Analyzing the Problem of Employee Internal Social Network Site Avoidance: Are Users Resistant due to their Privacy Concerns?

Ricardo Buettner

FOM University of Applied Sciences, Institute of Management & Information Systems, Germany
ricardo.buettner@fom.de

Abstract

I investigate the phenomenon of user resistance behavior concerning internal social networking sites through an empirical analysis of the behavioral attitudes of 253 working professionals from various sectors and all company sizes. Results from linear regression analysis indicates the importance the role of privacy concerns play in explaining user resistance behavior phenomenon. In addition, I found considerable negative interrelations between privacy concerns and perceived usefulness ($r_{PC-PU} = -0.421$) as well as privacy concerns and perceived ease of use ($r_{PC-PE} = -0.459$). Results from structural equation modeling using privacy concerns, usefulness and ease of use reveals an impressive predictive power ($R^2 = 0.731$).

1. Introduction

I define an internal social networking site (ISNS) as a social networking site (SNS, [1]) which is operated by a company, whose access is restricted to members of this company and which offers the members of the company the possibility to set up a personal profile and to connect with other members of the company. Hence, my definition does not include inter-organisational networks as examined in [2]–[4].

More and more companies such as IBM, Microsoft, Deloitte or Best Buy have implemented their own ISNS to internally improve the knowledge management and the building and maintaining of relationships with coworkers [5]–[13]. Companies have invested considerable amounts of money [13]–[16], time [15,16] and human resources [16] in ISNSs resulting in a great functionality and usability potential [13]–[23]. However, a lot of employees avoid using it [24]–[26].

To try to explain this resistance[1] behavior, research first focused on the established information systems (IS) acceptance models (e.g. TAM [29], UTAUT(2) [30,31]) and also confirmed influences of these classical/general factors for ISNSs (most important: perceived usefulness [19,32] and ease of use [33]). After that, in order to try to improve the prediction power of the classical IS acceptance models, researchers extended the models by non-individual factors (cultural factors, geographic location, social/peer group influence, relational ties, management support, one's rank in the hierarchy, or incentives [19,23,32]–[36]).

Recent research is currently also focusing on individual factors such as trust [32,33], risk [32] or controllability [19]. Interestingly, research lacks any investigation of the role of privacy concerns as an explanatory factor for the usage intention of ISNSs, even though IS-research revealed privacy concerns as an important user resistance factor in general [37]–[44] and also on public SNS [41,45]–[52]. In addition, there is not only a gap in the extant literature concerning privacy concerns as antecedents of ISNS resistance but also on the interplay between privacy concerns and the classical/general factors of ISNS usage (i.e. perceived usefulness [19,32] and ease of use [33]).

This is a very interesting research gap because privacy concerns may explain the still empirically observed ISNS avoidance behavior of employees [24]–[26] despite huge company investments in usefulness and ease of use resulting in a greater functionality and usability potential [13]–[23]. There is thus a theoretical gap concerning the role of privacy concerns in ISNS usage. As prior research has shown that the cost-benefit ratio [37,40,53]–[56] of publishing private information is much higher (especially more risky) in working/employer-employee settings compared to public environments [40,45,57]–[64], it can be spec-

---

1. I use the word "resistance" as the opposite of acceptance (following [27]); other researchers defined "resistance" as an own construct (e.g. [28]).

ulated that privacy concerns can significantly explain the avoidance problem of employees not using the companies' ISNS.

That is why in this paper I empirically analyze the influence of privacy concerns on the intention to use an ISNS by studying working professionals from various sectors and any company sizes. To the best of my knowledge, there is no other similar study. Not only could results from this investigation have implications for theorizing the role of privacy concerns in ISNS usage but they may also have implications for the importance of managing privacy concerns by the companies.

The paper is organized as follows: Section 2 spans the research background from ISNSs (2.1) via the research results on ISNS acceptance (2.2) to the state of the art of privacy concerns in public and internal SNSs (2.3) – thus identifying the research need. In section 3 the research methodology is presented, including the research model and the hypotheses (3.1) as well as the sampling strategy (3.2) and all measurements (3.3). Section 4 contains the results including sample characteristics (4.1), socio-demographic effects on privacy concerns (4.2), a comparison of users and non-users (4.3), linear regression analysis outcomes (4.4), structural model results (4.5) and model quality evaluation outcomes (4.6). The results are discussed in section 5. Finally, the conclusion is given in section 6, including limitations (6.1) and future research (6.2).

2. Research Background

2.1. Internal social networking sites

As various possibilities exist for implementing social media into the internal communication processes of companies, many different versions and descriptions of tools implementing social media in companies have been developed. Similarly, research on the topic sees different expressions employed to describe these features, social software [19], employee portals [65]–[67], business-to-employee-portals [65,68], wikis or weblogs [19], enterprise social software platforms [33], intra-organizational electronic networks [35] and enterprise social networks [34]. Most of these applications share the common feature that access is restricted to company members and that employees may set up an account and connect with others.

One of the main applications of ISNSs lies in the domain of knowledge management. Therefore, various studies have investigated ISNS-based knowledge management practices and the factors affecting knowledge sharing in ISNSs [5]–[8]. Even more specifically, the

performance of teams using ISNSs for knowledge sharing has been investigated [9]–[12]. Various other aspects of ISNSs have also been examined in recent years. A major part of the research on ISNSs focuses on the assessment of their success, key factors for successful implementation and improvement potentials [23,66,67,69]. Another major research stream shows the many individual and competitive advantages accompanying the usage of ISNSs in companies such as supporting communication [13,15,20], collaboration [13,13,15,20] and relationships between colleagues [13,19]; or the improvement of the individuals' and organizations' knowledge base [13,15,19,20] and the innovation- [15], morale- [17], cost- [15,23], turnover- [17], and productivity-situation [13,15,17,19]–[22].

However, despite of all these advantages there is still a limited practical use for it among employees [24]– [26]. Therefore, my research is focused on understanding the adoption of ISNSs.

