2010

Leveraging Trust and Privacy Concerns in Online Social Networks: An Empirical Study

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

Elena Kolesnikova
Humboldt University, helena_kolesnikova@yahoo.de

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

LEVERAGING TRUST AND PRIVACY CONCERNS IN ONLINE SOCIAL NETWORKS: AN EMPIRICAL STUDY

Journal:	*18th European Conference on Information Systems*
Manuscript ID:	ECIS2010-0375
Submission Type:	Research Paper
Keyword:	Human-computer interaction, Online communities, Privacy/information privacy, Structural modeling

LEVERAGING TRUST AND PRIVACY CONCERNS IN ONLINE SOCIAL NETWORKS: AN EMPIRICAL STUDY

Krasnova, Hanna, Humboldt-Universität zu Berlin, Institute of Information Systems, Spandauerstr 1, 10178 Berlin, Germany, krasnovh@wiwi.hu-berlin.de

Kolesnikova, Elena, helena_kolesnikova@yahoo.de

Günther, Oliver, Humboldt-Universität zu Berlin, Institute of Information Systems, Spandauerstr 1, 10178 Berlin, Germany, guenther@wiwi.hu-berlin.de

Abstract

Unprecedented success of Online Social Networks, such as Facebook, has been recently overshadowed by the privacy risks they imply. Weary of privacy concerns and unable to construct their identity in the desired way, users may restrict or even terminate their platform activities. Even though this means a considerable business risk for these platforms, so far there have been no studies on how to enable social network providers to address these problems. This study fills this gap by adopting a fairness perspective to analyze related measures at the disposal of the provider. In a Structural Equation Model with 237 subjects we find that ensuring interactional and procedural justice are two important strategies to support user participation on the platform.

Keywords: Social Networking, Privacy, Trust, Fairness, Justice, Identity, Structural Equation Modeling, Empirical Study.

1 INTRODUCTION[1]

Millions of users are flocking daily to Online Social Networks (OSNs) like Facebook or StudiVZ. Enormous popularity of these web-sites has its roots in the unique opportunities OSNs have to offer: possibility to manage one's identity and context in the desired way by allowing users to consciously self-present and control the image they project to others (Ellison et al. 2006, Krasnova et al. 2009a). In addition, by allowing users to efficiently keep in touch and develop relationships, OSNs promise to create social capital – an important contribution to the modern society and a source of their public value (Ellison et al. 2007).

However, OSNs' ability to create individual and public value is increasingly challenged by a wave of privacy critique coming from various stakeholders, who often question whether OSN participation is worth the risks. Sensitized by a number of privacy-related scandals and media attention, users are becoming more cautious in their self-communication on the platform (Boyd 2008). Even though this development can be viewed as a positive achievement from the point of view of privacy watchdogs, it also puts the long-term sustainability of OSNs at risk and, hence, threatens to undermine their public value. Indeed, dynamic self-disclosures keep the content of the OSN up-to-date – an important factor in ensuring stable user come-back rates and involvement. Furthermore, the content of self-presentation – information disclosed by users on OSNs - constitutes the basis for OSNs' commercial valuation (Krasnova et al. 2009b). By relying on personalized advertising, data-mining, and customer segmentation as important sources of their revenue, OSN providers may view voluntarily up-dated user profiles as a key to their long-term commercial survival.

However, despite the threats these developments bring with them, no studies exist to empower OSN providers with effective and practical means to leverage user privacy concerns and ensure healthy levels of self-presentation. Such means are, however, necessary to ensure the public value of these platforms is secured. Filling this gap we take a systematic view of the measures available to OSN providers. In a Structural Equation Model with 237 subjects we evaluate effectiveness of various means in reducing user privacy concerns and enhancing trust – two determinants of importance for user participation and self-disclosure levels. The insights from our study can serve as roadmap for OSN providers who can then invest their efforts and money into specific mechanisms to alleviate user privacy concerns, promote an atmosphere of trust and thereby increase user activity and network sustainability.

2 RELATED WORK

Several studies exist exploring the drivers and impediments behind user OSN participation. Typically, a 'privacy calculus' perspective is adopted to explain an often paradoxical user behavior (Acquisti and Gross 2006). In line with this approach, individual participation is a product of two paths: anticipated benefits (e.g. enjoyment, social acceptance) on the one hand and costs (e.g. privacy concerns) on the other hand (e.g. Dinev and Hart 2006). Users are expected to weigh both sides and act accordingly. Applying this framework, Krasnova et al. (2009c) find that privacy concerns, reflecting "*concerns about possible loss of privacy as a result of information disclosure*" (Xu et al. 2008, p.4), are negatively and the benefits of enjoyment are positively related to information disclosure on OSNs. However, whereas ensuring enjoyment as part of the user experience has always been a top priority for OSN providers, user privacy concerns have often been neglected (Boyd 2008). A study by Rizk et al (2009) shows that OSN providers themselves are often viewed as a source of privacy threats, as users

