SUBJECTIVE NORMS AND PRIVACY-PROTECTION BEHAVIORS

Lori Baker-Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-5940, leveleth@uidaho.edu

Daniel M. Eveleth, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-4396, eveleth@uidaho.edu

Robert Stone, College of Business and Economics, University of Idaho, Moscow ID 83843, 208-885-6788, rstone@uidaho.edu

ABSTRACT

Individuals with high privacy concerns tend to perform more protection-oriented behaviors, while individuals with high perceptions of technology-use benefits tend to perform less protection-oriented behaviors. These findings create a privacy paradox for organizations when it comes to motivating employees to capitalize on the benefits of technology use while also minimizing the risks. This research examined the extent to which online-technology users' perceptions of social norms, their concern for privacy, and their perceived technology-use benefits affected their privacy-protection behaviors. The results of the analysis found that concern for privacy and perceived subjective injunctive norms are significantly, and positively related to privacy-protection behaviors.

Keywords: Security, subjective norms, social norms, privacy concern, privacy protection

INTRODUCTION

Organizations consistently wrestle with the need to encourage employees to capitalize on the benefits of technology use with an opposing interest in discouraging technology-use behaviors that might increase risk to the organization. While promoting the benefits of technology use leads to greater use, individuals who perceive the benefits of technology use tend to disclose more information on the internet and perform less protection-oriented behaviors than do those who perceive less benefits. And, because individuals with high privacy concerns tend to disclose less information and perform more protection-oriented behaviors than do those with low concerns, organizations can increase protection behaviors by raising employees' privacy concerns. However, such efforts can have the unintended effect of decreasing technology use. The question, therefore, remains - how can organizations influence employee behaviors such that the organization gets the desired use of technology and the least amount of risk? The primary purpose of this study is to help answer this question by investigating the role that privacy-protection-oriented social norms play in affecting privacy protection behaviors.

One argument in favor of social norms is that while technology use and many decisions about privacy protection are individual choices, privacy and security are a collective or social interest. Thus, if an individual who perceives many benefits to disclosing information chooses to disclose information or chooses not to perform preventative protection behaviors, then collective interests may be at risk. A possible solution for organizations is to develop and encourage privacy norms. Privacy-related research would benefit from exploring the subjective norm construct as it relates to predicting intentions to perform preventive protection behaviors; it would likely help extend our understanding of users' privacy-related behaviors beyond the so-called privacy paradox. The paradox views behavior as a function of users weighing benefits of taking an action against the risk of taking the same action.

LITERATURE

One construct that would be useful for investigating the role of privacy norms in affecting preventive protection behaviors is the construct “subjective norms”, found in the theory of reasoned action and the theory of planned behavior. The theory of reasoned action and the theory of planned behavior conceptualize behavioral intentions (e.g., intentions to perform privacy-protection behaviors) as the antecedent to the behavior, and those intentions result from: 1. An individual’s attitude toward the desired behavior, 2. Their perceptions of subjective norms related to the desired behavior, and 3. Perceived behavioral control over the behavior (added in the theory of reasoned action). Attitudes, subjective norms, and perceived behavioral control are the product of expectancy theory-like combinations of beliefs and valences. For example, with respect to privacy-protection norms, an employee would first evaluate their beliefs about whether a specific referent group (e.g., other employees) would think the employee should or should not perform a preventative protection behavior. This would then be combined with their motivation to comply with the referent group to form their subjective norms about privacy-protection behaviors (Ajzen & Fishbein, 1980). Considering users’ perceptions of privacy norms may help eliminate the so-called paradox, this could give organizations more direction on how to encourage preventive protection behaviors beyond just playing up the potential risks (and therefore, creating increased concerns) as a counterweight to the effects of perceived benefits.

Subjective norms fall into two types, injunctive norms, and descriptive norms. Injunctive norms represent an individual’s perceptions of the behavior that other people in their referent group would want the individual to perform. Descriptive norms represent an individual’s perceptions of the behaviors that others in their referent perform (Smith, J. R. & Louis 2008). Consistent with prior research on the theory of planned behavior and the theory of reasoned action we hypothesize the following findings with respect to the relationship between subjective norms and privacy-protection behaviors:

H1: The greater the subjective injunctive norms to perform privacy-protection behaviors is, the greater the extent to which users perform protective behaviors.
H2: The greater the subjective descriptive norms to perform privacy-protection behaviors is, the greater the extent to which users perform protective behaviors.