2.2. Acceptance research on internal social networking sites

Early research on the acceptance and the intention to use (IU) ISNSs started around 2000 with examinations of the adoption and development of intranets [70]. Simultaneously with the development of the Web 2.0, early research on Web 2.0 technologies, e.g. social networking sites, in companies and their growing importance emerged [71]–[73]. Since then, a lot of research has been conducted on different factors influencing the adoption of ISNSs. Research revealed (1) perceived usefulness [19,32] and (2) ease of use [33] as the most important factors of ISNS acceptance – in line with prior knowledge from established IS acceptance models (e.g. TAM [29], UTAUT(2) [30,31]). However, despite huge company investments in usefulness and ease of use of their ISNS, a lot of employees still avoid using it [24]–[26].

That is why recent research currently also focuses on non-individual factors (cultural factors, geographic location, social and peer group influence, relational ties, management support, one's rank in the company hierarchy, or incentives [19,23,32]–[36]) and individual factors such as trust [32,33], risk [32] or controllability [19]. Interestingly, there is a lack of research into the role of privacy concerns [37] as an explanatory factor for the usage intention of ISNSs, even though it is known from IS-literature that privacy concerns are a very important user resistance factor [37]–[44,56], especially on *public* SNSs [41,45]–[52].

2.3. Privacy concerns as an important factor explaining user resistance

IS-research revealed privacy concerns (PC) as an important user resistance factor [37]–[44,56]. Specifically, a lot of research exists on PC-conceptualizing (e.g. [37,38,74]), individual differences such as personality [39] or non-individual influences such as culture [41], the coherent negative impact of PC on IU [74] and typical user responses to information privacy threats [42]. Interestingly, research shows that perceived benefits such as money [55], usefulness [75] and ease of use features [76] may outweigh PC.

2.3.1. Privacy concerns on public social network sites. PC regarding IS usage and especially internet and social media usage are a widely researched phenomenon. Various papers investigate internet users' PC in general (e.g. [38,43,44,77,78]), their privacy-protection methods [42,79], or more specifically the relationship between personality traits and PC [39]. PC regarding public SNSs is a widely research field of study. Part of the existing literature examines the implications of PC on self-disclosure on public SNSs [41,45,46]. The improvement of privacy settings and consequently the support of user participation on SNSs are also main research topics [47,49]. Cultural differences regarding PC on public SNSs [41,48,50] and distinctions between different public SNSs regarding PC were also investigated [51]. Additionally, there is research on PC perceptions and reality [80], the influence of PC on quitting behavior of SNSs [81] and the measurement of online privacy management [52]. The results of all these studies confirmed that PC play a major role as a resistent factor on *public* SNSs.

2.3.2. Privacy concerns on internal social networking sites. PC on ISNSs are less widely investigated. There is some work that examines the privacy-related concepts of trust [32,33] and confidentiality [65,68]. Donston-Miller [82] identified security and privacy risks for organizations and their customers accompanying ISNSs. Andriole [15] states serious concerns about intellectual property, proprietary information, privacy, security, and control on ISNSs. Wang and Kobsa [83] hypothesize a number of potential privacy issues relating to ISNSs such as impression management, peer pressure to reveal personal or working information or unintentional social undermining in the workplace, and suggest future research directions in this area. However, to the best of my knowledge, there is no further research on PC on ISNSs and their implications for the adoption of ISNSs in particular.

3. Methodology

3.1. Research model and hypothesizing

To analyze the impact of PC on IU an ISNS I adapted the technology acceptance model (TAM [29]) to ISNS and extended it by the PC construct. The resulting research model is shown in figure 1.
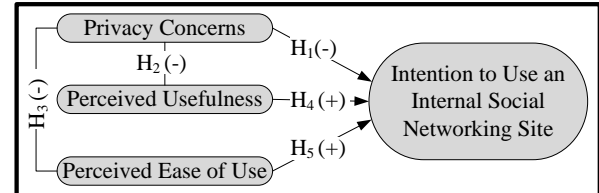

Figure 1: Research model and hypotheses

Literature on public SNS reveals a negative influence of PC on self-disclosing behavior on public SNSs [41,45,46] and a higher user participation on SNSs if PC are decreased [49]. PC were even found to be reasons for quitting SNSs [81]. In addition, meta-analytical research from *general online information* PC show a stable negative impact of PC on IU [74, p. 465]. Against this background, I hypothesize that:

H_1:   *PC will be negatively associated with the (continued) intention to use ISNSs.*

Dinev et al. argue that PC are "not absolute but [...] based on a cost-benefit analysis, that is, a calculus of behavior" [37, p. 299]. This calculus perspective is described in the literature as "the most useful framework for analyzing contemporary consumer privacy concerns" [54, p. 326]. From this perspective perceived benefits may have a huge impact on PC [53], e.g. monetary or non-monetary benefits [55] or information-giving [56]. Li and Unger [40] showed that "under certain circumstances, perceived personalization quality can outweigh the impact of privacy concerns" [40, p. 621]. Interestingly, besides monetary benefits [55] there are two major factors which potentially outweigh privacy concerns: (1) usefulness [75] and (2) ease of use features such as the facility of customizing IS [76]. Consequently, PC are not a fixed to a static value [37, p. 299]. They potentially negatively interrelate with PU [75] and PE [76]. Thus, I hypothesize that:

H_2:   *PC will be negatively associated with PU.*

H_3:   *PC will be negatively associated with PE.*

According to multiple initial studies [29]–[31,84] and the up-to-date meta-analytical review by Hess et al. [85, p. 19], both, PU and PE, are universally positively associated with behavioral intention. Against this background, I hypothesize that:

H_4: *PU will be positively associated with the (continued) intention to use ISNSs.*

H_5: *PE will be positively associated with the (continued) intention to use ISNSs.*

I consequently hypothesize the assumed negative impact of PC on IU (H_1), the negative interplay of PC and PU (H_2) as well as PC and PE (H_3), and the positive impact of PU on IU (H_4) as well as PE on IU (H_5). All hypotheses are shown in figure 1. The research question (RQ) was formulated as follows: *Do Privacy Concerns influence the (continued) intention to use Internal Social Network Sites stronger than Perceived Usefulness and Perceived Ease of Use do?*

3.2. Sampling strategy

I recruited *working professionals* who studied extra-occupationally at our university. The participants were electronically asked to take part in a survey concerning social networks. The call for participation was sent out with a link to the online questionnaire via our Germany-wide university. Working backgrounds were checked (see section 4.1).