[1] This research was funded by the European Fund for Regional Development and the Berlin Senate Department for Economics (project "Wireless City").

fear that they can engage in the aggregation and use of personal information for marketing purposes as well as share it with third parties such as for example advertising or recruiting agencies. Apart from privacy risks originating from an OSN provider, OSN users may face specific privacy-related dangers rooted in the public availability of their data (Krasnova et al. 2009a). Digital dossier aggregation by third parties, face recognition and linkability to anonymous profiles, refined spear phishing, online stalking or bullying by OSN members are only a few among the myriad of threats users face online (Hogben 2007). Taking into account the negative impact these threats are expected to have on user participation (Krasnova et al., 2009c), addressing user concerns should be a priority for OSN providers.

Beyond anticipated benefits, Dwyer et al. (2007) argue that trusting beliefs may also counter-balance the negative influence of privacy concerns and thereby support healthy information sharing levels. Even now, despite the presence of the imminent privacy threats, users continue to self-communicate on OSN platforms, which can be a result of users' trust in the OSN Provider (Acquisti and Gross 2006). Mayer et al. (1995, p. 716) define trust as "*the willingness of a party to be vulnerable to the actions of another party*". Thus, users might rely on the OSN provider not to abuse their information for its personal gain. Supporting this argument, Dwyer et al. (2007) has found that Facebook members had higher levels of trust in Facebook and were more willing to share personal information as opposed to MySpace users. According to McKnight et al. (2002, p. 314) "*merely believing that the vendor is competent, benevolent and honest may go a long way towards persuading a user to share information*".

Overall, privacy-related literature from other contexts also supports the centrality of anticipated benefits (Krasnova et al. 2009c), privacy concerns (e.g. Dinev and Hart 2006) and trusting beliefs (e.g. McKnight et al. 2002) as central determinants of user participation and information disclosure online. However, whereas OSN providers do have the means to influence user perceptions regarding privacy concerns and trusting beliefs, beliefs regarding benefits are often formed intrinsically and may depend on many other contextual factors including the network structure a user possesses. Hence, reducing user privacy concerns and enhancing trust may represent two important strategies for the OSN providers in their attempt to make a turning point in the 'privacy calculus' equation. In other words, the challenge for the OSN provider lies in finding *operable means to mitigate concerns and increase trust*.

Son and Kim (2008) apply a justice/fairness framework to identify relevant antecedents of the individual behavioral responses to the privacy threats. In fact, the fairness dimensions have received wide acceptance in the organizational studies due to the relative ease with which they can be translated into specific actions thereby providing a guideline for management (e.g. Aryee et al. 2002). Culnan and Bies (2003) differentiate between three types of fairness perceptions relevant for the consumer: distributive, procedural and interactional. They argue that the violation of justice principles magnifies privacy concerns and decreases trust. In line with these findings, in this study we propose that the justice/fairness perspective provides a useful framework for identifying and operationalizing the concrete measures OSN providers can take in order to reduce user concerns and increase trust - two important determinants of information disclosure online.

3 THE MODEL

As discussed above, each fairness dimension - distributive, procedural and interactional - represents an instrument to leverage user privacy concerns and trusting beliefs to ensure responsible self-communication and network sustainability. In the following we integrate these dimensions into a conceptual model, which we then test empirically.

3.1 Distributive Justice

In organizational theory, distributive justice refers "*to the perceived fairness of the amount of compensation employees receive*" (McFarlin and Sweeney 1992, p. 626). Applied to the online environment, distributive justice can be defined as "*Internet users' perceived fairness of the outcome that they receive from online companies in return for releasing their personal information*" (Son and Kim 2008, p. 510). In simple terms, distributive justice refers to the perceived fairness of the outcome an individual gets (Culnan and Bies 2003).