Substantial research has investigated the relationships between privacy concerns and privacy protection behaviors, between perceived benefits and privacy protection behaviors, and other privacy-related intentions and attitudes (e.g., Jahangir & Begum, 2007; Kumar, Mohan & Holowczak, 2008; Li, 2014; Osatuyl, 2015; Baker-Eveleth, Stone & Eveleth, 2021). Based upon this research we expect to find similar results in our study; represented in the following hypotheses:

H3: The greater the greater the concern for privacy, the greater the extent to which users perform protective behaviors.
H4: The greater the perceived benefits of technology use, the lower the extent to which users perform protective behaviors.

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 an 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 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 privacy concerns measure is composed of five items or indicants which are all focused on the respondent's concern about their privacy on social media sites; other sites can access personal information; social media sites do not take sufficient steps to secure personal information; and social media sites collect too much personal information. The measure of subjective injunctive norms (i.e., doing what others think one should do) is composed of three items. These items are in the spirit of my friends, people my age, and people important to me believe it is alright to share personal information on social media. The subjective descriptive norms construct (i.e., doing what others do) was measured by two questionnaire indicants. These items capture the respondents' feelings that the majority of people their age protect their privacy and limit access to personal data on social media. The measure for social media benefits is built on two questionnaire items which focus on the concepts of the value or benefits obtained from social media for exchanging personal information. The final measure is privacy protection behaviors developed from four questionnaire items. These items present social media settings users may set to limit the personal information and pictures exposed on social media.

The psychometric properties of the measures are evaluated using a confirmatory factor analysis (CFA) and structural equations modelling using procedure Calis in PC SAS 9.4. Each measure is reflective in its indicants (questionnaire items) 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 0.95 and the adjusted goodness of fit is 0.92. The root mean square residual is 0.07 and its standardized version is 0.05. Bentler's comparative fit index is 0.97 and the incremental fit indexes (e.g., Bentler and Bonett; Bollen) range from 0.92 to 0.97. While the chi-square statistic is statistically significant at a 1% level, the normed chi-square is less than 2 at 1.85. 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 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 social norm: share information has estimated path coefficients of 0.77, 0.768 and 0.68. The composite reliability coefficient and percentage of shared variance extracted are calculated to be 0.75 and 51%. The social norm limit information measures has standardized path coefficients of 0.85 and 0.74 with resulting composite reliability coefficient of 0.78 and 64% of shared variance extracted. The social media: benefits measure is formed by two items having standardized path coefficients of 0.66, and 0.78. The calculated composite reliability measure and percentage of shared variance extracted are 0.68 and 51%, respectively.

The final measure, privacy protection behaviors is formed using four questionnaire items. The standard path coefficients are 0.66, 0.73, 0.89, and 0.73. Its estimated composite reliability value is 0.84 with 57% of shared variance extracted.

Based on the magnitudes of the estimated standardized path coefficients that range from 0.66 to 0.89, it can be argued that item reliability is satisfied (Rainer and Harrison, 1993). However, three measures (i.e., social norm: share information; social media benefits; and privacy protection behaviors) each has at least one estimated standardized path coefficient less than 0.70, indicating these measures require additional refinement. In terms of composite reliability, all the measures demonstrate acceptable values based on the calculated reliability coefficients ranging from 0.68 to 0.91, however the social media benefit measure with a composite reliability coefficient less than 0.70 also requires additional refinement (Nunnally, 1978). Additionally, all the shared variances extracted percentages are above 50%. The combination of these results indicate that the measures may well satisfy convergent validity (Igbaria and Greenhaus, 1992; Rainer and Harrison, 1993).