3.3. Measurements

All constructs of the research model (figure 1) were operationalized by proven and established measurement instruments (see table 1). As shown by many researchers the TAM [29] was proven numerous times before to have a high level of construct reliability [85] (Chronbach's α were often above 0.9 which indicates redundance of the used items). I select three items for each of the constructs PU and PE from [29, p. 340]. For my purposes, I need to measure the specific PC representing a person's privacy concerns in a given IS-specific context, not a person's general overall concern for information privacy (cf. [74, pp. 466] and [77, p. 800]). That is why the PC items were taken from [77, p. 823] and adapted to the ISNS-context. The IU items were adapted from [30, p. 460] and [84, p. 314]. Each item was measured using a 7-point Likert scale. Furthermore I captured sociodemographic data and the occupational background of each participant.

4. Results

4.1. Sample characteristics

Data were collected via an online-based questionnaire. 280 completed questionnaires were received. After removing invalid (27) answers, 253 questionnaires

Table 1: Measurement items for constructs (* – reverse coded item)

Construct	Item	Question	References
Perceived Usefulness (PU)	PU-1	Using an ISNS in my job would enable me to accomplish tasks more quickly.	Davis [29]
	PU-2	Using an ISNS would improve my job performance.	
	PU-3	I would find an ISNS useful in my job.	
Perceived Ease of Use (EU)	PE-1	My interaction with an ISNS would be clear and understandable.	
	PE-2	I would find an ISNS inflexible to work with.*	
	PE-3	It would be difficult for me to become skillful at using an ISNS.*	
Privacy Concerns (PC)	PC-1	I am concerned that the information I submit to an ISNS could be misused.	Xu et al. [77]
	PC-2	I am concerned that others can find private information about me from an ISNS.	
	PC-3	I am concerned about providing personal information to an ISNS, because of what others might do with it.	
	PC-4	I am concerned about providing personal information to an ISNS, because it could be used in a way I did not foresee.	
Intention to Use (IU)	IU-1	I continue using/will use an ISNS.	Following Venkatesh et al. [30] and Venkatesh & Bala [84]
	IU-2	I continue sharing/will share information via an ISNS.	
	IU-3	(Assuming I had access to an ISNS,) I intend to use an ISNS.	
	IU-4	I will suggest using an ISNS to others.	

($\sim 90\%$) were used within my analysis. Criteria for invalid answers were (a) quite similar/equal answer patterns, and (b) inconsistent responses identified by reversed coded items (1). The remaining participants are aged from 19 to 60 years (M=28.5, S.D.=6.8). 137 ($\sim 54\%$) of the test persons are female, 116 male.

The participants are currently working in 33 different sectors (i.e. services industry (66), banking/finance (40), information technology (38), metal and electrical industries (25), retail industry (14), public administration (12), healthcare (11), chemical industry (8), education and research (7), other manufacturing industries (7), construction/mining (6), military (5), gastronomy (4), others (10)) of any company sizes (1-99 employees (51), 100-499 (42), 500-999 (30), 1,000-1,999 (21), 2,000-2,999 (19), 3,000-5,000 (15), >5,000 (72), n.a. (3)).

The participants comprised of 51 individuals ($\sim 20.2\%$) who are already using an ISNS in their company, 185 individuals ($\sim 73.1\%$) who do not use an ISNS in their company and 17 individuals ($\sim 6.7\%$) with no answer regarding whether they use an ISNS in their company.

All measured items from table 1 were normally distributed (Kolmogorov-Smirnov-Z test, SPSS 17.0).

4.2. Sociodemographic privacy concern effects

I found no significant gender effects on the PC-related items PC-1 to PC-4. Indeed, in line with prior research (e.g. the meta-analytical review of Li [74]) in my sample women are also (very slightly) more concerned about their privacy ($\varnothing_\Delta = 0.05$), but this difference is not significant. However, I found mixed effect results of age on privacy concerns. While there are no effects of age on PC-1 and PC-4 I found age-effects for PC-2 and PC-3 ($r_{PC-2}^{Pearson} = 0.144, r_{PC-3}^{Pearson} = 0.162$, $p < 0.05$). The mixed age-effects were consistent with the literature (cf. [74, p. 461]).

4.3. Comparison of ISNS users and non-users

In order to investigate potential between-group differences of ISNS users and non-users I visually present all 253 participants on a three-dimensional graphic in figure 2. As a result, there are no clear visual systematic differences between the three groups (users, non-users, no answer) concerning the data-room $[PU, PE, PC]$.
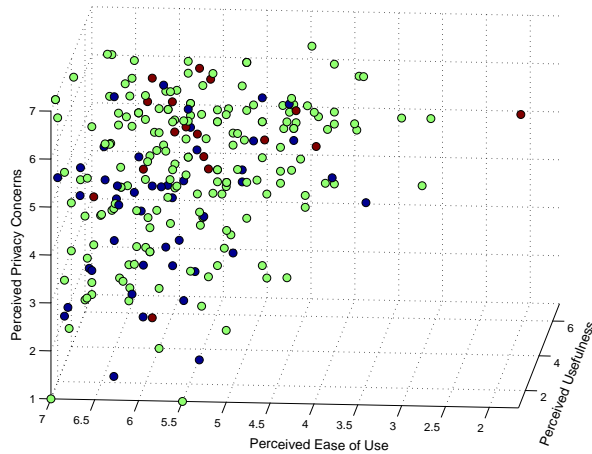

Figure 2: Comparison of individuals who are Company-ISNS users (blue), non-users (green) or individuals with no answer (brown).

A discriminant analysis of the independent variable triple $[PU, PE, PC]$ concerning the dependent group variable (user, non-user, no answer) shows no separation efficiency. Compared to the a priory probability of 33.3% only 37.1% could be classified correctly by the discrimination function (SPSS 17.0, data record deletion when missing values). Also the discriminant analysis of the independent quadruple $[PU, PE, PC, IU]$

shows no better results (36.5% correct classifications). However as shown in table 2 the privacy concerns (PC) may eventually be suitable to predict the user status (user, non-user, no answer).

