-3-642-21521-6\\_4](https://doi.org/10.1007/978-3-642-21521-6_4)).
- Junglas, I., Abraham, C., and Watson, R. 2008. "Task-Technology Fit for Mobile Locatable Information Systems," *Decision Support Systems* (45:4), pp. 1046–1057.
- Kern, E. 2013. "The Social Network Where We're All Just a Number," *USA Today*.
- Kiesler, S., Siegel, J., and McGuire, T. W. 1984. "Social Psychological Aspects of Computer-Mediated Communication," *The American Psychologist* (39:10), pp. 1123–1134.
- Koohikamali, M., Peak, D., and Prybutok, V. 2017. "Beyond Self-Disclosure: Disclosure of Information about Others in Social Network Sites," *Computers in Human Behavior* (69), pp. 29–42. (<https://doi.org/10.1016/j.chb.2016.12.012>).
- Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. 2010. "Online Social Networks: Why We Disclose," *Journal of Information Technology* (25:2), pp. 109–125.
- Lea, M., and Spears, R. 2001. "Knowing Me , Knowing You : Anonymity Effects on Social Identity Processes Within Groups," *Personality and Social Psychology Bulletin* (27:5), pp. 526–537.
- Liau, A. K., Khoo, A., and Hwaang, P. 2005. "Factors Influencing Adolescents Engagement in Risky Internet Behavior," *CyberPsychology & Behavior* (8:6), pp. 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), pp. 393–411.
- Mahan, J. E., Seo, W. J., Jordan, J. S., and Funk, D. 2015. "Exploring the Impact of Social Networking Sites on Running Involvement, Running Behavior, and Social Life Satisfaction," *Sport Management Review* (18:2), pp. 182–192.
- 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.
- Nissenbaum, H. 2004. "Privacy as Contextual Integrity," *Wash L. Rev.* (79), pp. 101–139. (<https://doi.org/10.1109/SP.2006.32>).
- Nissenbaum, H. 2010. *Privacy In Context: Technology Policy And The Integrity Of Social Life*, Stanford University Press. ([https://doi.org/10.1207/S15327051HCII16234\\_03](https://doi.org/10.1207/S15327051HCII16234_03)).
- Norberg, P. A., Horne, D. R., and Horne, D. A. 2007. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors," *Journal of Consumer Affairs* (41:1), pp. 100–126.
- O'Brien, H. L., and 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), pp. 938–955.
- O'Brien, H. L., and 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), pp.



50–69.

- Papadopoulos, E. P., Diamantaris, M., Papadopoulos, P., Petsas, T., Ioannidis, S., and Markatos, E. P. 2017. “The Long-Standing Privacy Debate: Mobile Websites Vs Mobile Apps,” *Proceedings of the 26th International Conference on World Wide Web* (v), pp. 153–162. (<https://doi.org/10.1145/3038912.3052691>).
- Pfitzmann, A., and Köhntopp, M. 2001. “Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology,” *Designing Privacy Enhancing Technologies* (2009), pp. 1–9. ([https://doi.org/10.1007/3-540-44702-4\\_1](https://doi.org/10.1007/3-540-44702-4_1)).
- Pinsonneault, A., and Heppel, N. 1997. “Anonymity in Group Support Systems Research: A New Conceptualization, Measure, and Contingency Framework,” *Journal of Management Information Systems* (14:3), pp. 89–108.
- Posey, C., Lowry, P. B., Roberts, T. L., and 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), pp. 181–195.
- Postmes, T., and Spears, R. 1998. “Deindividuation and Antinormative Behavior: A Meta-Analysis,” *Psychological Bulletin* (123:3), p. 238.
- Scott, S. V., and Orlikowski, W. J. 2014. “Entanglements in Practice: Performing Anonymity through Social Media,” *Mis Quarterly* (38:3), pp. 873–893.
- Sproull, L., and Kiesler, S. 1986. “Reducing Social Context Cues: Electronic Mail in Organizational Communication,” *Management Science* (32:11), pp. 1492–1512. (<https://doi.org/10.1287/mnsc.32.11.1492>).
- Staddon, J., Huffaker, D., Brown, L., and Sedley, A. 2012. “Are Privacy Concerns a Turn-off?: Engagement and Privacy in Social Networks,” in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ACM, p. 10.
- Takahashi, T. 2010. “MySpace or Mixi? Japanese Engagement with SNS (Social Networking Sites) in the Global Age,” *New Media & Society* (12:3), pp. 453–475. (<https://doi.org/10.1177/1461444809343462>).
- Tian, X. 2015. “Network Domains in Social Networking Sites: Expectations, Meanings, and Social Capital,” *Information, Communication & Society* (4462:December 2015), pp. 1–15. (<https://doi.org/10.1080/1369118X.2015.1050051>).
- Trepte, S., and 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), pp. 1102–1112. (<https://doi.org/10.1016/j.chb.2012.10.002>).
- Vasalou, A., Oostveen, A. M., Bowers, C., and Beale, R. 2015. “Understanding Engagement with the Privacy Domain through Design Research,” *Journal of the Association for Information Science and Technology* (66:6), pp. 1263–1273. (<https://doi.org/10.1002/asi.23260>).
- Webster, J., and Ahuja, J. S. 2006. “Enhancing the Design of Web Navigation Systems: The Influence of User Disorientation on Engagement and Performance,” *MIS Quarterly* (30:3), pp. 661–678.
- Westin, A. F. 2003. “Social and Political Dimensions of Privacy,” *Journal of Social Issues* (59:2), pp. 431–453.
- Zhou, Z., Jin, X.-L., Fang, Y., and 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), pp. 247–261.
- Zimmer, J. C., Arsal, R., Al-Marzouq, M., Moore, D., and Grover, V. 2010. “Knowing Your Customers: Using a Reciprocal Relationship to Enhance Voluntary Information Disclosure,” *Decision Support Systems* (48:2), pp. 395–406.

**APPENDIX A – MEASUREMENT OF PRINCIPAL CONSTRUCTS**

<b>Construct</b>	<b>Item</b>	<b>Measurement Item</b>	<b>Reference</b>
Privacy concern	PC1	I am concerned that I am asked to provide my personal information on this app.	(Junglas et al. 2008; Zhou et al. 2015)
	PC2	I am concerned that there is the possibility of unauthorized access to databases that contain my information on this app.	
	PC3	I am concerned that this app does not have thorough procedures to prevent errors in my personal information.	
	PC4	I am concerned that this app uses my personal information for other purposes without getting my authorization.	
Self-disclosure depth	DD	Numbers of specific personal information disclosed/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.	(O'Brien and Toms, 2010)
	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	I lose track of time, when I use it.	
Actual Engagement (Sum)	Connectivity	Number of friends they have connected to.	(Burke et al., 2010)
		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.	