Hui et al. (2006) argue that service providers should offer users benefits in exchange for using their information thus supporting equitable exchange. In fact, OSNs do provide users with a unique value: they connect them with each other and support their communication in a convenient and enjoyable way. Apart from the networking and entertainment value, OSNs allow for self-enhancement and social adjustment, while also satisfying curiosity. However, supporting an OSN with millions of users has its price. For example, making use of the distributive justice motive, StudiVZ (2010a), a popular German OSN, expands on the effort it takes to support the network: "*Our servers ensure that the data is available to you at the speed of 5.400 MBit per second during the peak times. As a comparison: a regular DSL-connection reaches 16 MBit/s. So, we are 338 times "faster" […] VZ-Networks finance themselves exclusively through advertising. In this way we can offer you quick and entertaining social network in which you can find your friends, write your news, chat, view, comment and tag photos for free…*" (translated from German by the authors). Similarly Facebook (2010b)'s privacy policy states: "*We use the information we collect to try to provide a safe, efficient, and customized experience"*. Thus, in order to justify the use of personal information, OSN providers can stress the value the users get from the platform as well as underscore the efforts they make to provide this value to users. Such measures are effective in creating organizational trust (Aryee et al. 2002). In addition, positive perception of the distributive justice can mitigate user privacy concerns. For example, Hann et al. (2002) have shown that users are willing to "trade" their privacy in return for other benefits. We therefore hypothesize that:

Hypothesis H1a: Distributive Justice will have a positive influence on user's Trust in OSN Provider.

Hypothesis H1b: Distributive Justice will have a negative influence on user's Privacy Concerns.

3.2 Procedural Justice

Laufer and Wolfe (1977) suggest that self-disclosure of personal information is possible in exchange for some benefits but only if user information will be used fairly and will not bring any negative consequences in the future. Similarly, Culnan and Armstrong (1999) find that if fair information practices are observed, customers will more willingly continue the relationship with the firm that collects information about them. These insights bring us to the notion of procedural justice, which, in general, relates to the perceived fairness of the procedures (Thibaut and Walker 1975) and the way of how these procedures are applied (Leventhal 1980). Son and Kim (2008, p. 511) define procedural justice as the "*degree to which an Internet user perceives that online companies give him or her procedures for control of information privacy and make him or her aware of the procedures*". According to OECD (1980) guidelines, the individuals must have *control* over actual outcomes such as disclosure and subsequent use of their personal information. Similarly, Malhotra et al. (2004) argue that procedural justice is enforced when individuals are empowered with *control* over these procedures.

Spiekermann (2005) differentiates between two types of control in the privacy context: *control over being accessed* and *control over information use*. OSN providers address *the first dimension* by allowing users to control access to the self through various privacy settings. For example, Facebook allows defining accessibility rights for different types of information (e.g. status up-date) on a "piece-by-piece" level. This gives users a possibility to manage information they reveal in a particularly

granular way. In fact, a recent update of the Facebook (2010a)'s privacy guidelines underscores the role of control: "*Privacy is built around a few key ideas: You should have control over what you share. It should be easy to find and connect with friends. Your privacy settings should be simple and easy to understand*". StudiVZ also allows users to see who visited their profile thereby allowing to at least post factum control the incoming audience. OSN users are also sometimes given control over the actions of other users with respect to themselves: e.g. possibilities to remove photo tags, comments or report improper behavior allow for some protection against the threats arising from the user environment. *Control over information use* is typically addressed through Terms of Use and Privacy Policies, where providers state which information they use and how. For example, StudiVZ (2010b) is paying a lot of attention to visually explain that no information is shared with third parties at any time. Facebook (2010b) asserts to share user information with third parties in cases when it believes that "*… the sharing is permitted by [the user], reasonably necessary to offer [Facebook's] services, or when legally required to do so*". Making use of the procedural fairness argumentation, Facebook (2010b) underlines the fact that user information relevant for marketing does not get linked to a person behind it in its transactions with third parties: "*…we might use your interest in soccer to show you ads for soccer equipment, but we do not tell the soccer equipment company who you are*."

Overall, privacy research shows that privacy concerns and trusting beliefs are closely interconnected with control perceptions (Das and Teng, 1998). For example, Malhotra et al. (2004) identify control as an integral element of privacy concerns. In OSN context, Xu et al. (2008) find significant relationship between perceived privacy control and privacy concerns and show the importance of providing self-controlling mechanisms for diminishing privacy risk on the OSNs. In the study of Hoffman et al. (1999) consumers' privacy concerns and trusting beliefs are governed by environmental control and control over secondary use of information, where the former implies the ability of the consumer to control the actions of the provider and the latter involves control of the information provided during the transaction. Furthermore, Das and Teng (1998) view control as an alternative mechanism that may help to ensure confidence in cooperative behavior inside the organization, or promulgate an atmosphere of trust on a platform (Dinev and Hart 2003). Recognizing the importance of control in diminishing privacy concern and ensuring trust we hypothesize that:

Hypothesis H2a: Ensuring Procedural Justice via Control will have a positive influence on user's Trust in OSN Provider.

Hypothesis H2b: Ensuring Procedural Justice via Control will have a negative influence on user's Privacy Concerns.