Table 2: Univariate separation efficiency of the independent variables PU, PE, PC, IU

Var.	Wilks-Lambda	F	df1	df2	Significance
PU	0.986	1.695	2	241	0.186
PE	0.978	2.661	2	241	0.072
PC	0.937	8.117	2	241	0.00039***
IU	0.989	1.297	2	241	0.275

In contrast to this speculation a more detailed discriminant analysis if the PC-related items $[PC - x, x = 1..4]$ can predict user status (user, non-user, no answer) failed again (only 37.2% correct classifications). But as shown in table 3 the PC-x items systematically differ between the user status groups. Non-users are more concerned about their privacy (three of four items significantly differ). Interestingly, participants who did not answer the question as to whether they use an ISNS show very high PC values ($\geqslant 5.65$).

Table 3: Test of between-user-status group significance of the PC-related items

Item	Mean ($\varnothing$)			Test of significance (t-test, p-value)		
	User	Non-U.	No Ans.	User/Non-U.	User/No A.	Non-U./No A.
PC-1	3.88	4.86	5.71	0.00054***	0.00035***	0.058
PC-2	3.75	4.75	5.82	0.004**	0.00002***	0.005**
PC-3	4.80	4.99	5.94	0.474	0.014*	0.011**
PC-4	4.25	5.04	5.65	0.006**	0.008**	0.170

4.4. Exploring the Intention to Use function and linear regression analysis results

In a next step I visually analyze the 253 $[PU, PE, PC, IU]$ data points on a scatter plot using MATLAB R0214a. As shown in figure 3 it seems to be a functional interrelation in a manner that high PU- combined with low PC-values lead to high IU-values and vice versa. PE-values seem not to play a major role when explaining IU as the PE-values visually occur almost relative high. In fact, a statistical analysis using SPSS 17.0 reveals relative high PE-ratings at a small variance ($(\mu, \delta)_{PE-1} = (5.74, 1.11), (\mu, \delta)_{PE-2} = (5.18, 1.34) (\mu, \delta)_{PE-3} = (5.86, 1.31)$; item rating $(1...7)$).

In order to understand the influences of $[PU, PE, PC]$ on IU I carried out a linear regression analysis (SPSS 17.0) using the mean values of the $PU - x$, $PE - x$, $PC - x$ and $IU - x$ items. As a result I could explain 64.9% of the IU variance with
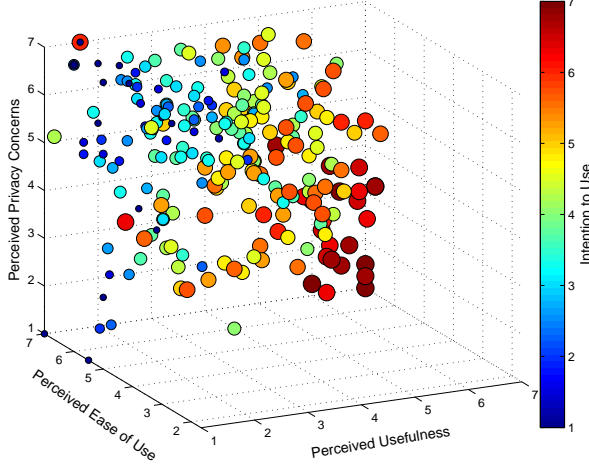
Figure 3: Visual representation of the IU-dependency based on $[PU, PE, PC]$ from low Intention to Use (small blue bubble) to high (big dark red bubble).

the following formula (adjusted $R^2 = 0.649$, $df = 3$, $F = 151.018$):

$$IU = 0.686 * PU + 0.121 * PE - 0.159 * PC$$

When I expose a two factor model to competition ($PU + PE$ versus $PU + PC$), the latter wins. While PU and PE together explain 63.1 % of the IU variance ($df = 2$, $F = 208.478$), PU and PC together explain 63.7 % ($df = 2$, $F = 216.451$). This is a first indication that privacy concerns are potentially more important compared to perceived ease of use when explaining the intention to use an ISNS.

4.5. Structural model results

To investigate the latent structure of the hidden constructs PU, PE, PC, and IU and their causal relations with more sophistication, I conducted a structural equation modeling using smartPLS, version 2.0.M3 by [86]. The model used the reflective indicators as described in table 1. Conducting the bootstrapping algorithm of smartPLS [86] ($n = 5,000$ samples) I found that all path coefficients were significant ($p < 0.001$). As a result, figure 4 shows the structural model explaining 73.1% of the intention to use an ISNS ($R^2 = 0.731$).

4.6. Structural model quality

As shown in figure 4, all reflective indicators load at a significance level of $p < 0.001$ from 0.607 to 0.952. The average variance extracted (AVE) values are greater than 0.5 for each construct (table 4).
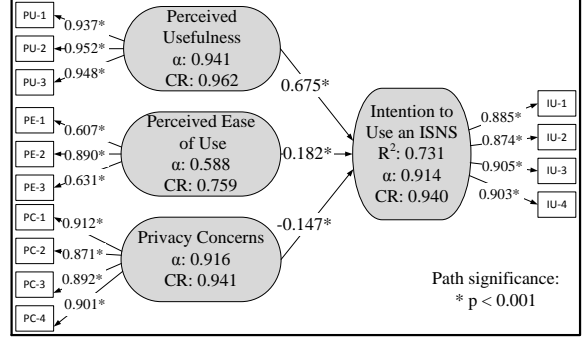

Figure 4: Structural Model: Values and significance of path coefficients and factor loadings

Table 4: Quality criteria: average variance extracted (AVE), Chronbach's (α), composite reliability (CR), diagonal contains $\sqrt{AVE}$ values

	AVE	α	CR	PU	PE	PC	IU
PU	0.895	0.941	0.962	0.946			
PE	0.520	0.588	0.759	0.459	0.721		
PC	0.799	0.916	0.941	−0.421	−0.459	0.894	
IU	0.796	0.914	0.940	0.820	0.559	−0.515	0.892

The internal consistency of all constructs is given as both values, Cronbach's α and composite reliability CR, were greater than 0.7 for each construct (table 4, cf. [87]), except PE (α failed, CR is ok). In addition, the discriminant validity check was successful. Finally, the Fornell-Larcker criterion [88] is also fulfilled as $\sqrt{AVE(construct_i)} < CORR_{construct_i, construct_j}$ (table 4). In summary I can state that the measurement model is valid (cf. [89]).