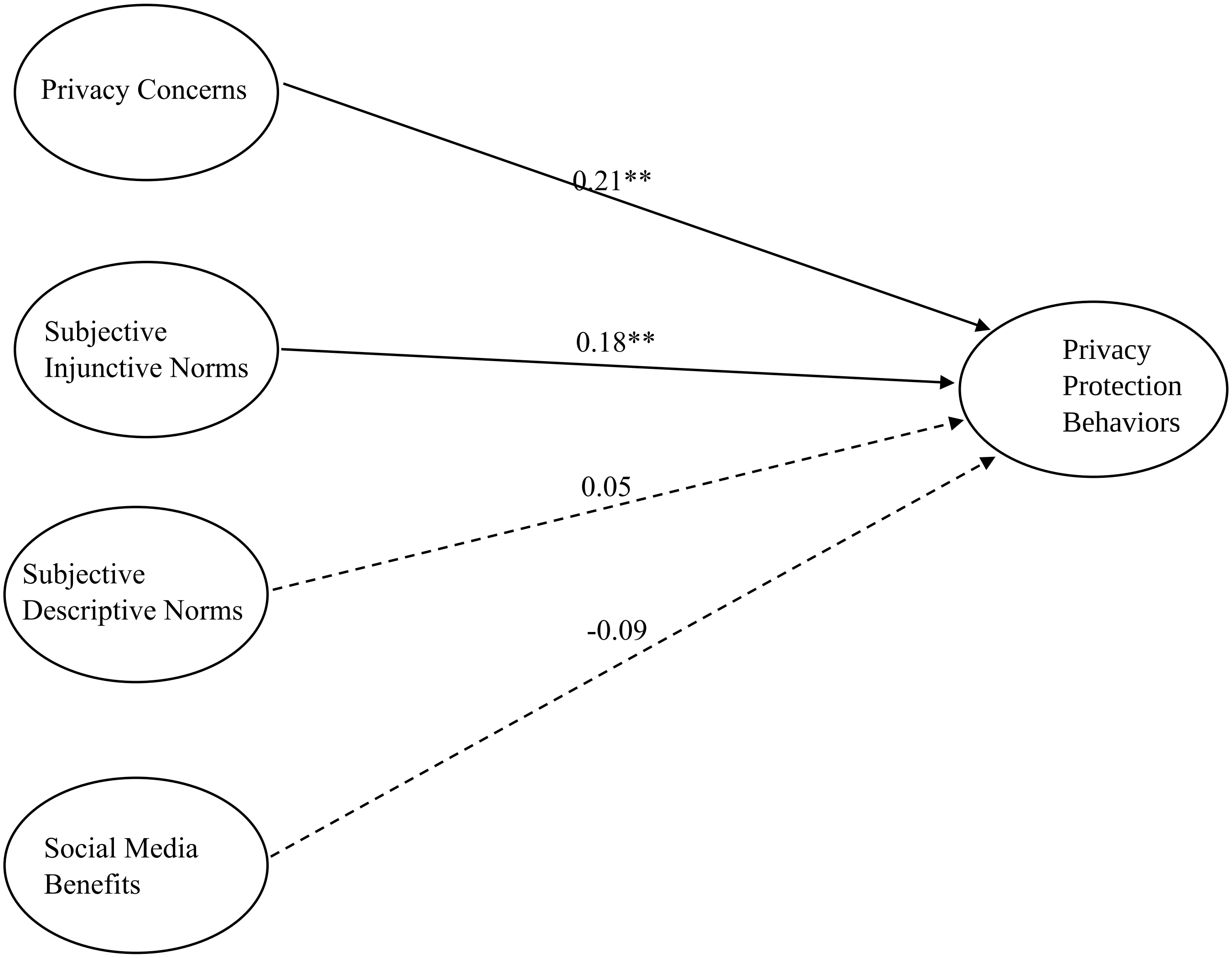
Discriminant validity is also examined by comparing, for each pair of measures, its squared correlation to the individual measures' percentages of shared variance extracted. If discriminant validity is satisfied, the items within a measure share greater common variation among themselves than between 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 and Larcker, 1981). All the correlations are calculated using the confirmatory factor analysis. The calculated correlation range, in absolute value, from 0.03 to 0.30 and the resulting squared correlation range is 0.0009 to 0.09. Because the percentages of shared variance extracted are 0.51 or 51% or greater, discriminant validity is satisfied for all the measures. respectively. 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, and Black, 1992). Since convergent and discriminant validity are both satisfied, it can be argued that construct validity is satisfied (Hair, Anderson, Tatham, and Black, 1992).

