Association for Information Systems
AIS Electronic Library (AISeL)

2009

"It Won't Happen To Me!": Self-Disclosure in Online Social Networks

Hanna Krasnova
Humboldt-University, Berlin, krasnovh@wiwi.hu-berlin.de

Elena Kolesnikova
Humboldt-University, Berlin, helena_kolesnikova@yahoo.de

Oliver Guenther
Humboldt-University, Berlin, guenther@wiwi.hu-berlin.de

Follow this and additional works at: http://aisel.aisnet.org/amcis2009

"IT WON'T HAPPEN TO ME!":
SELF-DISCLOSURE IN ONLINE SOCIAL NETWORKS

Hanna Krasnova
Humboldt-Universität zu Berlin
krasnovh@wiwi.hu-berlin.de

Elena Kolesnikova
Humboldt-Universität zu Berlin
helena_kolesnikova@yahoo.de

Oliver Günther
Humboldt-Universität zu Berlin
guenther@wiwi.hu-berlin.de

ABSTRACT

Despite the considerable amount of self-disclosure in Online Social Networks (OSN), the motivation behind this phenomenon is still little understood. Building on the Privacy Calculus theory, this study fills this gap by taking a closer look at the factors behind individual self-disclosure decisions. In a Structural Equation Model with 237 subjects we find *Perceived Enjoyment* and *Privacy Concerns* to be significant determinants of information revelation. We confirm that the privacy concerns of OSN users are primarily determined by the perceived likelihood of a privacy violation and much less by the expected damage. These insights provide a solid basis for OSN providers and policy-makers in their effort to ensure healthy disclosure levels that are based on objective rationale rather than subjective misconceptions.

Keywords

Social Networking, Privacy, Self-Disclosure, Optimistic Bias, Perceived Likelihood, Perceived Damage, Empirical Study.

INTRODUCTION

Participation in Online Social Networks (OSNs) has become part of daily routine for many Internet users worldwide. Facebook (2009) alone counts more than 200 million active members. OSN users are given the possibility to find friends and stay in contact quickly and efficiently. For example, a status update can be immediately transferred to everyone on one's friend's list and thus help to keep friendships alive. A myriad of living links among individuals allow participants to build up social capital – an individual investment that might prove crucial in the future (Ellison, Steinfield and Lampe, 2007).

Despite these positive social aspects, OSNs have become subject of growing critique with regard to privacy threats users face. User groups and online media including major news sites are continuously discussing privacy risks, warning members against revealing too much information (Boyd, 2008). Despite this rising privacy awareness, Facebook (2009) reports that "*More than 1 billion pieces of content*" are shared on its platform weekly.

The revelation of personal information despite existing privacy concerns is often called "privacy paradox" (Jensen, Potts and Jensen, 2005) and has been partly explained by the extensions of the Social Exchange theory (e.g. Hui, Tan and Goh, 2006) and Privacy Calculus theory (Dinev and Hart, 2006). In line their insights individuals are consciously weighing the risks and benefits of their disclosure. However, whereas the gratification is clear and immediate, the privacy risks are hard to assess (Aquisti, 2004). Dinev and Hu (2007) argue that an "It won't happen to me" attitude of users might explain much of the users' behavior.

Building on the Privacy Calculus theory, we aim to understand the dynamics behind self-disclosure on OSN platforms. Recognizing the role of benefits in the disclosure decision, in this article we pay specific attention to the risk variable of the disclosure equation. We empirically investigate the role of perceptions regarding (i) the *likelihood* and (ii) the *expected damage associated with a privacy violation* in the formation of individual privacy concerns. A deeper understanding how these factors affect user behaviour may help OSN providers and policy-makers to refine their efforts in encouraging more responsible information disclosure and communication.

RELATED WORK

Together with personally identifiable information, such as address, e-mail, or phone number, OSN users often reveal their tastes in music, books, movies, relationship status and friends' circle in their *profiles*. In addition they are given the opportunity to publicly *communicate* with other users by writing on their "wall", commenting or up-dating their status. User updates may be mirrored on Facebook in the News Feed section for others to observe.