4.7. A comparison of the relative importance of privacy concerns

Despite the high R^2 value of the structural model in figure 4, the effect size when including PC into the TAM is only weak ($f^2 = 0.037$, cf. [89]). However, when I expose a two factor model to competition ($PU + PE$ vs. $PU + PC$), both models reach similar variance results ($R^2_{[PU,PE] \to [IU]} = 0.721$, $R^2_{[PU,PC] \to [IU]} = 0.714$).

5. Discussion

I revealed a significant impact of PC on IU of -0.147 (figure 4) and consequently support hypothesis H_1 ($p < 0.001$). The standardized path coefficient $c_{PC-IU} = -0.147$ is in line with prior research results as the meta-analytical review on privacy concerns of Li [74] shows an empirical range of $[-0.107 \leqslant c_{PC-IU} \leqslant 0.710]$ [74, p. 465].

As shown in table 4 I found considerable negative correlations between PC–PU of $r_{PC-PU} = -0.421$ ($p < 0.001$, support of H_2) as well as between PC–PE by $r_{PC-PE} = -0.459$ ($p < 0.001$, support of H_3).

Furthermore I found significant path coefficients between both the PU–IU and the PE–IU relationships which leads to the support of both H_4 and H_5 ($p < 0.001$). Comparing these results with the up-to-date meta-analysis of Hess et al. [85] I can state that my path coefficient $c_{PC-IU} = 0.675$ matches the calculated mean of $c_{PC-IU}^{\varnothing} = 0.609$ (cf. [85, p. 19]). In contrast, my $c_{PE-IU} = 0.182$ does not match the meta-analytical results of $c_{PE-IU}^{\varnothing} = 0.555$ (cf. [85, p. 19]). Interestingly, in my results the intention to use an ISNS is much more influenced by perceived usefulness instead of perceived ease of use.

In addition, as shown in section 4.5 I can explain 73.1% of the intention to use an ISNS ($R^2 = 0.731$). This result is impressive because both UTAUT [30] and UTAUT2 [31] reach similar R^2 values for usage intention (UTAUT $R^2 = 0.77$ [30, p. 465], UTAUT2 $R^2 = 0.74$ [31, p. 169]), but included much more constructs (UTAUT includes eight and UTAUT2 ten constructs/moderators). My model only needs three constructs (PU, PE, PC).

Furthermore, results from linear regression analysis and structural model results indicate that privacy concerns are at least as important compared to perceived ease of use when explaining ISNS usage intention.

The implications of this research are twofold. From a theoretical point of view, an ISNS-situational substitution of perceived ease of use by privacy concerns is potentially indicated but needs further investigation. At least the $[PU, PC] \rightarrow [IU]$ model is a serious alternative to TAM [29] when analyzing ISNS usage behavior. From a practical point of view, companies should invest in lowering ISNS-specific privacy concerns such as trust-building measures or monetary compensations before implementing the ISNS (cf. [32,33,40,55,56,75, 76,90]), as it was shown in my study that privacy concerns have a major impact on the ISNS usage intention (similar to the importance of perceived ease of use). This practical recommendation is underpinned by the fact that prior research revealed that specific privacy concerns are not absolute [37,54] but changeable by activities/benefits [40,53,55,56,75,76]. In addition, due to the considerable influence of perceived usefulness and perceived ease of use on the ISNS usage intention and due to the negative interrelations between privacy concerns and perceived usefulness ($r_{PC-PU} = -0.421$) as well as between privacy concerns and perceived ease of use ($r_{PC-PE} = -0.459$) system designers and implementing companies should pay attention both

to usefulness and ease of use. Since the impact of perceived usefulness on the usage intention is enormous ($c_{PC-IU} = 0.675$) system designers are advised to further strengthen the communication- [13,15,20], collaboration- [13,13,15,20], relationship- [13,19] and information-functions [13,15,19,20]. Companies are advised to motivate their employees by pointing to these ISNS-advantages in order to strengthen their perception of useful ISNS features.

6. Conclusion

Addressing the ISNS avoidance problem of employees [24]–[26] I investigated the role of privacy concerns on that problem, in particular on the impact of privacy concerns on intention to use an ISNS and the interplay between privacy concerns and usefulness as well as ease of use. Conducting an empirical analysis of the behavioral attitudes of 253 working professionals who had extensive industry experience coming from different sectors and all company sizes, my results indicate the important role of privacy concerns when explaining the ISNS avoidance problem. Considering the privacy concerns, perceived usefulness and perceived ease of use in a structural model explaining the intention to use an ISNS, I reach an impressive predictive power ($R^2 = 0.731$). Finally, I showed the practical and theoretical implications of these findings.

6.1. Limitations

One limitation of my study concerns the measurement quality of the PE construct, as Chronbach's α was only 0.588. However, I used three of the six original items from [29, p. 340] since in numerous studies Chronbach's α were often above 0.9 which indicates redundance of the used items. Despite the bad α value, the PE construct reliability in terms of the composite reliability ($CR = 0.759$) was fine [89]. Another limitation is the problem that I do not know from the respondents who do not use an ISNS if they have never used ISNSs because the company they work for has not adopted ISNSs, or if they have used ISNSs before but have stopped using it.

