WHY WE DARE TO DISCLOSE: TRUST, PRIVACY MANAGEMENT STRATEGIES AND DISCLOSURE OF FACEBOOK USERS

Linda Chang, Ph.D. student, Institute of International Management of a national university in Taiwan. Address: No. 1, University Road, Tainan 701, Taiwan; e-mail: mypinkrainbow66@gmail.com

Dr. Jengchung Victor Chen, Professor and Director, Institute of International Management of a national university in Taiwan. Address: 1 University Road, Tainan 701, TAIWAN; e-mail: victor@mail.ncku.edu.tw Tel:886-6-2757575, ext.53551 or 53561

ABSTRACT

US consumers continue to spend more time on social networks than on any other category of Internet sites. Social networks thrive on user disclosed information, namely willingness to disclose information, yet little is known about what mediates information disclosure. This study holds that trust, use of privacy management strategies, and usage will influence information disclosure. We also argue that trust mediates the relationship between privacy concern and information disclosure, privacy management strategies mediates the relationship between privacy concern and disclosure. The proposed model is empirically supported with survey data from 305 adults aged 20-55, delineating the motivations underlying individuals' information disclosure behavior in social networking communities.

Keywords: privacy, privacy management strategies, social network sites, Communication Privacy Management (CPM), Social Penetration Theory

INTRODUCTION

Individuals who are concerned about the privacy are revealing abundant amounts of personal information on social networking sites such as Facebook. Some manage their privacy concerns by personalizing privacy settings provided by Facebook while others manage their privacy concerns trusting their ability to control the information they provide and the external access to it. Altman (Altman 1975) and Petronio (Petronio 2002) suggest that exerting control over disclosure through rule making can allow an individual new freedom to engage in disclosure. The rationale behind this hypothesis is that, by personalizing or customizing privacy settings, people will feel more comfortable sharing information because they have greater control over who can access it.

While most Facebook studies utilize student-only samples, we surveyed both students and working adults in order to examine the relationship among different privacy control behaviors, trust, and privacy concerns with regard to Facebook among both young and old people.

We examine whether the privacy control strategies identified by Hoy and Milne (2010) give people peace of mind when revealing personal information in Facebook. The relationship between such privacy control strategies and information disclosure behavior has not been tested empirically.
RESEARCH DESIGN AND METHODOLOGY

Participants And Data Collection

Participants were recruited widely from the National Cheng Kung University community through email solicitations. We restricted the sample to students, employees, and alumni that used Facebook, inviting them to follow a link to complete a survey about privacy issues on Facebook. Data was collected during November and December of 2012.

Research Methodology

305 valid responses were collected for the survey. Respondents ranged in age from 20 to 55 years of age. In 2012, the demographics of Facebook users aged 18 and older in Taiwan in the age groups of 18-24, 25-34, and 35 and above are: 30%, 39%, and 31%, respectively, and those of our sample are 27%, 43%, and 30%, respectively. The percentage of male and female Facebook users are 51% and 49%, respectively, and those of our sample are 46% and 54%, respectively. Our sample resembles the population in terms of distribution of age groups.

Data analysis utilized a two-step approach as recommended by Anderson and Gerbing [3]. The first step involves the analysis of the measurement model, while the second step tests the structural relationships among latent constructs. The aim of the two-step approach is to assess the reliability and validity of the measures before their use in the full model. Confirmatory factor analysis (CFA) was applied to assess the construct validity of the scales with AMOS 20. Descriptive statistics were first obtained using SPSS version 19. Table 1 presents the model fit indicies of the CFA analysis.

TABLE 1. Model Fit Indices for the Proposed Structural Model

<table>
<thead>
<tr>
<th>Model fit indices</th>
<th>Proposed Model</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chi-square statistic $\chi^2$/df</td>
<td>2.151</td>
<td>$\leq 5$</td>
</tr>
<tr>
<td>NNFI</td>
<td>0.890</td>
<td>$\geq 0.9$</td>
</tr>
<tr>
<td>CFI</td>
<td>0.937</td>
<td>$\geq 0.9$</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0.062</td>
<td>$\leq 0.08$</td>
</tr>
</tbody>
</table>

THEORY AND HYPOTHESIS DEVELOPMENT

Theory

This paper applies Petronio’s Communication Privacy Management theory and Altman’s Social Penetration Theory from communication to investigate what motivate users to disclose information in social networking sites, and how different privacy management strategies affect disclosure.
The Internet offers a platform for social interactions in which alternative forms of the self can be expressed (Sherry 1995; Bargh, McKenna et al. 2002). Such behaviors of self expression have important consequences for establishing liking, relationships and bonds of understanding with other people (Bargh, McKenna et al. 2002), prompting individuals to open their privacy boundaries depending on their needs, adjusting access as whenever necessary according to Altman’s Privacy Regulation Theory (1975) and CPM, or the Communication Privacy Management theory (Petronio, 2002).

Communication Privacy Management, or CPM, is an evidence-based theory about how people manage information, both theirs and others’ who have granted access to their information (Petronio,2002). The goal of CPM is to offer a theoretical perspective that suggests a way to understand the tension between revealing and concealing private information (Petronio 2007).

The theory of social penetration (Altman and Haythorn 1965) offers a framework for characterizing the development of interpersonal relationships. Social penetration refers to the reciprocal behaviors that occur between individuals in the development of an interpersonal relationship. These behaviors include exchange of information (e.g., attitudes, values, biographical-demographic, and personal data), exchange of expressions of positive and negative affect, and mutual activities. Interpersonal development is thought to proceed along two related dimensions, breadth of penetration, or the amount of interaction, information exchange, etc., per unit time (e.g., the amount of communication per week), and depth of penetration or the degree of intimacy of a typical interaction or exchange.