Empirical research studying self-disclosure on OSNs remains limited. On the basis of a representative profile pool, Gross and Acquisti (2005) have demonstrated the massive character of the information disclosure phenomenon on Facebook as well as the underutilization of privacy settings. Dwyer, Hiltz and Passerini (2007) integrated Privacy Concern and Trust beliefs into an empirical model to explain individual information sharing on OSNs, concluding, however, that the relationship is still unclear.

In the online shopping context, the degree of self-disclosure relates mainly to individuals' perception of *privacy risks*, *trusting beliefs* and *benefits* from revelation (e.g. Chellappa and Sin, 2005). Dinev and Hart (2006) argue that when deciding to disclose information individuals are weighing the *benefits* and *risks* of their disclosure action.

Hui, Tan and Goh (2006) further posit that users can derive extrinsic and intrinsic benefits in the online environment. They argue that online platforms can use these benefits to induce information from customers. Taking a closer look at the OSN context, Rosen and Sherman (2006) argue that *Perceived Enjoyment* is the main motivator to use Social Networking platforms, which can be generally described as hedonic information systems.

Perceived Risk is typically viewed as a product of two variables: *Perceived Likelihood* of an event and *Perceived Damage* if the event takes place (Cunningham, 1967). These two constructs have been often researched as part of the Health Belief Model (Becker, 1974) which aims to understand what drives people to take health-related precautionary measures. Applied to the OSN context, these constructs can be the key to interpret the dynamics behind individual privacy risk perceptions and self-disclosure.

THE MODEL

Building on the literature insights described above and taking Privacy Calculus theory and the Health Belief Model as a basis for our model, we distinguish between two salient paths, which are assumed to independently influence the breadth (amount) of individual self-disclosure on OSN platforms: (i) *Perceived Benefits*, and (ii) *Privacy Concerns*. To understand the dynamics behind the formation of individual *Privacy Concerns* we integrate *Perceived Likelihood* and *Perceived Damage* constructs as main antecedents of the *Privacy Concerns* construct. In the following paragraphs, each model construct and related hypotheses are presented in detail.

Perceived Benefit: Enjoyment

Extrinsic benefits users derive from using the system have been continuously summarized under the umbrella of *Perceived Usefulness* construct, which is an essential component of the Technology Acceptance Model (TAM) by Davis (1989). Driven by the criticisms of the model inapplicability beyond the workplace, TAM has been extended to include a *Perceived Enjoyment* construct (Davis, Bagozzi and Warshaw, 1992). Later, Moon and Kim (2001) have shown that when applied to the Internet context *Perceived Playfulness*, a broader application of the original perceived enjoyment concept, has a more significant effect on individual attitudes towards the system than perceived usefulness. This result is rooted in the nature of many Internet applications, which are built around a pleasure component and whose usefulness is often hard to define.

Rosen and Sherman (2006) propose a modified TAM model, in which perceived usefulness is substituted by Perceived Enjoyment arguing that OSNs can be described as hedonic information systems with Enjoyment constituting their primary value. Similarly, Sledgianowski and Kulviwat (2008) have found Playfulness to be the strongest predictor of OSN intentional and actual use. Hogben (2007) mentions a sense of connectedness, self-enhancement, possibility to interact and share experiences with like-minded individuals as possible benefits of OSNs. Recognizing presence of numerous gratification elements OSNs provide, we consider Enjoyment to be their central benefit. Indeed, OSNs, such as Facebook or MySpace, are organized and presented in a way that enables pleasurable user experiences so that users participate and (self-) communicate more. Following Hui, Tan and Goh (2006) we assume that experiencing enjoyment can justify information disclosure in the eyes of a user. We hypothesize that:

Hypothesis 1: Perceived Enjoyment benefits are positively related to Self-disclosure.