3.3 Interactional Justice

The impact of fair information policies on user behavior is questioned when users are not aware of them. This brings us to the concept of Interactional Justice, which relates to the fairness of interpersonal treatment of one party in an exchange relationship with another (Son and Kim 2008). Malhotra et al. (2004) posit that interactional justice is directly related to the issues of transparency with regard to enacted procedures. Overall, interactional justice is ensured if the OSN provider is perceived to be honest and caring about the needs of its members (Son and Kim 2008).

Interactional justice can be ensured in two independent ways in the OSN context. First, the OSN provider should act openly and honestly and inform users with regard to its information practices (awareness dimension). Second, the OSN provider should care for its users and by doing so proactively warn them about existing privacy threats as well as instruct them about possible protection methods (warning dimension). Even though both dimensions ultimately imply increase in user awareness, they differ in the "source of threat" they address. Whereas the former aims to make sure that users are aware of how OSN provider can collect and use their information, the latter mainly addresses threats arising from third parties and other users.

3.3.1 Awareness of the OSN Provider's Policies

Awareness implies that the individuals must know how their personal information is collected and used and what consequences can be as a result, i.e. be aware of the procedures (Culnan and Bies 2003). Culnan (1995) has demonstrated the importance of awareness by showing that people, who knew about the possibility to remove their names from the marketer's list, had lower privacy concerns related to self-disclosure. Similarly, Hui et al. (2007) argue that reading the privacy statement about information practices of online companies can encourage the individuals to reveal their personal information. Thus, informing users about the consequences of their information disclosure is an important step in ensuring the interactional justice principles are met. Increasing user awareness is especially important in the OSN context due to significant social distance between participants (Culnan and Armstrong 1999). Unaware about the motivation and incentives of the OSN providers, users often adjust their behavior on the basis of the distorted rumors and negative publicity portraying OSN providers as a malicious party. Thus, making fair privacy policies accessible, transparent and easy-to-understand could signal that an OSN provider can be trusted and simultaneously reduce privacy concerns. We therefore hypothesize that:

Hypothesis H3a: Increasing user awareness of the OSN Provider's Policies will have a positive influence on user's Trust in OSN Provider.

Hypothesis H3b: Increasing user awareness of the OSN Provider's Policies will have a negative influence on user's Privacy Concerns.

3.3.2 Proactive Warning

As OSN users can only react to the risks they are aware of, falling prey to the unknown threats can post factum provoke anger and result in the hyperbolic negative assessment of the imminent future threats. This, in turn, can have a detrimental effect on OSN participation. For example, Facebook users were not initially aware of the privacy threats involved in the Beacon application. Delayed realization provoked massive negative publicity in the Internet and stained the Facebook image (Rizk et al. 2009). Preventing these incidents is one of the most important tasks of an OSN provider. Therefore, proactive communication which brings information about privacy threats and protection methods and creates awareness, i.e. *warning*, represents another important awareness-related lever for OSN providers. Such proactive measures can include warnings about possible misuse of one's information on the network by other parties or clear communication of the methods on how one's information can be protected against abuse. By integrating such measures into its routine communication with users, an OSN provider can create an image of itself as a caring and fair party which takes responsibility for member needs and concerns. An excellent example of how an OSN provider can warn and thereby protect its members against privacy abuse is a popular gay online community: www.gayromeo.com. Apart from constantly warning users about AIDS threats (which widely exceeds online platform responsibility), this provider gives users a large number of tips in the "Safety rules" section on how privacy risks can be reduced. For example, on the technical side users are warned to use complex passwords, conceal their login data and reject cookies when using computers on their workplace. Platform members are explicitly advised to look beyond their 'imagined audience' and also consider malicious users or online crawlers. In addition, users are discouraged from giving any identifying references as a protection against social aggregators (Hogben 2007). Furthermore, users are cautioned against sharing their personal details with newly-made friends (Gayromeo 2010) – something OSN users are inclined to do as well. For example, Sophos's (2007) research has shown that 41% of Facebook users are ready to disclose their personal information (e.g. email address, date of birth, phone number) to an unknown user. By proactively publicizing privacy threats and guidelines on how information can be protected, OSN providers signal their responsibility with regard to user needs and concerns. We therefore hypothesize that:

Hypothesis H4a: Proactively warning users with regard to privacy-related threats will have a positive influence on user's Trust in OSN Provider.

Hypothesis H4b: Proactively warning users with regard to privacy-related threats will have a negative influence on user's Privacy Concerns.

4 EMPIRICAL STUDY

4.1 Survey Design and Sampling

The answers to the online questionnaire targeting Facebook users were collected in Fall 2008. The invitation to the survey was sent via numerous mailing lists as well by posting on popular Facebook groups. Every survey participant received 5 Euro as a reward upon survey completion. The final net sample consisted of 237 observations. 45.6% of the sample were female and 53.2% were male. The sample consisted to 73.4% of students – an important target group of Facebook. As the study was based in Germany the majority of the participants were either German (58.2%) or foreigners living in Germany (41.8%). Only marginal differences were found between the answers of these two groups.