The advent of e-mails, blogs and social networking sites provide users multiple opportunities to engage in computer-mediated communication (CMC). As a result, privacy, communication, and technology are interwoven in critical ways.

3.2 Hypotheses

We propose the following:

H1: Greater privacy concern negatively influences disclosure.

H2a : Privacy concern negatively influences trust in the provider.

H2b : Privacy concern negatively influences trust in the members.

H3a : Trust of provider positively influences information self-disclosure

H3b: Trust of members positively influences information self-disclosure

H4: Trust of the provider mediates the relationship between privacy concern and information self-disclosure.

Hypothesis 5: Greater privacy concern is positively related to the use of “Careful” identity management strategy.
Hypothesis 6: Greater privacy concern is positively related to the use of “Customization” identity management strategy.

Hypothesis 7: Greater privacy concern is positively related to the use of “Secrecy” identity management strategy.

Hypothesis 8: The use of “Careful” identity management strategy is positively related to information self-disclosure.

Hypothesis 9: The use of “Customization” identity management strategy is positively related to information self-disclosure.

Hypothesis 10: “Secrecy” identity management strategy mediates the relationship between privacy concern and information disclosure.

Hypothesis 11: “Secrecy” identity management strategy mediates the relationship between privacy concern and information disclosure.

Hypothesis 12: “Careful” identity management strategy mediates the relationship between privacy concern and information disclosure.

Hypothesis 13: “Customization” of privacy settings mediates the relationship between privacy concern and information disclosure.

Hypothesis 14: “Customization” of privacy settings mediates the relationship between trust of member and information self-disclosure.

Privacy, Identity Management Strategies, and Information Disclosure

Privacy paradox. Recent surveys, anecdotal evidence, and experiments have highlighted the relevance of the privacy paradox: individuals state privacy concerns but behave in ways that seemingly contradict their statements (Acquisti 2004; Acquisti and Grossklags 2005; Squicciarini and Griffin 2012).

Sheehan and Hoy (1999) found that stated privacy concern correlates negatively with the reported frequency of registering with websites in the past and positively with providing incomplete information during registration (Sheehan and Hoy 2000). Secrecy, or providing incomplete information and or falsifying information is one way in which individuals seek to actively protect his/her privacy.

Control of personal information requires that an individual manages the outflow of information as well as the subsequent disclosure of that information to third parties (Hann, Hui et al. 2007). Individuals have various privacy control tactics at his/her own disposal in addition to, or in the absence of the controls required by the FTC. Customizing the privacy settings in Facebook is another privacy management strategy.
Being careful about friends and group membership or use mental control to limit the scope of disclosure is yet another strategy for privacy management.

**Note:** TR_P: Trust of provider; TR_M: trust of members; SF_DIS: self-disclosure

**Mediating Effects:**
- **H4a:** Trust of the provider mediates the relationship between privacy concern and information self-disclosure.
- **H4b:** Trust of the members mediates the relationship between privacy concern and information self-disclosure.
- **H12:** CAREFUL mediates the relationship between privacy concern and information self-disclosure.
- **H13:** CUSTOMIZE mediates the relationship between privacy concern and information self-disclosure.
- **H14:** CUSTOMIZE mediates the relationship between trust of member and information self-disclosure.

**FIGURE 1. Proposed Research Model**

**RESULTS AND DISCUSSION**

The results of this study delineate the complex process in which trust and subjective privacy management strategy choices influence information self-disclosure in social networking sites. Contrary to our expectation, privacy concern does not significantly influence disclosure in our research framework. However, trust and privacy management strategies may mitigate privacy concerns. In particular, privacy concern negatively and significantly influences both dimensions...
of trust- trust of provider and trust of members. As expected, trust of provider positively and significantly influences disclosure. Contrary to our expectation, trust of members alone has a small and significantly negative influence on disclosure. This result suggests that trust of members by itself has little effect on disclosure without any privacy management strategy in place. When trust of members is combined with customization strategy, customization might have a mediating effect on the relationship between trust of members and disclosure ($z=1.707<1.96^*$), though the result indicates that the effect is only borderline significant.

The results indicate that trust play an important role underlying self-disclosure in terms of both trust of provider and trust of members while privacy management strategies such as careful and secrecy have a positive but insignificant effect on quantity of self-disclosure, and customization of privacy settings has a negligible negative effect on information disclosure.

Contrary to our expectation, the secrecy strategy is not significantly related to privacy concern. This result is understandable in the context of social networking. In order to be visible to one’s old acquaintances and friends, one must keep his/her real identity visible.

**LIMITATIONS AND IMPLICATIONS FOR FUTURE RESEARCH**

Although the findings are potentially useful, the present study has certain limitations. First, our data does not originate from a random sample of Facebook users. Our trends are based on a panel of Facebook users dominated by students and adults affiliated with one university. Hence, our results may not extrapolate to more diverse samples of users. Second, the results may have been impacted by self-selection bias. Our sample comprises of only active participants. Individuals who had already ceased to participate in Facebook might have different perceptions about the influence of trust and privacy management strategies, and so could have been affected differently by them. Therefore, the results should be interpreted as only explaining information self-disclosure of current social networking sites users. Third, information self-disclosure is an on-going phenomenon. However, trust and privacy strategy factors were measured at a fixed point in time rather than over a period of time as they change, thus losing the richness of explanation. Future studies incorporate a longitudinal design and compare users’ initial and longer-term use of social networks for information self-disclosure in order to capture the dynamic process of information disclosure decisions.

**REFERENCES**


