FACTORS AFFECTING USERS' PERCEPTIONS OF SOCIAL-MEDIA BENEFITS AND PRIVACY CONCERNS

Robert Stone, College of Business and Economics, University of Idaho, Moscow ID 83843, rstone@uidaho.edu
Daniel M. Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, eveleth@uidaho.edu
Lori Baker-Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, leveleth@uidaho.edu

ABSTRACT

This research examined the extent to which social-media users' privacy-invasion experience, risk intolerance, knowledge of privacy issues, and knowledge of others' privacy invasion experiences, influenced their concern for privacy and their perceptions about the benefits of using social media. The results of the analyses show that users' privacy-invasion experience, risk intolerance and knowledge of others' privacy-invasion experiences affected their concern for privacy. In addition, their level of risk intolerance had a negative effect on their perceptions of the benefits of using social media.

Keywords: Social-media, privacy concern, risk intolerance, privacy invasions experience

INTRODUCTION

While it is clear that social media users frequently express privacy concerns with respect to social media use (Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M. & Turner, E., 2019), much remains to learn about the influence that privacy-related factors play in affecting users' attitudes, and therefore, their behavior (Coopamootoo, 2020). Extending our knowledge of these factors and relationships is the primary purpose of this manuscript. The central research question is how social media users' privacy-invasion experiences, and their knowledge of others' privacy-invasion experiences, affect their attitudes towards social media. Specifically, do privacy-invasion experiences (i.e., their own and those of others) affect users' perceptions of the benefits of using social media and their concern for privacy when using social media?

LITERATURE REVIEW

Studies on the antecedents and consequences of privacy concern have consistently found that a privacy-invasion experience is associated with increased concern for privacy (Degirmenci, 2020; Hong, Chan, & Thong, 2019; Kenny & Connolly, 2016). Others have found that when individuals have been the victim of a privacy invasion they are more likely to believe that such invasions will occur in the future (Bansal, Zahedi, & Gefen, 2016); a negative experience affects users' trust in a website (Shin, 2010), device (Keith, Babb, Lowry, Furner, & Abdullat, 2015), or perception to privacy-protection technology effectiveness (Wang, Sun, Dai, Zhang, & Hu, 2019). In addition, others (Mohamed & Ahmad, 2012, Adhikari & Panda, 2018) have found that perceptions of vulnerability, which is likely a consequence of privacy experiences, are positively related to privacy concerns. In addition, Fianu Ofori, Boateng, and Ampong (2019) found that a privacy

invasion experience negatively affected trust in the social media provider. For these reasons we expect the following hypothesis:

H1: A social media user's privacy experiences significantly and positively influence their perceptions of privacy concerns.

H2: A social media user's privacy experiences significantly and negatively influences their perceptions of social media benefits.

H3: A social media user's degree of risk intolerance significantly and positively influences their perceptions of privacy concerns.

H4: A social media user's degree of risk intolerance significantly and positively influences their perceptions of social media benefits.

H1: A social media user's knowledge of privacy issues significantly and positively influences their perceptions of privacy concerns.

H2: A social media user's knowledge of privacy issues significantly and negatively influences their perceptions of social media benefits.

METHOD

The Data

The data collection process took place over three academic semesters, fall 2021, spring 2022, and fall 2022 in three different business courses. These courses are Introduction to Financial Accounting, Introduction to Managerial Accounting, and Managing Information. All are required to complete an undergraduate degree in business at a AACSB-accredited business college in medium-sized university in the mountain west of the United States.

A questionnaire was developed in Qualtrics and a link to this questionnaire was provided to the students in the selected classes. A total of 518 students were enrolled in these classes and 403 students submitted the questionnaire, probably due to the extra credit the instructors provided for completing the questionnaire. The resulting response rate is 78%. Eight responses were excluded from the analysis due to missing values, leaving 395 usable responses in the analysis.

The Measures

The theoretical constructs discussed earlier are measured by collecting student responses to specific questionnaire items. The measures and sample questionnaire items used to form the measures are provided below. The risk tolerance measure is composed of two items or indicants which are focused on the respondent's attitudes toward trying new things. The measure of privacy invasion experiences: personal is composed of two items. These items examine whether the respondent has felt their personal data was used without permission and their personal privacy had been invaded through social media. The privacy invasion experiences: others is measured by two

indicants. These items capture the respondents' feelings that others say their personal data was used without permission and their personal privacy had been invaded through social media. The measure for knowledge of privacy issues is built on two questionnaire items which focus on respondent's perceived knowledge of privacy issues on social media and the Internet. The measure of privacy concerns is developed from five questionnaire items. These items present social media settings users may set to limit the personal information and pictures exposed on social media. The final measure of social media benefits is developed from two questionnaire items. These items focus on the respondent's perceived value received from social media in exchange for providing personal information.