4.2 Development of Measurement Scales

In order to ensure content validity of the measured constructs we relied on pre-tested scales where possible. Nevertheless, operationalization for some constructs had to be developed anew or adapted to the OSN context. All constructs were modeled as reflective with most questions anchored on a 7-point Likert scale (if not specified otherwise). Table 1 summarizes the items used to evaluate a model in this study.

We initially relied on Dinev and Hart (2006) to operationalize our "Privacy Concerns" construct. However, many items had been modified and added to reflect specifics of OSNs. For example, stalking or improper access dimensions have been integrated. Further, Son and Kim (2008, p. 526) provide an excellent instrument to measure beliefs regarding distributive justice. They ask respondents whether online companies possessing personal information about the user provide better value. This approach is, however, inapplicable in the context of our study as our survey addressed a particular OSN provider – Facebook. Hence, the items were self-developed. Furthermore, even though we initially relied on the scales suggested by Malhotra et al. (2004) to operationalize Procedural Justice: Control and Interactional Justice: Awareness dimensions, most items had been developed anew to reflect specifics of OSNs. The scales for Interactional Justice offered by Son and Kim (2008) were not suitable in our study as they were strongly based on previous trust operationalizations.

Category / Source	Items used in the study
Privacy Concerns (partly based on Dinev and Hart 2006)	How much are you concerned that the information submitted on OSN[2]: 1. ...can be used in a way you did not foresee; 2. ...can be used against you by someone; 3. ...can become available to someone without your knowledge; 4. ...can become available to someone you don't want (e.g. "ex", parents, teacher, employer, unknown person, etc.); 5. ...can be misinterpreted; 6. ...can be continuously spied on (by someone unintended); 7. ...can be used for commercial purposes (e.g. market research, advertising). (1= Not concerned at all / Never thought about it; 4= Moderately concerned; 7= Very

[2] In an actual survey the words 'OSN' and 'my OSN' were replaced by the word 'Facebook'.

	much concerned)
Trust in OSN Provider (based on McKnight et al. 2002)	In general, my OSN: 1. ...is open and receptive to the needs of its members; 2. ...makes good-faith efforts to address most member concerns; 3. ...is honest in its dealings with me; 4. ...keeps its commitments to its members; 5. ...is trustworthy.
Distributive Justice (self-developed, inspired by Son and Kim 2008)	How fair is the following? 1. I would find it fair that some of the profile information I provide can be used for personalized advertising in exchange for free social networking services. 2. The benefits I receive from OSN are attractive enough to let OSN use some of my profile information for marketing purposes. 3. The fact that some of my profile information can be used for commercial purposes could be compensated by benefits I receive from OSN.
Procedural Justice: Control (self-developed)	How much control is given to you by OSN (e.g. through functionality, privacy policies) over: 1. …the information you provide on OSN (e.g. in the profile, on the Wall etc.); 2. …who can view your information on OSN; 3. …what information is accessible to whom.
Interactional Justice: Awareness about OSN Policies (self-developed, inspired by Malhotra et al. 2004)	1. Generally, I find my OSN transparent in how the personal information I provide can be used. 2. My OSN clearly communicates what information it can collect about me. 3. My OSN clearly communicates in which cases my personal information can be shared with the other parties (marketing, HR agencies etc.).
Interactional Justice: Proactive Warning (self-developed)	My OSN makes a reasonable effort to: 1. …communicate how I can protect my information against abuse (e. g. by other parties or users); 2. …warn me about possible misuse of my information (by other parties or users); 3. …warn me about possible threats on the network (e.g. viruses, information misuse).

Table 1. Construct Operationalization.

4.3 Research Methodology and Model Evaluation

We have chosen the Partial Least Squares (PLS) approach in order to estimate the Structural Equation Model (SEM), which we have built on the basis of hypotheses formulated above. PLS is a widely-used methodology to evaluate the SEM model in a situation when the theory behind the model is still evolving. Taking into account the novelty of the topic and a multitude of newly developed scales, the choice of the PLS approach is justified. All calculations were carried out using SmartPLS 2.0.M3 (Ringle et al. 2005).

