Unauthorized Information Sharing Vs. Hacking: The Moderating Role of Privacy Concern on Trust Found and Lost

Gaurav Bansal
Austin E. Cofrin School of Business, University of Wisconsin - Green Bay, Green Bay, WI, United States., bansalg@uwgb.edu

Unauthorized Information Sharing Vs. Hacking: The Moderating Role of Privacy Concern on Trust Found and Lost

Gaurav Bansal
University of Wisconsin – Green Bay
bansalg@uwgb.edu

ABSTRACT

This study examines the moderating role of privacy concern (PC) on initial trust and the related trust loss associated with news pertaining to hacking of user information and unauthorized sharing of user information by a website. This study is among the first to study the moderating role of the level of privacy concern on the degree of attribution. The relationships are examined individually for ability, benevolence and integrity based trust. The findings suggest that the users were more punitive of the fact that the company willingly, unethically, and in an unauthorized fashion shared its users' information for its gain. The study unravels an interesting dual nature of privacy concern and trust. The findings suggest that initial trust leads to bigger integrity based trust drop for high PC people, however, trust propensity cushions the trust drop for low PC users across all three trust types i.e. ability, benevolence and integrity. This paper provides several theoretical and managerial implications.

Keywords

Trust, Privacy Concern, Trust Lost, Violation, Ability, Integrity, Benevolence

INTRODUCTION

It is widely acknowledged that trust is necessary in order for any business to thrive, and it is even more necessary in online environments where the trustor is even more vulnerable to a *face-less* and *remote* trustee. Loss of trust leads to lost sales and other irreparable and "devastating damages" (Tomlinson and Mayer 2009 p. 85). Several researchers (e.g., Kim et al. 2009) have recently called for a deeper analysis of the trust-repair processes. The trust-repair literature has recently started gaining momentum in Management (e.g., Elangovan et al. 2007; Kim et al. 2009; Schoorman et al. 2007; Tomlinson and Mayer 2009), Marketing (e.g., Wang and Huff 2007) and MIS (e.g., Goles et al. 2009; Liao et al. 2008). However, there is a need to examine the trust-violation and repair in online environments from an information perspective, since information serves as the key resource for any online business in general and e-commerce in particular. Moreover, any trust rebuilding examination should be preceded by an examination of trust lost – including how much was lost, and how-, where-, why-, and when- it was lost. Echoing similar sentiments, Schoorman et al. (2007) stated that "it is critical to first understand how it [trust] was damaged in the first place, since different means of damaging trust are likely to require different repairing responses" (p. 349).

In this study, relying on Attribution Theory, (Weiner 1986) we argue that the trust revision and subsequent trust drop pertaining to negative news about hacking of user information or unauthorized sharing of user information, would be attributed to the cause of the violation and the degree of attribution would depend upon one's level of privacy concern (PC). Attribution Theory has found "rich support in empirical studies conceptually similar to trust repair" (Tomlinson and Mayer 2009, p. 90). Attribution Theory suggests that in lieu of negative news, the degree of attribution primarily depends upon three things: locus- whether the cause of the violation is perceived to be internal or external, stability – perceived likelihood of recurrence, and controllability - the extent to which the user perceives that the violator could have controlled the outcome (Wang and Huff 2007; Weiner 1986). Attribution theory subtly brings in the role of individual differences and this can be shown in two ways. First, the perceived likelihood of stability, controllability and locus are bound to have individual differences. Second and more importantly, per the philosophy of Attribution Theory, the attribution chain starts when a person encounters "a *subjectively* [emphasis added] important act*"* (Weiner 1985, p. 564) which sets "the boy [person] overtly or covertly wondering" (p. 564).

We argue that both trust and PC play a dual role. Contrary to the belief that initial trust is associated with positive subsequent trust revision, we demonstrate that initial trust is also associated with a subsequent bigger drop in trust, obviously there will be little drop if there is little trust to start with. We show that PC positively moderates these relationships such that it accelerates the drop in trust for any given level of initial trust, and retards the cushioning effect of trust propensity. We also show that drop in integrity is more than the drop in ability based trust, and the drop in benevolence based trust is intermediate to the two depending upon the news hacking / sharing scenario.

THEORY AND RESEAERCH MODEL

The research model is shown in Figure 1.

Trust Violation

Trust lost has often been equated with psychological contract violation (Pavlou and Gefen 2005), trust violation, service failure (Goles et al. 2009), trust erosion (Elangovan et al. 2007), and decline (Tomlinson and Mayer 2009). For this study we abide by Bies and Tripp's (1996) definition of trust violation as "unmet expectations concerning another's behavior or when the person [or the trustee] does not act consistent with one's values" (p. 248). In that sense it is broader than service failure, and is sensitive to the broader responsible behavior of the trustee.

Privacy Concern

There are several perspectives as well as definitions of information privacy. Information privacy has been viewed as a right, commodity, state and control (Smith et al. MISQ 2011). However, information privacy has also been viewed as fairness (Malhotra et al. 2004). In this paper we define information PC as the individual's subjective views of fairness within the context of information privacy (Malhotra et al. 2004). PC is a personal disposition (Bansal et al. 2010). PC has been found to be positively associated with conscientiousness (Junglas et al. 2008). Individuals with high conscientiousness place more importance on equity and procedural fairness. Conscientiousness has been known to moderate the relationship between perceived procedural fairness and attitude (Burnett et al. 2009). Extending this line of thought, it could be argued that high PC users would be more sensitive for perceived fairness related to the usage and handling of the user information by websites. Specifically, the degree of PC would positively moderate the trust drop in such a way that for any given level of initial trust, high PC users would experience greater trust loss as compared to low PC users. Conversely, low PC users would experience less trust loss as compared to high PC users for trust cushions which minimize the trust drop (i.e. trust propensity). Thus, relying on the fact that degree of attribution would depend upon the "person" it could be argued that the degree of attribution for high PC users would be more severe than that for low PC users.