The Model Estimation

The earlier proposed model linking respondents' attitudes regarding social media to their privacy protection behaviors 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 0.95 and the adjusted goodness of fit is 0.92. the root mean square residual is 0.07 and its standardized version is 0.05. Bentler's comparative fit index is 0.97 and the incremental fit indexes (e.g., Bentler and Bonett; Bollen) range from 0.92 to 0.97. While the chi-square statistic is statistically significant at a 1% level, the normed chi-square is less than 2 at 1.85. 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 significantly and positively influence privacy protection behaviors. Similarly, subjective injunctive norms significantly and positively in fluence respondents' privacy protection behaviors. For both paths, the significance is at a 1% level. Additionally, the four exogenous measures hypothesized to influence privacy protection behaviors are pair-wised correlated. Four of these correlations are statistically significant at either a 5% or 1% level. The significant, negative correlations identified are between privacy concerns and subjective descriptive norms and privacy concerns and social media benefits. Significant, positive correlations are found between social media benefits and subjective injunctive norms and social media benefits and subjective descriptive norms.

Figure 1: the Estimated Model


Privacy Concerns
0.21**
Subjective Injunctive Norms
0.18**
Privacy Protection Behaviors
0.05
Subjective Descriptive Norms
-0.09
Social Media Benefits

CONCLUSIONS

It is clear from the extensive literature on privacy concerns, the privacy paradox, and other privacy-related research that many technology users react according to their own self-interest when it comes to privacy-related behaviors. While much is known about factors that drive technology users' personal-interest behaviors, less is known about the factors that affect an individual's willingness or intentions to perform security- or privacy-related behaviors that serve the collective interests with respect to privacy and security.

Individuals with high privacy concerns tend to disclose less personal information about themselves and perform more protection-oriented behaviors than do those with low concerns. Further, individuals who perceive the benefits of disclosing personal information tend to disclose more information and perform less protection-oriented behaviors than do those who perceive less benefits. These findings create a dilemma for organizations when it comes to both motivating employees to capitalize on the benefits of technology (by increasing employees' perceptions of benefits) while also minimizing the level of risk to the company (by increasing employees privacy concerns). In this study we helped fill this gap of understanding by investigating the roles that subjective norms play in affecting a technology user's willingness to perform privacy-protection behaviors that affect the collective interest. The finding that subjective injunctive norms (i.e., perceptions about the behaviors that a referent group would want the individual to perform) are positively related to privacy protection behaviors provides organizations with an additional tool for motivating appropriate privacy-related behaviors.

REFERENCES

Ajzen, I. & Fishbein, M. Understanding attitudes and predicting social behavior, Prentice-Hall, Englewood Cliffs, NJ, 1980.

Baker-Eveleth, L. J., Stone, R. W., & Eveleth, D. M. Understanding Social Media Users Privacy-Protection Behaviors, *Information and Computer Security*, 2022, *30*(3), 324-345.

Fishbein, M. & Ajzen, I. Theory-based behavior change interventions: Comments on Hobbis and Sutton." Journal of health psychology, 2005, 10(1), 27-31.

Fornell, C., & Larcker, D. F. (1981). 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.

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.

Jahangir, N., & N. Begum. Effect of perceived usefulness, ease of use, security and privacy on customer attitude and adaptation in the context of e-banking. *Journal of Management Research*, 2007, 7(3).

Kumar, N., K. Mohan, and R. Holowczak, Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. *Decision Support Systems*, 2008. 46(1): p. 254-264.

Li, Y., A multi-level model of individual information privacy beliefs. *Electronic Commerce Research and Applications*, 2014. 13(1): p. 32-44.

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

Osatuyl, B., Personality traits and information privacy concern on social media platforms. *Journal of Computer Information Systems*, 2015. 55(4): p. 11-19.

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

Smith, J. R., & Louis, W. R. Do as we say and as we do: The interplay of descriptive and injunctive group norms in the attitude–behaviour relationship. *British Journal of Social Psychology*, 2008, 47(4), 647-666.