The model was evaluated in two steps: first the *Measurement Model (MM)* and then the *Structural Model (SM)* were estimated. In order to ensure the validity of the MM Convergent and Discriminant validity of the measured constructs was assessed. Convergent validity was verified by evaluating the Indicator Reliability, Composite Reliability and Average Variance Extracted (AVE) parameters. Indicator Reliability was ensured as all factor loadings were higher than a required cut-off criteria of 0.7 (Hulland 1999). Additionally, Internal Consistency was evaluated with the Cronbach's Alpha, which was higher than a threshold of 0.7 for all constructs in our study (Nunnally 1978). The Composite Reliability values for all constructs exceeded the required level of 0.6 (Ringle 2004) as shown in Table 2. Finally, the AVE values for all measured constructs surpassed the threshold level of 0.5 (Ringle 2004). Summarizing the results from the different criteria, Convergent validity was ensured.

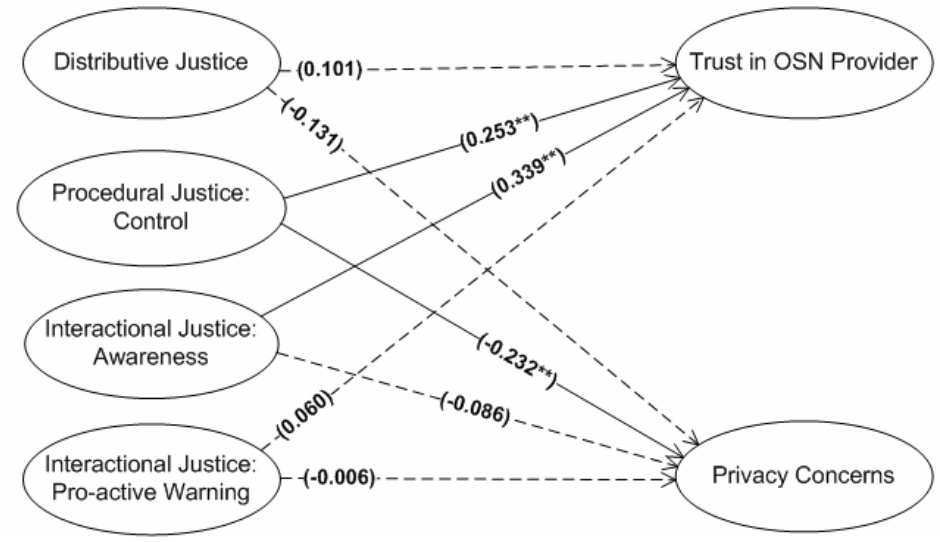
Appropriate level of the Discriminant validity indicates that the constructs are sufficiently different from each other. Discriminant validity can be assumed when the AVE for a particular latent variable exceeds the squared correlation between this variable and any other latent variables included in the model (Fornell and Larcker 1981). This requirement is fulfilled for all constructs in our model as can be seen in Table 3.

Construct	Number of indicators	Composite Reliability	Average Variance Extracted (AVE)	Cronbach's Alpha
Privacy Concerns	7	0.93	0.65	0.91
Trust in OSN Provider	5	0.92	0.69	0.89
Distributive Justice	3	0.94	0.83	0.90
Procedural Justice: Control	3	0.88	0.72	0.80
Interactional Justice: Awareness	3	0.91	0.77	0.85
Interactional Justice: Warning	3	0.95	0.85	0.91

Table 2. Quality criteria of the constructs.

Construct	PC	Tr	DJ	PJC	IJA	IJW
Privacy Concerns (PC)	*0.806*					
Trust in OSN Provider (Tr)	-0.209	*0.831*				
Distributive Justice (DJ)	-0.208	0.238	*0.911*			
Procedural Justice: Control (PJC)	-0.287	0.372	0.264	*0.849*		
Interactional Justice: Awareness (IJA)	-0.166	0.453	0.182	0.228	*0.877*	
Interactional Justice: Warning (IJW)	-0.141	0.357	0.146	0.264	0.636	*0.922*

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



*: Significance at 5%, **: Significance at 1% or less;

——— represents a significant link; – – – represents an insignificant link

Figure 1. Results of the Structural Model.

Next, the SM was evaluated. We find that our fairness dimensions explain R^2= 29.3% and 10.9% of the variance in the Trust in OSN Provider and Privacy Concerns respectively. Even though R^2 for Privacy Concerns is slightly low, overall our model shows an adequate explanatory power considering explorative nature of this study.

Finally, the value and the significance of the path coefficients were assessed as shown in Figure 1. We find that ensuring *Procedural Justice via Control* is an important means to reduce *Privacy Concerns* and enhance *Trust in OSN Provider* (H2a and H2b are supported). Furthermore, increasing user *Awareness* regarding policies of OSN Provider appears to be a powerful medium to improve trust between users and an OSN provider (H3a is supported). These measures are, however, not efficient in decreasing user privacy concerns (H3b rejected). Interestingly, neither publicizing compliance with *Distributive Justice* principles nor *Proactively Warning* users with regard to other threats is found to have a significant effect (at 5% level) on privacy concerns or trusting beliefs (H1a, H1b, H4a, H4b are rejected).