Privacy Concerns

As discussed, the impact of privacy concerns on self-disclosure has been studied thoroughly within the online context (e.g. Chellappa and Sin, 2005; Malhotra, Kim and Agarwal, 2004). Hogben (2007) mentions that OSN privacy risks range from *organizational* threats such as e.g. digital dossier aggregation by the third parties to dangers stemming from the user *social* environment such as online stalking, bullying or reputation slander. Driven by media coverage, users are becoming increasingly aware of the privacy risks they face on the platform. In the light of daunting privacy concerns restriction of the amount of self-disclosure appears to be the most natural response. We hypothesize that:

Hypothesis 2: Privacy Concerns are negatively related to Self-disclosure.

Looking into the dynamics of individual risk perceptions, Aquisti (2004) argues that individuals are unable to correctly assess privacy-related risks due to incomplete information, bounded rationality and various psychological distortions, such as for example hyperbolic discounting, self-control bias or optimistic bias. Aiming to integrate elements of this theory into our model, we view *Privacy Concerns* as a product of two variables: *Perceived Likelihood* of an event and *Perceived Damage* if the event takes place (Cunningham, 1967). This causal structure is in line with the classical Health Belief Model, in which the impact of perceived susceptibility and severity on the preventive behavior is mediated by the perceived threat of disease (Becker, 1974).

Perceived Likelihood

The construct of *Perceived Likelihood* represents the subjective probability that a negative event will take place and corresponds to the notion of „susceptibility" used in the Health Belief Model often applied to predict the degree of the preventive behavior.

The individual assessment of the likelihood of negative events is often distorted due to the so-called *optimistic bias*. According to the optimistic bias theory, individuals tend to perceive negative events as less likely and positive events as more likely to happen to them (Higgins, St Amand and Poole, 1997). This phenomenon is typically described as "It won't happen to me" attitude and can been observed in many aspects of human behavior, such as e.g. Internet events (Campbell, Greenauer, Macaluso and End, 2007). The reasons for these distortions include egocentricity, focus on the base-rate information, as well as various motivational causes (e.g. Higgins, St Amand and Poole, 1997). Despite its partial usefulness in dealing with a stressful situation, unrealistic optimism may be a factor discouraging precautionary behavior, which in turn elevates the real risk of a negative event (Higgins, St Amand and Poole, 1997). Applied to OSN context, the "It won't happen to me" phenomenon can indeed explain massive information revelation and under-utilization of privacy controls despite looming privacy threats. Based on the previous studies (e.g. Campbell et al., 2007) we assume that Perceived Likelihood construct would implicitly include an optimistic bias effect.

Acquisti and Gross (2006) and Strater and Richter (2007) provide evidence for the privacy-related ignorance of users. According to their findings, users are neither able to assess the real accessibility of their profile, nor are they able to truly understand the legal consequences depicted in the OSN privacy policy. In fact, user knowledge about OSN provider and third party rights with regard to their information are plagued by misconceptions and false ideas. Our focus groups conducted in Germany have shown that users are often convinced that their information can be sold to third parties without asking for their consent – a practice strictly forbidden by law in Germany.

These arguments show that users are likely to misjudge the likelihood of privacy abuse happening to them. Aiming to understand the role of *Perceived Likelihood* in the formation of risk perceptions we integrate it as a direct antecedent of individual *Privacy Concerns* in our model. We hypothesize that:

Hypothesis 3: Perceived Likelihood of privacy threats is positively related to Privacy Concerns.

Perceived Damage

The *Perceived Damage* construct reflects the individual assessment of the magnitude of a negative event and its consequences. Studies, mostly dealing with health-related behavior, have shown a small but significant impact of this construct on behavior (e.g. Harrison, Mullen and Green, 1992).

Beyond financial loss as a result of e.g. identity theft, possible damage arising from participation in OSNs can be attributed to negative psychological and social consequences such as detrimental impact on one's sense of worth, social standing and relations, or employment. It is important to note that the perception of damage highly depends on personality and cultural context (Janz and Becker, 1984). For example, Muslim female OSN users are likely to perceive the revelation of an intimate relationship more damaging than their Western counterparts.