The psychometric properties of the measures are evaluated from the results of a confirmatory factor analysis (CFA) using structural equations modelling through procedure Calis in PC SAS 9.4. Each measure is reflective in its indicants and all measures are pair-wise correlated. There are no paths defined between any measures. The fit results for the CFA are good. The goodness of fit index is 0.96 and the adjusted goodness of fit is 0.94. The root mean square residual is 0.05 and its standardized version is 0.03. Bentler's comparative fit index is 0.99 and the incremental fit indexes (e.g., Bentler & Bonett; Bollen) range from 0.95 to 0.99. While the chi-square statistic is statistically significant at a 1% level, the normed chi-square is less than 2 at 1.45. In total, these statistics indicate a good fit between the data and the CFA model (Hair, Anderson, Tatham, & Black, 1992; Hooper, Coughlen, & Mullen, 2008; Rainer & Harrison, 1993).

The statistics evaluating the psychometric properties of the measures are calculated using the standardized path coefficients between the construct and its indicants from the CFA. The measure of privacy concerns has standardized path coefficients of 0.76, 0.86, 0.87, 0.87 and 0.76. Using these estimated coefficients, the composite reliability statistic is 0.91 and the percentage of shared variance extracted is 68%. The risk tolerance measure has estimated path coefficients of 0.72 and 0.73. The composite reliability coefficient and percentage of shared variance extracted are calculated to be 0.69 and 53%. The measure of privacy invasion experiences: personal has standardized path coefficients of 0.87 and 0.83 with resulting composite reliability coefficient of 0.84 and 72% of shared variance extracted. The social media benefits measure is formed by two items having standardized path coefficients of 0.86, and 0.60. The calculated composite reliability measure and percentage of shared variance extracted are 0.70 and 55%, respectively. The privacy invasion experiences: others is formed using two questionnaire items. The standard path coefficients are 0.95 and 0.92. Its estimated composite reliability value is 0.93 with 87% of shared variance extracted. The measure for knowledge of privacy issues is measured by two questionnaire items with estimated path coefficients of 0.78 and 0.87. Its resulting composite reliability coefficient is 0.78 and percentage of shared variance extraction of 64%.

Based on the magnitudes of the estimated standardized path coefficients that range from 0.60 to 0.95, it can be argued that item reliability is satisfied (Rainer & Harrison, 1993). However, one measure (social media benefits) has one estimated standardized path coefficient less than 0.70, indicating the measure requires additional refinement. In terms of composite reliability, all the measures demonstrate acceptable values based on the calculated reliability coefficients ranging from 0.69 to 0.93, however the risk tolerance measure with a composite reliability coefficient less than 0.70 requires additional refinement (Nunnally, 1978). Additionally, all the shared variances

extracted percentages are at or above 53%. The combination of these results indicate that the measures satisfy convergent validity (Igbaria & Greenhaus, 1992; Rainer & Harrison, 1993).