5 DISCUSSION AND MANAGERIAL IMPLICATIONS

Our model shows that amidst several means available to the OSN provider, only measures related to the *Control* dimension of the *Procedural Justice* represent an efficient instrument to ensure that both user *Privacy Concerns* and *Trust in the OSN provider* are addressed. Users' needs for active control over their information can be met through effective privacy settings, fair privacy policies and clear escalation procedures. However, even though *privacy settings* represent a powerful means to control one's information, Strater and Richter (2007) have demonstrated that even when participants changed their privacy options, they were still often misjudging the accessibility of their networks. In this case, a simple index of one's accessibility built-in on the profile page, visually similar to "Activity meter" on Xing.com, could signal users to what extent their information is accessible. This would help users make an "informed choice" about the degree of their privacy protection and create a feeling of being in control (Culnan and Bies, 2003). In contrast, OSN users often have to fight through a myriad of privacy options often inconclusive about the result of their protection.

Despite the fact that great progress has already been made in making *privacy policies* more transparent and compliant with fairness principles, there is still a long way to go. Moreover, the influence of fair information policies is questioned when users are not aware of them. Our *Awareness dimension* of the *Interactional Justice* captured the measures OSN providers can take to publicize its information-related procedures, such as collection or secondary use. Our study shows that increasing awareness about these practices can help OSN providers build up user trust. This finding brings us to the conclusion that OSN providers should not put privacy in the backroom of their web-sites. On the contrary, more information on to how and what information is collected and used should be integrated into future PR campaigns. Awareness of the rules of the game would help users to feel more positive about their participation. In addition, this publicity would help to destroy some negative myths portraying OSN provider as a malicious party continuously selling user data.

Despite the role of *Awareness* in building *Trust*, it does not have a direct impact on user *Privacy Concerns*. Awareness is often viewed as a passive dimension of the information privacy – as opposed to control (Malhotra et al. 2004) - and therefore might not have a direct impact on the privacy concern but can be rather mediated by the active control perceptions.

Our study has shown that perceptions regarding *Distributive Justice* do not have a significant effect (at 5% level) on user risk and trusting beliefs. However, the path coefficient from *Distributive Justice* to *Trust in OSN Provider* was found to be significant at 10% level (p-value equals 1.698). Moreover, several studies provide evidence for the interrelation between distributive and procedural justice dimensions. In fact, when information about procedures precedes the information about the outcomes, procedural information will have a greater influence on the fairness judgment (Konovsky 2000). Taken together, these findings call for future studies to look in more detail into the role of beliefs regarding *Distributive Justice* in shaping user perceptions.

In addition, we also find that warning users about privacy threats directly will not produce a hypothesized effect.

6 CONCLUSION

Our study identifies that OSN providers can effectively use mechanisms of procedural and interactional justice to mitigate privacy concerns and increase trust. These findings call for immediate actions to be taken by OSN providers in enabling effective privacy options as well as providing users with transparent privacy policies.

References

Acquisti, A. and Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. In Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58.

Aryee, S., Budhwar P.S., Chen Z.X. (2002). Trust as a mediator of the relationship between organizational justice and work outcomes: test of a social exchange model. Journal of Organizational Behavior, 23, 267-285.

Boyd, D. (2008). "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence". Convergence, 14 (1).

Culnan, M. J. and Armstrong, P. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10 (1), 104-115.

Culnan, M. J. and Bies, R.J. (2003). Consumer privacy: Balancing economic and justice considerations. Journal of Social Issues, 59 (2), 323-342.

Culnan, M.J. (1995). Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing. Journal of Direct Marketing, 9 (2), 10-19.

Das, T. K. and Teng, B. (1998). Between trust and control: developing confidence in partner cooperation in alliances. Academy of Management Review, 23 (3), 491-512.

Dinev, T. and Hart, P. (2003) Privacy Concerns and Internet Use – A Model of Trade-off Factors. Academy of Management Meeting, Seatle, USA.

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

Dwyer, C., Hiltz, S.R., Passerini, K. (2007). Trust and Privacy Concern within Social Networking Sites: A Comparison of Facebook and MySpace. In AMCIS 2007 Proceedings, Keystone, CO.

Ellison N, Steinfield C, 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), 2007.

Ellison, N., Heino, R., Gibbs, J. (2006). Managing impressions online: Self-presentation processes in the online dating environment. Journal of Computer-Mediated Communication, 11 (2), article 2.