The expected magnitude of the damage resulting from such negative events as, for example, access to personal information by the potential employer, will be an important element contributing to individual privacy concerns. We hypothesize that:

Hypothesis 4: Perceived Damage from privacy threats is positively related to Privacy Concerns.

EMPIRICAL STUDY

Survey Design and Sampling

To evaluate the model, an empirical study was conducted in November 2008. An online questionnaire was distributed among Facebook users by posting in popular groups as well as by using student mailing lists. Each participant received a 5 Euro cash reward upon survey completion. As a result, 237 usable observations were obtained, 45.6% of them women, 73.4% students. 87.7% of the respondents were between 20-28 years old, 10.1% - between 30 – 39 years old. 58% of the participants were German and the rest were foreigners mainly living in Germany.

Development of Measurement Scales

We tried to use existing scales wherever possible. However, due to specific context of our study most of the scales had to be changed significantly or self-developed as shown in Table 1. The items for Privacy Concerns, Perceived Likelihood and Perceived Damage constructs were initially based on the formulations suggested by Dinev and Hart (2006), and then changed significantly to fit the OSN context. All items were anchored on a 7- point scale.

Category / Source	No of items	Examples of Items
Self-Disclosure (self-developed)	5	1. I have a comprehensive profile on Facebook; 2. I have a detailed profile on Facebook; 3. My profile tells a lot about me; 4. From my Facebook profile it would be easy to find out my preferences in music, movies or books; *Answer Categories: Strongly disagree - Strongly agree*
Perceived Enjoyment (partly based on Nambisan and Baron, 2007)	3	1. Spending time on Facebook is entertaining 2. I spend enjoyable and relaxing time on Facebook *Answer Categories: Strongly disagree - Strongly agree*
Privacy Concerns (some formulations partly based on Dinev and Hart, 2006)	4	How much are you concerned that the information submitted on Facebook: 1. ...can be used in a way you did not foresee 2. ...can become available to someone you don't want 3. ...can become available to someone without your knowledge *Answer Categories: Not concerned at all – Very much concerned*
Perceived Likelihood (some formulations partly adapted from Dinev and Hart, 2006)	4	Please assess the likelihood of the following events: Information you provide on Facebook: 1. … will be used in a way you did not foresee 2. … will be accessed by someone you don't want *Answer Categories: Not at all likely - Very likely*
Perceived Damage (some formulations partly adapted from Dinev and Hart, 2006)	4	Please assess the amount of the resulting damage to you (financial, to your reputation, social, psychological) if the following events took place? Information you provide on Facebook: 1. … was used in a way you did not foresee 2. … was accessed by someone you don't want *Answer Categories: Very low damage - Very high damage*

Table 1. Construct Operationalization

The dimensions of Self-Disclosure scales suggested by Wheeless and Grotz (1976) have been widely applied by researchers in the past. Nevertheless due to their focus on inter-personal communication, they do not fully reflect the communication dynamics specific to OSNs. Taking the "Amount" dimension of the Self-Disclosure Scale (Wheeless and Grotz, 1976) as a basis for our construct operationalization, we have developed new items which account for ways of how information can be communicated on an OSN.

In order to estimate the general perception of Likelihood and Damage and isolate the influence of the information already published on their profiles, an introductory phrase preceded questions for these both constructs: *"Please answer the following*

question independently of what and how much information you have on your profile at the moment! Imagine you are about to present yourself on Facebook by adding or updating some details (address, e-mail, relationship status, interests, your preferences, photos etc)". Our pre-test has shown that such introduction prevented users from a reverse understanding of the relation between likelihood/damage and self-disclosure.

It is important to note that we asked respondents to assess the amount of the resulting damage in a cumulative way. Despite a common practice of differentiating between various risk and hence damage dimensions separately (e.g. financial, social, psychological) (e.g. Kaplan, Szybillo and Jacoby, 1974; Krasnova, Rothensee and Spiekermann, 2007), our focus groups have shown that users often have difficulty to single out a particular damage type resulting from a disclosure of a specific information piece but are able to intuitively anticipate overall magnitude of possible loss based on knowledge or previous experience.