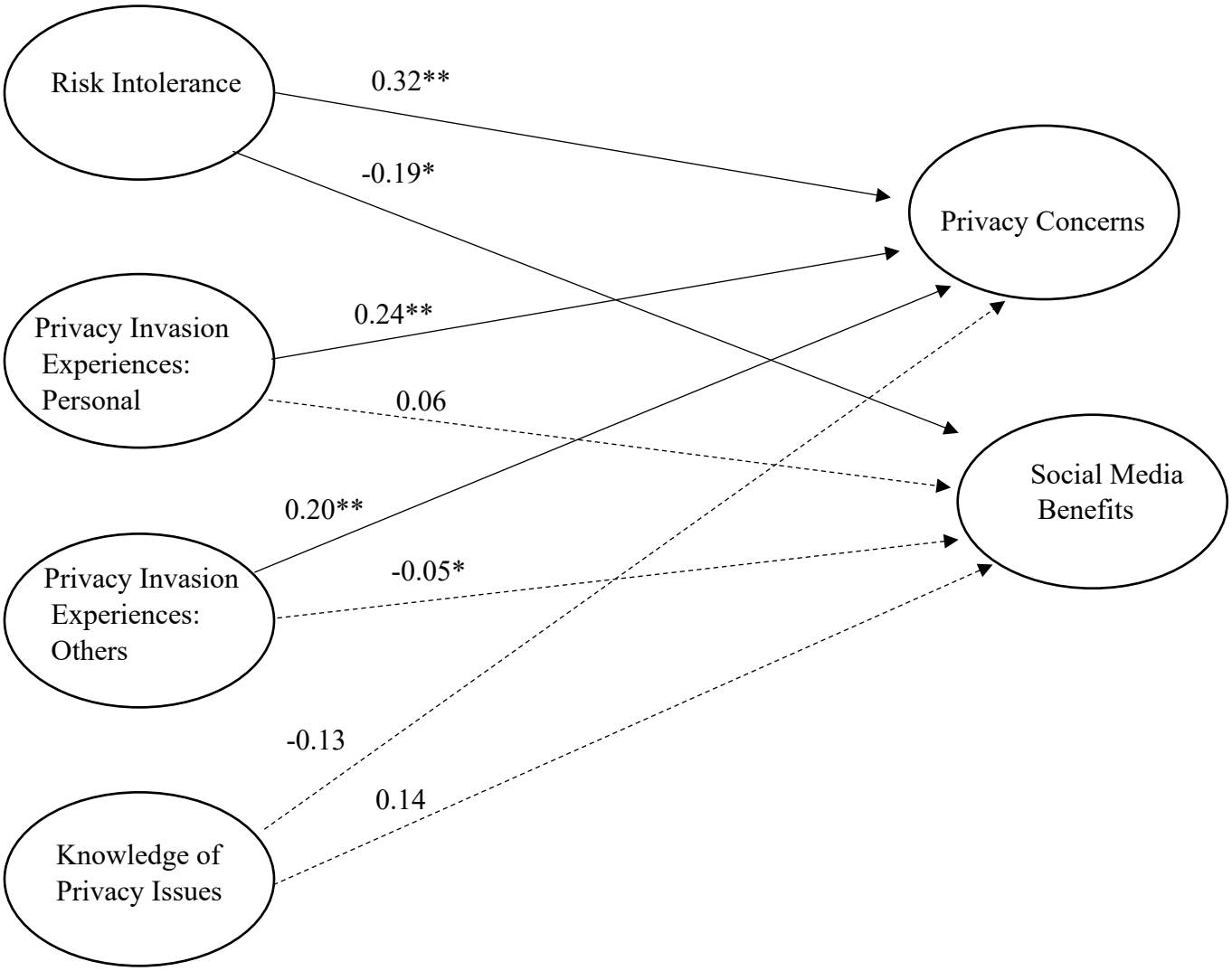
Discriminant validity is also examined by comparing, for each pair of measures, its squared correlation to the individual measures' percentages of shared variance extracted. If discriminant validity is satisfied, the items within a measure share greater common variation among themselves than between the two measures. This is demonstrated when, for each measure pair, the individual measures' percentage of shared variance extracted are greater than the squared correlation between the two measures (Fornell & Larcker, 1981). All the correlations are calculated using the confirmatory factor analysis. The calculated squared correlations are all 0.41 or lower. Because the percentages of shared variance extracted are 53% or greater, discriminant validity is satisfied for all the measures. Based on these values, all the percentages of shared variance extracted are greater than the squared correlations between the corresponding measures. Thus, discriminant validity is satisfied (Hair, Anderson, Tatham, & Black, 1992). Since convergent and discriminant validity are both satisfied, it can be argued that construct validity is satisfied (Hair, Anderson, Tatham, & Black, 1992).

The Model Estimation

The proposed model linking respondents' risk tolerance, privacy invasion experiences: personal, privacy invasion experiences: others, and knowledge of privacy issues relate to both privacy concerns and social media benefits is estimated using the previously discussed measures and data. The estimation method employed is structural equations modeling, specifically procedure Calis in PC SAS version 9.4. As in the CFA, the fit of the model to the data is good as demonstrated by several statistics. The goodness of fit index is 0.97 and the adjusted goodness of fit is 0.94. the root mean square residual is 0.03 and its standardized version is 0.03. Bentler's comparative fit index is 0.99 and the incremental fit indexes (e.g., Bentler and Bonett; Bollen) range from 0.95 to 0.99. The chi-square statistic is statistically significant at a 1% level, however the normed chi-square is less than 2 at 1.45. In total, these statistics indicate a good fit between the data and the CFA model (Hair, Anderson, Tatham, and Black, 1992; Hooper, Coughlen, and Mullen, 2008; Rainer and Harrison, 1993).