6.2. Future research

Subsequent research should focus on the possibilities of reducing ISNS-specific privacy concerns through company activities and benefits (cf. [40,53, 55,56,75,76]). In addition, future research should investigate the moderator effect of trust on the negative

PC–IU relationship as prior research, e.g. [50,56], indicated that trust may weaken the PC–IU relationship. Finally I found an interesting phenomenon in my data (Figure 5), namely that people either report a high usage intention always combined with high ratings on perceived usefulness and low on privacy concerns or vice versa (low usage intention always combined with low usefulness and high privacy concern ratings). This phenomenon could be explained by an individual's tendency to reduce cognitive dissonance (cf. [91]), i.e. either I like/use it and everything is perfect which leads to the exclusion of any privacy concerns or I do not like/use it and everything is bad including the appearance of an individual's privacy concerns. This is also a consideration for future research.
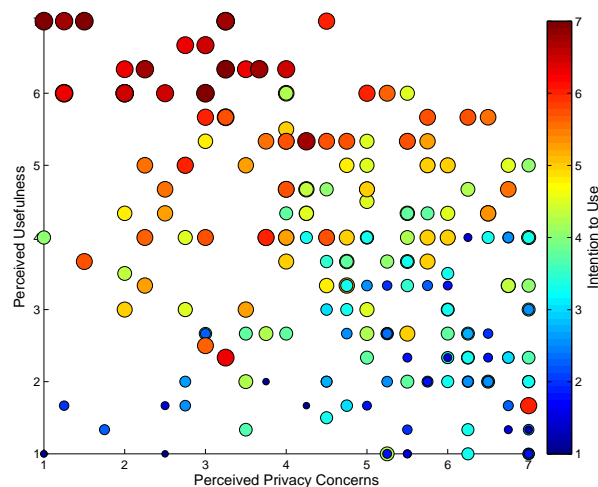

Figure 5: "Either-or principle": Either people like/use ISNSs and report subsequently high usefulness and low privacy concern rating or vice versa. [Intention to use from low (small blue bubble) to high (big dark red bubble)].

Acknowledgments

References

[1] d. m. boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship," *JCMC*, vol. 13, no. 1, pp. 210–230, 2008.

[2] M. Ibrahim, P. M. Ribbers, and B. Bettonvil, "Human-knowledge resources and interorganisational systems," *ISJ*, vol. 22, no. 2, pp. 129–149, 2012.

[3] P. Kazienko, N. Szozda, T. Filipowski, and W. Blysz, "New business client acquisition using social networking sites," *Electr Markets*, vol. 23, no. 2, pp. 93–103, 2013.

[4] W. Y. C. Wang, M. S. H. Heng, and P. Y. K. Chau, "The adoption behaviour of information technology industry in increasing business-to-business integration sophistication," *ISJ*, vol. 20, no. 1, pp. 5–24, 2010.

[5] A. Braganza, R. Hackney, and S. Tanudjojo, "Organizational knowledge transfer through creation, mobilization and diffusion: a case analysis of InTouch within Schlumberger," *ISJ*, vol. 19, no. 5, pp. 499–522, 2009.

[6] R. M. Davison, C. X. J. Ou, and M. G. Martinsons, "Information technology to support informal knowledge sharing," *ISJ*, vol. 23, no. 1, pp. 89–109, 2013.

[7] D. Sedera and G. G. Gable, "Knowledge Management Competence for Enterprise System Success," *JSIS*, vol. 19, no. 4, pp. 296–306, 2010.

[8] G. von Krogh, "How does social software change knowledge management? Toward a strategic research agenda," *JSIS*, vol. 21, no. 2, pp. 154–164, 2012.

[9] A. Majchrzak, A. Malhotra, and R. John, "Perceived Individual Collaboration Know-How Development Through Information Technology-Enabled Contextualization: Evidence from Distributed Teams," *ISR*, vol. 16, no. 1, pp. 9–27, 2005.

[10] P. H. Gray, "The effects of knowledge management systems on emergent teams: towards a research model," *JSIS*, vol. 9, no. 2-3, pp. 175–191, 2000.

[11] R. F. Easley, S. Devaraj, and J. M. Crant, "Relating Collaborative Technology Use to Teamwork Quality and Performance: An Empirical Analysis," *JMIS*, vol. 19, no. 4, pp. 247–265, 2003.

[12] S. Kudaravalli and S. Faraj, "The Structure of Collaboration in Electronic Networks," *JAIS*, vol. 9, no. 10, pp. 706–726, 2008, article 1.

[13] J. M. DiMicco, W. Geyer, D. R. Millen, C. Dugan, and B. Brownholtz, "People Sensemaking and Relationship Building on an Enterprise Social Network Site," in *HICSS '09 Proc.*, 2009, pp. 1–10.

[14] S. J. Barnes, M. Böhringer, C. Kurze, and J. Stietzel, "Towards an Understanding of Social Software: The Case of Arinia," in *HICSS '10 Proc.*, 2010, pp. 1–9.

[15] S. J. Andriole, "Business Impact of Web 2.0 Technologies," *CACM*, vol. 53, no. 12, pp. 67–79, 2010.

[16] A. Stocker and K. Tochtermann, "Exploring the Value of Enterprise Wikis - A Multiple-Case Study," in *KMIS'09 Proc.*, 2009.

[17] H. Koch, E. Gonzalez, and D. Leidner, "Bridging the work/social divide: the emotional response to organizational social networking sites," *EJIS*, vol. 21, no. 6, pp. 699–717, 2012.

[18] M. Kügler and S. Smolnik, "Just for the Fun of It? Towards a Model for Assessing the Individual Benefits of Employees' Enterprise Social Software Usage," in *HICSS '13 Proc.*, 2013, pp. 3614–3623.

[19] P. Raeth and S. Smolnik, "Antecedents and Consequences of Corporate Weblog Usage in the Intranet: A Process Perspective," in *HICSS '10 Proc.*, 2010, pp. 1–10.

[20] P. Raeth, M. Kügler, and S. Smolnik, "The Impact of Organizational Social Web Site Usage on Work Performance: A Multilevel Structural Interaction

Perspective," in *HICSS '12 Proc.*, 2012, pp. 4011–4020.

[21] L. Wu, "Social Network Effects on Productivity and Job Security: Evidence from the Adoption of a Social Networking Tool," *ISR*, vol. 24, no. 1, pp. 30–51, 2013.

[22] A. Majchrzak, C. Wagner, and D. Yates, "Corporate Wiki Users: Results of a Survey," in *WikiSym '06 Proc.*, 2006, pp. 99–104.