Research Methodology and Model Evaluation

The evaluation of the Structural Equation Model formulated on the basis of hypotheses H1-H4 involved two steps: First the *Measurement Model* (MM) and then the *Structural Model* (SM) were evaluated.

A Confirmatory Factor Analysis (CFA), using maximum likelihood estimation with AMOS 7.0 was used to assess reliability and validity of our MM. The items included into the analysis were restricted to load on their respective constructs, which were allowed to correlate. We first evaluated Internal Consistency, Convergent and Discriminant Validity of the measured constructs to ensure the validity of our MM as shown in Tables 2 and 3. Cronbach's Alpha exceeded the recommended value of 0.7 for all constructs providing evidence for their Internal Consistency (Nunnally, 1978). Furthermore, the Indicator Reliability, Composite Reliability and Average Variance Extracted (AVE) parameters were evaluated to ensure Convergent Validity. Eighteen out of twenty indicators of our MM had standardized loadings higher than 0.7 and only two were slightly lower than the required threshold (Bagozzi and Yi, 1988). Thus, indicator reliability was ensured. The Composite Reliability values for all constructs exceeded the cut-off value of 0.6 (Bagozzi and Yi, 1988). The AVE values for all measured constructs were higher than the required level of 0.5 (Fornell and Larcker, 1981).

Construct	Number of indicators	Composite Reliability	Average Variance Extracted (AVE)	Cronbach's Alpha
Self-Disclosure	5	0.900	0.645	0.893
Perceived Enjoyment	3	0.859	0.672	0.891
Privacy Concerns	4	0.884	0.657	0.882
Perceived Likelihood	4	0.839	0.569	0.807
Perceived Damage	4	0.865	0.618	0.860

Table 2. Quality criteria

Criterion for Discriminant Validity was also fulfilled as the AVE for all latent variables was higher than the squared correlation between a certain variable and all other latent variables in the model (Fornell and Larcker, 1981) as can be derived from Table 3.

Construct	SD	PE	PC	PL	PD
Self-Disclosure (SD)	*0.803*				
Perceived Enjoyment (PE)	0.301	*0.820*			
Privacy Concerns (PC)	-0.253	-0.101	*0.810*		
Perceived Likelihood (PL)	-0.119	-0.118	0.589	*0.754*	
Perceived Damage (PD)	-0.130	0.013	0.435	0.527	*0.786*

Table 3. Square Root of AVE (Diagonal Elements) and Correlation between Latent Variables (Off-diagonal Elements)

Further, measures of goodness of fit were evaluated for our MM. All required thresholds have been surpassed as shown in Table 4.

At the next step, the SM was assessed. Again, our SM met all cut-off goodness of fit criteria as shown in Table 4. As a result of SM evaluation, hypotheses 1, 2, 3, 4 were supported as shown in Figure 1, with our model explaining R^2 = 13.6% and 36.8% of the variance in Self-Disclosure and Privacy Concerns respectively.

An initial look at the path coefficients *Perceived Likelihood – Privacy Concerns (0.498)* and *Perceived Damage – Privacy Concerns (0.172)* hints at an interesting dynamics taking place in the formation of the individual *Privacy Concerns*. To shed the light on the differences in the impact of both constructs, the effect sizes of *Perceived Likelihood* and *Perceived Damage* were assessed, showing that whereas Perceived Likelihood has a *medium* effect size on *Privacy Concerns* (f^2=0.28), *Perceived Damage* has only a marginal effect size (f^2=0.03) (Cohen, 1988). Furthermore, a t-test rejected the equality of both path coefficients (t-statistic equals 2.76), providing evidence that *Perceived Likelihood* has a stronger impact on *Privacy Concerns* than *Perceived Damage*. These findings provide evidence for the importance of *Perceived Likelihood* in the formation of *Privacy Concerns*.