The estimation results for the structural model are shown below in Figure 1. Using the standardized path coefficients, privacy concerns is significantly and positively influenced by risk tolerance, privacy invasion experiences: personal, and privacy invasion experiences: others. Social media benefits is also significantly and negatively influenced by risk tolerance. All paths are significant at a 1% level. Additionally, the four exogenous measures hypothesized to influence privacy concerns and social media benefits are pair-wised correlated. Four of these correlations are statistically significant at a 1% level. The two insignificant correlations are between risk tolerance and privacy invasion experiences: personal and between privacy invasion experiences: personal and knowledge of privacy issues.

Figure 1: The Estimated Model



Conclusions

Results from this study showed that users' privacy-invasion experience, risk intolerance and knowledge of others' privacy-invasion experiences affected their concern for privacy. These findings should concern organizations that need users to disclose information. According to a recent study by Pew Research Center (2021) nearly 70% of "Americans use social media to connect with one another, engage with news content, share information and entertain themselves" (p.1). But this strong level of participation could be at risk if privacy invasions grow. As privacy invasion techniques continue to adapt, one can expect privacy-invasions to continue to grow; providing users with more privacy-invasion experiences and greater awareness of the invasion experiences of others. The result will likely be a growing concern for privacy and possibly greater distrust of such things as social media, consumer products organizations, or the Internet of Things that seek our personal information. As one anonymous commenter noted in a 2017 Pew Research

Center paper on the topic: "…[bad actors] who attack individuals and systems will always be a step ahead of any possible security measures. As people hear more and more about data breaches, etc., they will become more distrustful. Already, many people who are not technically sophisticated take a blanket approach in which they wish to reveal nothing to anyone" (Raine & Anderson, 2017).

REFERENCES

Adhikari, K., & Panda, R. K. Users' information privacy concerns and privacy protection behaviors in social networks. *Journal of Global Marketing*, 2018, 31(2), 96-110.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. Americans and privacy: Concerned, confused and feeling lack of control over their personal information, *Pew Research Center*, 2019. Retrieved from https://policycommons.net/artifacts/616499/americans-and-privacy/1597152/

Bansal, G., Zahedi, F. M., & Gefen, D. Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, 2016, 53(1), 1-21.

Coopamootoo, K. P. Usage patterns of privacy-enhancing technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, October: 1371-1390.

Degirmenci, K. Mobile users' information privacy concerns and the role of app permission requests. International Journal of Information Management, 2020, 50, 261-272.

Fianu, E., Ofori, K. S., Boateng, R., & Ampong, G. O. A. The Interplay Between Privacy, Trust and Self-disclosure on Social Networking Sites. In I*nternational Working Conference on Transfer and Diffusion of IT*, 2019, June: 382-401.

Fornell, C. & Larcker, D. F. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 1981*, 18(1), 39-50.

Hair, J., Jr., Anderson, R. E., Tatham, R. L., & Black, W. C. *Multivariate data analysis: with readings*. New York: MacMillan Publishing Company, 1992.

Hong, W., Chan, F. K., & Thong, J. Y. Drivers and inhibitors of internet privacy concern: a multidimensional development theory perspective. *Journal of Business Ethics*, 2021, 168(3), 539-564.

Hooper, D., Coughlan, J., & Mullen, M. Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods,* 2008, 6(1), 53-60.

Igbaria, M. & Greenhaus, J. H. Determinants of MIS employees' turnover intentions: a structural equation model. *Communication of the ACM, 1992, 35*(2), 34-49.

Keith, M. J., Babb, J. S., Lowry, P. B., Furner, C. P., & Abdullat, A. The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal*, 2015, 25(6), 637-667.

Kenny, G., & Connolly, R. Drivers of health information privacy concern: a comparison study. *Twenty-second Americas Conference on Information Systems*, San Diego, 2016.

Mohamed, N., & Ahmad, I. H. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 2012, 28(6), 2366-2375.

Nunnally, J. (1978). *Psychometric methods*: New York: McGraw-Hill.

Pew Research Center. *Social Media Fact Sheet*, April 7, 2021. Retrieved from: https://www.pewresearch.org/internet/fact-sheet/social-media/

Rainer, R. K., and Harrison, A. W. Toward development of the end user computing construct in a university setting. *Decision Sciences*, 1993, 24(6), 1187-1202.

Rainie, L., & Anderson, J. The fate of online trust in the next decade, *Pew Research Center*, 2017.

Wang, L., Sun, Z., Dai, X., Zhang, Y., & Hu, H. H. (2019). Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns. *Information Technology & People*, 2019.