[23] J. Bughin, "The rise of enterprise 2.0," *J Direct Data Digit Mark Pract*, vol. 9, no. 3, pp. 251–259, 2008.

[24] M. Healey, "Why Enterprise Social Networking Falls Short," *IW*, March 4 2012.

[25] M. Healey, "DISLIKE - Why employees arent taking to enterprise social networks, and what IT can do to help," *IW*, January 30 2012.

[26] D. F. Carr, "10 Enterprise Social Networking Obstacles," *IW*, January 03 2012.

[27] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Manage Sci*, vol. 35, no. 8, pp. 982–1003, 1989.

[28] H.-W. Kim and A. Kankanhalli, "Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective," *MISQ*, vol. 33, no. 3, pp. 567–582, 2009.

[29] F. D. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MISQ*, vol. 13, no. 3, pp. 319–340, 1989.

[30] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MISQ*, vol. 27, no. 3, pp. 425–478, 2003.

[31] V. Venkatesh, J. Y. L. Thong, and X. Xu, "Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology," *MISQ*, vol. 36, no. 1, pp. 157–178, 2012.

[32] G. Harden, "Knowledge Sharing in the Workplace: A Social Networking Site Assessment," in *HICSS '12 Proc.*, 2012, pp. 3888–3897.

[33] M. Kügler, S. Smolnik, and P. Raeth, "Determining the Factors Influencing Enterprise Social Software Usage: Development of a Measurement Instrument for Empirical Assessment," in *HICSS '13 Proc.*, 2013, pp. 3635–3644.

[34] J. Cao, H. Gao, L. E. Li, and B. Friedman, "Enterprise Social Network Analysis and Modeling: A Tale of Two Graphs," in *IEEE INFOCOM '13 Proc.*, 2013, pp. 2382–2390.

[35] R. Teigland, M. Wasko, and F. Landqvist, "Examining knowledge exchange and organizational outcomes within intra-organizational electronic networks of practice with restricted access," in *ECIS '06 Proc.*, 2006, paper 143.

[36] J. Yang, Z. Wen, L. Adamic, M. Ackerman, and C.-Y. Lin, "Collaborating Globally: Culture and Organizational Computer-Mediated Communications," in *ICIS '11 Proc.*, 2011, paper 3.

[37] T. Dinev, H. Xu, J. H. Smith, and P. Hart, "Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts," *EJIS*, vol. 22, no. 3, pp. 295–316, 2013.

[38] W. Hong and J. Y. L. Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MISQ*, vol. 37, no. 1, pp. 275–298, 2013.

[39] I. A. Junglas, N. A. Johnson, and C. Spitzmüller, "Personality traits and concern for privacy: an empirical study in the context of location-based services," *EJIS*, vol. 17, pp. 387–402, 2008.

[40] T. Li and T. Unger, "Willing to pay for quality personalization? Trade-off between quality and privacy," *EJIS*, vol. 21, no. 6, pp. 621–642, 2012.

[41] P. B. Lowry, J. Cao, and A. Everard, "Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures," *JMIS*, vol. 27, no. 4, pp. 163–200, 2011.

[42] J.-Y. Son and S. S. Kim, "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MISQ*, vol. 32, no. 3, pp. 503–529, 2008.

[43] F. Stutzman, R. Capra, and J. Thompson, "Factors mediating disclosure in social network sites," *Comput Hum Behav*, vol. 27, no. 1, pp. 590–598, 2011.

[44] Z. Tufekci, "Can You See Me Now?: Audience and Disclosure Regulation in Online Social Network Sites," *B Sci Technol Soc*, vol. 28, no. 1, pp. 20–36, 2008.

[45] R. Chen, "Living a private life in public social networks: An exploration of member self-disclosure," *DSS*, vol. 55, no. 3, pp. 661–668, 2013.

[46] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)," in *WPES '05 Proc.*, 2005, pp. 71–80.

[47] S. Weiss, "Privacy threat model for data portability in social network applications," *Int J Inform Manage*, vol. 29, no. 4, pp. 249–254, 2009.

[48] H. Krasnova and N. F. Veltri, "Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA," in *HICSS '10 Proc.*, 2010, pp. 1–10.

[49] H. Krasnova, E. Kolesnikova, and O. Guenther, "Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study," in *ECIS '10 Proc.*, 2010, paper 160.

[50] H. Krasnova, E. Kolesnikova, and O. Günther, "One Size Fits All? Managing Trust and Privacy on Social Networking Sites in Russia and Germany," in *ECIS '11 Proc.*, 2011, paper 71.

[51] L. Sørensen, "User managed trust in Social Networking - comparing Facebook, MySpace and Linkedin," in *Wireless VITAE '09 Proc.*, 2009, pp. 427–431.

[52] C. Dwyer, S. R. Hiltz, M. S. Poole, J. Gußner, F. Hennig, S. Osswald, S. Schließlberger, and B. Warth, "Developing Reliable Measures of Privacy Management within Social Networking Sites," in *HICSS '10 Proc.*, 2010, pp. 1–10.

[53] B. Berendt, O. Günther, and S. Spiekermann, "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior," *CACM*, vol. 48, no. 4, pp. 101–106, 2005.

[54] M. J. Culnan and R. J. Bies, "Consumer Privacy: Balancing Economic and Justice Considerations," *J Soc Issues*, vol. 59, no. 2, pp. 323–342, 2003.

[55] H. Li, R. Sarathy, and H. Xu, "Understanding Situational Online Information Disclosure as a Privacy Calculus," *JCIS*, vol. 51, no. 1, pp. 62–71, 2010.

[56] J. C. Zimmer, R. Arsal, M. Al-Marzouq, D. Moore, and V. Grover, "Knowing your customers: Using a

reciprocal relationship to enhance voluntary information disclosure," *DSS*, vol. 48, no. 2, pp. 395–406, 2010.

[57] E. Christofides, A. Muise, and S. Desmarais, "Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes?" *CyberPsychol Behav*, vol. 12, no. 3, pp. 341–345, 2009.