Goodness-of-Fit Measure	Recommended Value / Source	CFA Results	SM Results
χ^2/df	< 2.00 (Carmines and McIver, 1981)	1.592	1.574
GFI	> 0.90 (Jöreskog and Sörborm, 1989)	0.908	0.907
AGFI	> 0.80 (Jöreskog and Sörborm, 1989)	0.879	0.880
RMSEA	< 0.06 (Jöreskog and Sörborm, 1989)	0.050	0.049
CFI	> 0.95 (Hu and Bentler, 1999)	0.963	0.964
IFI	> 0.95 (Hu and Bentler, 1999)	0.964	0.964
TLI	> 0.95 (Hu and Bentler, 1999)	0.957	0.958

Table 4. Goodness-of-Fit Measures
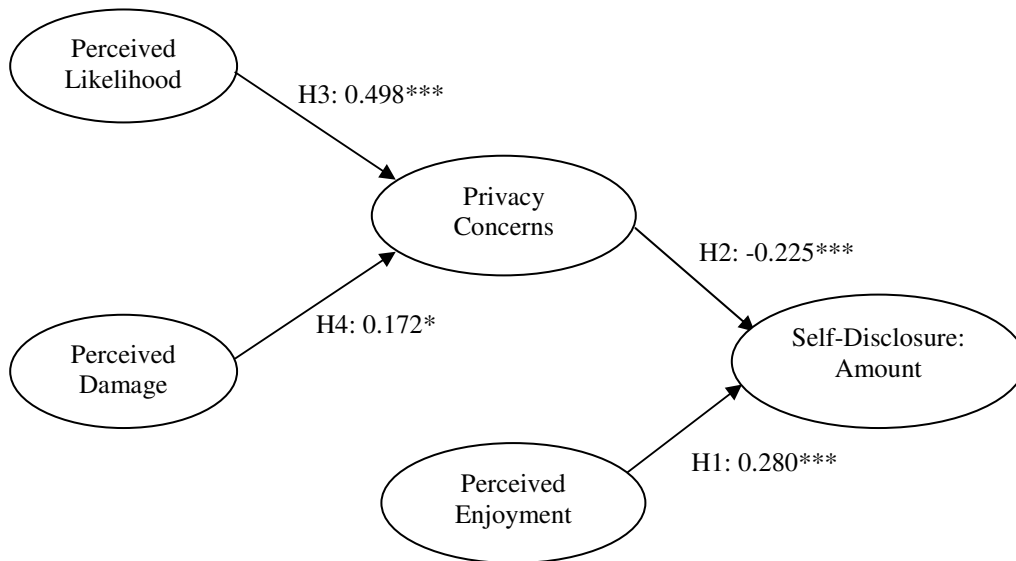
*: Significance at 5%. **: Significance at 1%. ***: Significance at 0.1%;

Figure 1. The Structural Model

DISCUSSION AND MANAGERIAL IMPLICATIONS

Our results provide an empirical basis for OSN providers and public policy-makers for refining their efforts in encouraging more responsible information disclosure without undermining OSN sustainability.

Our findings confirm the presence of privacy calculus (Dinev and Hart, 2006) in the self-disclosure behaviour on OSNs, thereby providing an explanation to the 'concern – behaviour' dichotomy discussed in previous studies (Acquisti and Gross, 2006). In absolute terms, the effect of both Privacy Concerns and Perceived Enjoyment are similar, which hints at the comparable importance of both variables in the disclosure decision. Despite being aware of the privacy risks on the platform, OSN users may reveal personal information in the process of looking for fun. Indeed, OSNs are often described as hedonic platforms with participants looking for entertainment and distraction from everyday routines. Our findings confirm that by investing into platform interactivity, curiosity-stimulating features and other pleasure-invoking functionality OSN providers can ensure an appropriate level of communication necessary for long-term self-sustainability of their site.

Privacy Concerns were found to be a significant impediment to self-disclosure with Perceived Likelihood and Perceived Damage being significant antecedents. We have empirically shown that Perceived Likelihood has a stronger impact on Privacy Concerns than Perceived Damage and hence plays a more important role in its formation. Taking into account the susceptibility of the Perceived Likelihood construct to the Optimistic Bias, it becomes clear that users might indeed care about their privacy less than they should, due to probability misjudgment. In addition, Perceived Likelihood can be miscalculated due to lacking knowledge on the profile accessibility, effectiveness of privacy settings, as well as legal implications of the privacy policy. Driven by common misconceptions users might get more worried about unrealistic risks and ignore imminent threats.