Facebook (2010a). A guide to privacy on Facebook. http://www.facebook.com/privacy/explanation.php?ref=pf, last access on 14.01.2010.

Facebook (2010b). Facebook's Privacy Policy. http://www.facebook.com/policy.php?ref=pf, last access on 14.01.2010.

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

Gayromeo (2010). Info Zone: Safety rules: Safety on GayRomeo. http://www.gayromeo.com, last access on 14.01.2010.

Hann, I-H., Hui, K-L., Lee, T.S., Png, I.P.L. (2002). Online Information Privacy: Measuring the Cost-Benefit Trade-off. In Proceedings of the 23rd ICIS, Barcelona.

Hoffman, D.L., Novak, T.P., Peralta, M. (1999). Building consumer trust online. Communications of the ACM, 42(4), 80-85.

Hogben, G. (2007). Security Issues and Recommendations for Online Social Networks. ENISA Position Paper, No. 1.

Hui, K.L., Teo, H.H., Lee, S.Y.T. (2007). The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Quarterly, 31 (1), 19-33.

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

Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. Strategic Management Journal, 20, 195-204.

Konovsky, M. (2000). Understanding Procedural Justice and Its Impact on Business Organizations. Journal of Management, 26 (3), 489-511.

Krasnova, H. Günther, O., Spiekermann, S., Koroleva, K. (2009a). Privacy Concerns and Identity in Online Social Networks. Identity in the Information Society Journal, DOI 10.1007/s12394-009-0019-1.

Krasnova, H., Hildebrand, T., Günther, O. (2009b). Investigating the Value of Privacy on Online Social Networks: Conjoint Analysis. In ICIS 2009 Proceedings, Phoenix, Arizona, USA.

Krasnova, H., Kolesnikova , E., Günther, O. (2009c). It Won't Happen To Me!: Self-Disclosure in Online Social Networks. In AMCIS 2009 Proceedings, San Francisco, USA.

Laufer, R.S. and Wolfe, M. (1977) Privacy as a Concept and a Social Issue – Multidimensional Developmental Theory. Journal of Social Issues, 33 (3), 22-42.

Leventhal, G.S. (1980). What should be done with equity theory? In K.J. Gergen, M.S. Greenberg & R.H. Willis (Eds.) (1980). Social exchange: Advances in theory and research. Plenum, New York, 27- 55.

Malhotra, N.K, Kim, S.S., Agarwal J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15 (4), 336-355.

Mayer R.C., Davis J.H., Schoorman F.D. (1995). An integrative model of organizational trust. Academy of Management Review, 20, 709-734.

McFarlin, D.B. and Sweeney, P.D. (1992). Distributive and procedural justice as predictors of satisfaction with personal and organizational outcomes. Academy of Management Journal, 35, 626–637.

McKnight, D.H., Choudhury, V., Kacmar, C. (2002). The Impact of Initial Consumer Trust on Intentions to Transact with a Web site: A Trust Building Model. Journal of Strategic Information Systems, 11, 297-323.

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

OECD (1980). Guidelines on the protection of privacy and transborder flows of personal data.

Ringle, C. M. (2004). Gütemaße für den Partial Least Squares-Ansatz zur Bestimmung von Kausalmodellen. Working paper 16. Institute of Industrial Management, University of Hamburg.

Ringle, C. M., Wende, S.., Will, A. (2005). SmartPLS 2.0. Release 2.0.M3. Hamburg, Germany.

Rizk, R., Marx, D., Schrepfer, M., Zimmermann, J., Günther, O. (2009). Media Coverage of Online Social Network Privacy Issues in Germany - A Thematic Analysis", In AMCIS 2009 Proceedings, San Francisco, USA.

Son, J.-Y. and Kim, S. S. (2008). Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly, 32 (3), 503-529.

Sophos (2007). Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html, last access on 15.01.2010.

Spiekermann, S. (2005). Perceived Control: Scales for Privacy in Ubiquitous Computing. In Proceedings of the 10th International Conference on User Modeling, Scotland.

Strater, K. and Richter, H. (2007). Examining Privacy and Disclosure in a Social Networking Community. In Symposium on Usable Privacy and Security, Pittsburgh.

StudiVZ.net (2010a). Über uns. http://www.studivz.net/l/about_us/1/, last access on 14.01.2010.

StudiVZ.net (2010b). Wie funktioniert Werbung auf StudiVZ? http://www.studivz.net/l/wozu_das_ganze, last access on 14.01.2010.

Thibaut, J. and Walker, L. (1975). Procedural Justice: A Psychological Analysis. Erlbaum. Hillsdale, NJ.

Xu, H., Dinev, T., Smith, H. J., Hart, P. (2008). Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View. In ICIS 2008 Proceedings, Paris, France.