[58] H. K. Davison, C. C. Maraist, R. H. Hamilton, and M. N. Bing, "To Screen or Not to Screen? Using the Internet for Selection Decisions," *Employee Resp Rights J*, vol. 24, no. 1, pp. 1–21, 2012.

[59] H. Krasnova, O. Günther, S. Spiekermann, and K. Koroleva, "Privacy concerns and identity in online social networks," *Identity Inform Soc*, vol. 2, no. 1, pp. 39–63, 2009.

[60] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online social networks: why we disclose," *JIT*, vol. 25, no. 2, pp. 109–125, 2010.

[61] K. Lewis, J. Kaufman, and N. Christakis, "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," *JCMC*, vol. 14, no. 1, pp. 79–100, October 2008.

[62] L. Massari, "Analysis of MySpace user profiles," *ISF*, vol. 12, no. 4, pp. 361–367, September 2010.

[63] D. L. Stone, K. M. Lukaszewski, E. F. Stone-Romero, and T. L. Johnson, "Factors affecting the effectiveness and acceptance of electronic selection systems," *HRMR*, vol. 23, no. 1, pp. 50–70, 2013.

[64] H. Zafar, "Human resource information systems: Information security concerns for organizations," *HRMR*, vol. 23, no. 1, pp. 105–113, 2013.

[65] L.-F. Sugianto and D. R. Tojib, "Modeling User Satisfaction with an Employee Portal," *Int J Bus Inform*, vol. 1, no. 2, pp. 239–255, 2006.

[66] N. Urbach, S. Smolnik, and G. Riempp, "An empirical investigation of employee portal success," *JSIS*, vol. 19, no. 3, pp. 184–206, 2010.

[67] N. Urbach, S. Smolnik, and G. Riempp, "Determining the Improvement Potentials of Employee Portals Using a Performance-based Analysis," *Bus Proc Manage J*, vol. 17, no. 5, pp. 829–845, 2011.

[68] D. R. Tojib, L.-F. Sugianto, and S. Sendjaya, "User satisfaction with business-to-employee portals: conceptualization and scale development," *EJIS*, vol. 17, no. 6, pp. 649–667, 2008.

[69] M. Steinhüser, S. Smolnik, and U. Hoppe, "Towards a Measurement Model of Corporate Social Software Success - Evidences from an Exploratory Multiple Case Study," in *HICSS '11 Proc.*, 2011, pp. 1–10.

[70] J. Bansler, J. Damsgaard, R. Scheepers, E. Havn, and J. Thommesen, "Corporate Intranet Implementation: Managing Emergent Technologies and Organizational Practices," *JAIS*, vol. 1, no. 1, 2000, article 10.

[71] A. P. McAfee, "Enterprise 2.0: The Dawn of Emergent Collaboration," *MIT Sloan Manage Rev*, vol. 47, no. 3, pp. 21–28, 2006.

[72] J. Sena and M. Sena, "Corporate Social Networking," *IIS*, vol. 9, no. 2, pp. 227–231, 2008.

[73] D. Stenmark, "Web 2.0 in the Business Environment: The New Intranet or a Passing Hype?" in *ECIS 2008 Proc.*, 2008, paper 35.

[74] Y. Li, "Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework," *CAIS*, vol. 28, pp. 453–496, 2011.

[75] N. F. Awad and M. S. Krishnan, "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingeness to be Profiled Online for Personalization," *MISQ*, vol. 30, no. 1, pp. 13–28, 2006.

[76] I.-H. Hann, K.-L. Hui, S.-Y. T. Lee, and I. P. L. Png, "Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach," *JMIS*, vol. 24, no. 2, pp. 13–42, 2007.

[77] H. Xu, T. Dinev, J. Smith, and P. Hart, "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *JAIS*, vol. 12, no. 12, pp. 798–824, 2011.

[78] H. Krasnova, N. F. Veltri, and O. Günther, "Self-disclosure and Privacy Calculus on Social Networking Sites: The Role of Culture - Intercultural Dynamics of Privacy Calculus," *BISE*, vol. 4, no. 3, pp. 127–135, 2012.

[79] A. Viejo, D. Sánchez, and J. Castellà-Roca, "Preventing automatic user profiling in Web 2.0 applications," *Knowl-Based Syst*, vol. 36, pp. 191–205, 2012.

[80] M. Netter, M. Riesner, M. Weber, and G. Pernul, "Privacy Settings in Online Social Networks - Preferences, Perception, and Reality," in *HICSS '13 Proc.*, 2013, pp. 3219–3228.

[81] S. Stieger, C. Burger, M. Bohn, and M. Voracek, "Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters," *Cyberpsychol Behav Soc Netw*, vol. 16, no. 9, pp. 629–634, 2013.

[82] D. Donston-Miller, "Our Love-Hate Relationship With Enterprise Social Networking," *IW*, February 14 2012.

[83] Y. Wang and A. Kobsa, "Privacy in Online Social Networking at Workplace," in *CSE '09 Proc.*, vol. 4, 2009, pp. 975–978.

[84] V. Venkatesh and H. Bala, "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sci*, vol. 39, no. 2, pp. 273–315, 2008.

[85] T. Hess, A. L. McNab, and A. Basoglu, "Reliability Generalization of Perceived Ease of Use, Perceived Usefulness, and Behavioral Intentions," *MISQ*, vol. 38, no. 1, pp. 1–28, 2014.

[86] C. M. Ringle, S. Wende, and A. Will. (2005) Smartpls 2.0 (beta). University of Hamburg. http://www.smartpls.de.

[87] W. Revelle, "Hierarchical Clustering and the Internal Structure of Tests," *Multivar Behav Res*, vol. 14, no. 1, pp. 57–74, 1979.

[88] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *J Marketing Res*, vol. 18, no. 1, pp. 39–50, 1981.

[89] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks: Sage, 2013.

[90] Z. Tang, Y. J. Hu, and M. D. Smith, "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor," *JMIS*, vol. 24, no. 4, pp. 153–173, 2008.

[91] L. Festinger, H. W. Riecken, and S. Schachter, *When Prophecy Fails: A social and psychological study of a modern group that predicted the destruction of the world*. Minneapolis, MN: UMP, 1956.