Our model and empirical findings can also help to explain why "*more than 70% of Facebook users engage with Platform applications*" monthly (Facebook, 2009), even though they are explicitly warned beforehand that their information possibly becomes accessible to this application. Whereas gratification in the form of enjoyment is immediate, privacy risks are vague. Users often think that third parties have little interest in their data and consider their information trivial. They also assume to be protected by privacy legislation. All these factors reduce the perceived likelihood of the data misuse. All in all, our model shows that even though individuals do integrate privacy concerns into their self-disclosure decision, they base their concerns on their perception of the risks – which can be "optimistically biased" or subject to false beliefs (Acquisti, 2004).

In line with our results, policy-makers and OSN providers are advised to provide users with more information that can help users to adequately assess individual risk predisposition. Indeed, according to Becker (1974)'s Health Belief Model, individuals should be provided with adequate action cues to enable more rational decisions. On the functionality side, OSN providers might integrate intuitive privacy indices showing users the level of their protection from various threats. Apart from helping users to make more informed decisions regarding self-disclosure, these measures will help to build trust in OSN provider, as shown by previous studies (e.g. Culnan and Armstrong, 1999).

CONCLUSION

This study contributes to a better understanding of privacy calculus dynamics behind the self-disclosure decision process on OSNs. We show that Perceived Enjoyment and Privacy Concerns play a key role in this process. Further, we confirm that privacy concerns are primarily determined by the individual perception of likelihood and much less by the expected damage of privacy breaches. These insights provide a solid basis for OSN providers and policy-makers in their effort to ensure healthy disclosure levels based on objective rationale rather than subjective misconceptions.

REFERENCES

1. Acquisti, A. (2004) Privacy in Electronic Commerce and the Economics of Immediate Gratification, *Proceedings of the ACM Conference on E-Commerce*, New York, USA, ACM Press, 21-29.

2. Acquisti, A. and Gross, R. (2006) Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook, *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, Cambridge, UK, Berlin: Springer-Verlag, 36-58.

3. Bagozzi, R. P. and Yi, Y. (1988) On the evaluation of structural equation models, *Journal of the Academy of Marketing Science*, 16, 1, 74-94.

4. Becker, M. (1974) The Health Belief Model and Personal Health Behavior, *Health Education Monographs*, 2, 4.

5. Boyd, D. (2008) Facebook's Privacy Trainwreck: Exposure. Invasion. and Social Convergence, *Convergence: The International Journal of Research into New Media Technologies*, 14, 1, 13-20.

6. Campbell, J., Greenauer, N., Macaluso, K. and End, C. (2007) Unrealistic Optimism in Internet Events, *Computers in Human Behavior*, 23, 1273-1284.

7. Carmines, E. G. and McIver, J. P. (1981) Analyzing models with unobserved variables: Analysis of covariance structures, in G. W. Bohrnstedt and E.F. Borgatta, (eds.) *Social measurement: Current issues*, Newbury Park: Sage.

8. Chellappa, R. K. and Sin, R. (2005) Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma, *Information Technology and Management*, 6, 2-3, 181 – 202.

9. Cohen, J. (1988) Statistical Power Analysis for the Behavioral Sciences, 2nd ed., Academic Press, New York.

10. Culnan, M. J. and Armstrong, P. (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation, *Organization Science*, 10, 1, 104.

11. Cunningham, S. M. (1967) The Major Dimensions of Perceived Risk, in Cox. D. (Eds.) *Risk Taking and Information Handling in Consumer Behavior*, Harvard University Press, Boston, 82-108.

12. Davis, F. D. (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology, *MIS Quarterly*, 13, 3, 319–340.

13. Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1992) Extrinsic and intrinsic motivation to use computers in the workplace, *Journal of Applied Social Psychology*, 22, 14, 1111-1132.

14. Dinev, T. and Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, 17, 1, 61-80.

15. Dinev, T., and Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies, *Journal of the AIS*, 8, 7, 386-408.

16. Dwyer, C., Hiltz, S. R. and Passerini, K. (2007) Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace, *Proceedings of the Thirteenth American Conference on Information Systems*, Keystone, USA.

17. 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, article 1.

18. Facebook.com (2009), Statistics, Press Center [WWW document] http://www.facebook.com/press/info.php?statistics (accessed 18th April 2009).

19. Fornell, C. and Larcker, D. F. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research*, 18, 3, 39-50.

20. Gross, R. and Acquisti, A. (2005) Information Revelation and Privacy in Online Social Networks (The Facebook case), *Proceedings of the ACM Workshop on Privacy in Electronic Society*, November 7, Alexandria, VA, USA, ACM Press, 71-80.

21. Harrison, J. A., Mullen, P. D. and Green, L. W. (1992) A meta-analysis of studies of the Health Belief Model with adults, *Health Education Research*, 7, 107-116.

22. Higgins, N. G., St Amand, M. D. and Poole, G. D. (1997) The Controllability Of Negative Life Experiences Mediates Unrealistic Optimism, *Social Indicators Research*, 42, 299–323.

23. Hogben, G. (2007) Security Issues and Recommendations for Online Social Networks, ENISA Position Paper (1).

24. Hu, L. and Bentler, P. M. (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, *Structural Equation Modeling*, 6, 1, 1-55.

25. Hui, K-L., Tan, B. C. Y. and Goh, C-Y. (2006) Online Information Disclosure: Motivators and Measurements, *ACM Transactions on Internet Technology*, 6, 4, 415-441.

26. Janz, N. K. and Becker, M. H. (1984) The health belief model: A decade later, *Health Education Quarterly*, 11, 1-47.

27. Jensen, C., Potts, C. and Jensen, C. (2005) Privacy Practices of Internet Users: Self-reports versus observed behavior, *International Journal Human-Computer Studies*, 63, 1-2, 203-227.

28. Jöreskog, K. G. and Sörbom, D. (1989) LISREL-7 user's reference guide, Mooresville: Scientific Software.

29. Kaplan, L., Szybillo, G. and Jacoby, J. (1974) Components of Perceived Risk in Product Purchase: A Cross-Validation, *Journal of Applied Psychology*, 59, 3, 287-291.

30. Krasnova, H., Rothensee, M. and Spiekermann, S., Perceived Usefulness of RFID-enabled Information Services – A Systematic Approach, *Wirtschaftsinformatik 2007 (WI'07)*, Karlsruhe, March, 2007.

31. 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, 336-355.

32. Moon, J. W. and Kim, Y. G. (2001) Extending the TAM for a World-Wide-Web Context, *Information and Management*, 38, 217-230.

33. Nambisan, S. and Baron, R. (2007) Interactions in Virtual Customer Environments: Implications for Product Support and Customer Relationship Management, *Journal of Interactive Marketing*, 21, 2, 42-62.

34. Nunnally, J. C. (1978) Psychometric Theory, 2nd edition, New York: McGraw-Hill.

35. Rosen, P. and Sherman, P. (2006) Hedonic Information Systems: Acceptance of Social Networking Website. In *Proceedings of the Twelfth Americas Conference on Information Systems*, August 4-6, Acapulco. Mexico.

36. Sledgianowski, D. and Kulviwat, S. (2008) Social Network Sites: Antecedents of User Adoption and Usage. *Proceedings of AMCIS*, Toronto, Canada, Paper 83.

37. Strater, K. and Richter, H. (2007) Examining Privacy and Disclosure in a Social Networking Community, *Proceedings of the 3rd symposium on Usable privacy and security*, Pittsburgh, ACM International Conference Proceeding Series, Vol. 229, 157-158.

38. Wheeless, L. R., and Grotz, J. (1976) Conceptualization and measurement of reported self-disclosure, *Human Communication Research*, 2, 4, 338-346.