Control Variables

Individuals are known to possess high levels of initial trust even in absence of any prior familiarity (McKnight et al. 1998). But, this trust is quite fragile because of its tentative nature (Kim et al. 2009). Thus we control for familiarity in the study. We also control for gender in this study as advised by Xie and Peng (2009).

Initial Trust

Mayer et al. (1995) argued that "outcomes of trusting behaviors will lead to updating of prior perceptions of the ability, benevolence and integrity of the trustee" (1995 p.728). Zahedi and Song (2008) showed that prior trust evaluation is positively associated with trust revision. However, in lieu of negative evidence, we argue that a prior pool of trust would also decline faster, especially if it is newly based trust. Trust declines only when one has "developed some level of trust and then perceives distrusting evidence due to the causal attributions made for the negative outcome" (Tomlinson and Mayer 2009, p. 89). Ostensibly there will be little decline if there is little trust to begin with.

> Hypothesis 1: Controlling for familiarity, and gender, initial trust is positively associated with a drop in trust following negative news related to hacking of user information from a website's possession or unauthorized sharing of user information by the website.
>
> Hypothesis 2: The above relationship is positively moderated by PC in such a way that there is a significantly bigger loss in trust for high PC users as compared to low PC users.

Trust Propensity

Trust propensity describes the general trusting outlook one possesses about trusting others which enables the trustor to look past the trustee's shortcomings, faults and even failures (Jarvenpaa et al. 1998). Even though initial trust is based out of trust propensity, in the context of this study the two are argued to play entirely different roles. We argue that initial trust is also responsible for "crushing" the trust, and trust propensity serves to soften the trust-landing. Trust propensity would help in shifting the attribution from internal *locus* to external, help lower the perceived likelihood of *recurrence* of the negative behavior, and give the benefit of the doubt to the trustee in terms of degree of *controllability* – all suggesting that this variable will help scale down the severity of the attribution pertaining to the negative news or predicament. Trust propensity is a trust maker, and in lieu of a negative predicament, would likewise act as a "cushion" softening the trust decline. We argue that this cushioning will be more effective for people who are not seriously *involved* (Bansal et al. 2008) in the issue. Hence,

> Hypothesis 3: Controlling for familiarity and gender, trust propensity is negatively associated with a drop in trust accompanying the news pertaining to hacking or unauthorized sharing of data.
>
> Hypothesis 4: The above relationship is positively moderated by PC in such a way that there is significantly less loss in trust for low PC users as compared to high PC users.

News Scenario

Based on Attribution Theory, trust would decline more severely if the trustor perceives that the trustee had the ability to control the event but chose not to, when the attribution is internal as opposed to external to the trustee, and when the trustor perceives that the event has a high likelihood of recurrence. With the unauthorized sharing of user information, the trustor believes that the event was controllable, the trustee could have avoided sharing the information in an unauthorized way, the trustee was responsible, and, if the trustee is unethically involved in information sharing, it might do it again in the future. The same thing cannot be said of hacking. Hacking is done by external unknown hackers, and the trustee has less control over the hackers. Hacking might be prevented in the future if the trustee employs updated software, hardware and policies. Hence, sharing news as opposed to news pertaining to hacking would cause greater attribution.

> Hypothesis 5: Controlling for familiarity and gender, news about unauthorized sharing of user information leads to a higher degree of trust lost, as opposed to the trust lost by news about hacking of the user information in the website's possession.

Perceived Seriousness of News (PSN)

Attribution Theory allows for a subjective evaluation of the predicament by the user. Thus it could be stated that those who perceive the news predicament to be "subjectively" more "important" (Weiner 1985 p. 564) will experience more severe attributions than those who do not. This argument is supported by the research finding of Jones and George (1998) that the magnitude of the perceived violation is positively associated with the shift in trust. Hence,

> Hypothesis 6: Controlling for familiarity and gender, the perceived seriousness of the news pertaining to hacking or unauthorized sharing of data is positively associated with the degree of trust lost.

Design and Reputation

Website design and reputation are known to be positively associated with trust building. High design quality lowers risk beliefs associated with the website, and hence enhances the degree of trust (Bansal et al. 2008). Reputation as a source of social knowledge plays a role in trust formation and maintenance (Zahedi and Song 2008).

> Hypothesis 7: Controlling for familiarity and gender, perceived website design quality is negatively associated with a drop in trust accompanying the news pertaining to hacking or unauthorized sharing of data.
>
> Hypothesis 8: Controlling for familiarity and gender, reputation of the website is negatively associated with a drop in trust accompanying the news pertaining to hacking or unauthorized sharing of data.

The above relationships (H1-H8) will be observed for (a) ability based trust, (b) benevolence based trust, and (c) integrity based trust.

Morality vs. Competence

Studies suggest that individuals tend to weigh positive information more heavily than negative information about ability, but tend to weigh negative information more heavily than positive information about integrity (Kim et al., 2004). However, they are believed to neither weigh negative information about benevolence as heavily as negative information about integrity nor weigh positive information about benevolence as heavily as positive information about competence (Kim et al. 2009; Trafimow and Trafimow 1999). This would lead us to hypothesize that the drop in benevolence based trust would be less than the corresponding loss in integrity, and would be significantly more than the corresponding drop in ability based trust.

> Hypothesis 9: The relative amount of subsequent loss in trust accompanying the news pertaining to hacking or unauthorized sharing of data is significantly more for (a) integrity based trust as opposed to ability based trust; (b) benevolence based trust as opposed to ability based trust; and (c) integrity based trust as opposed to benevolence based trust.

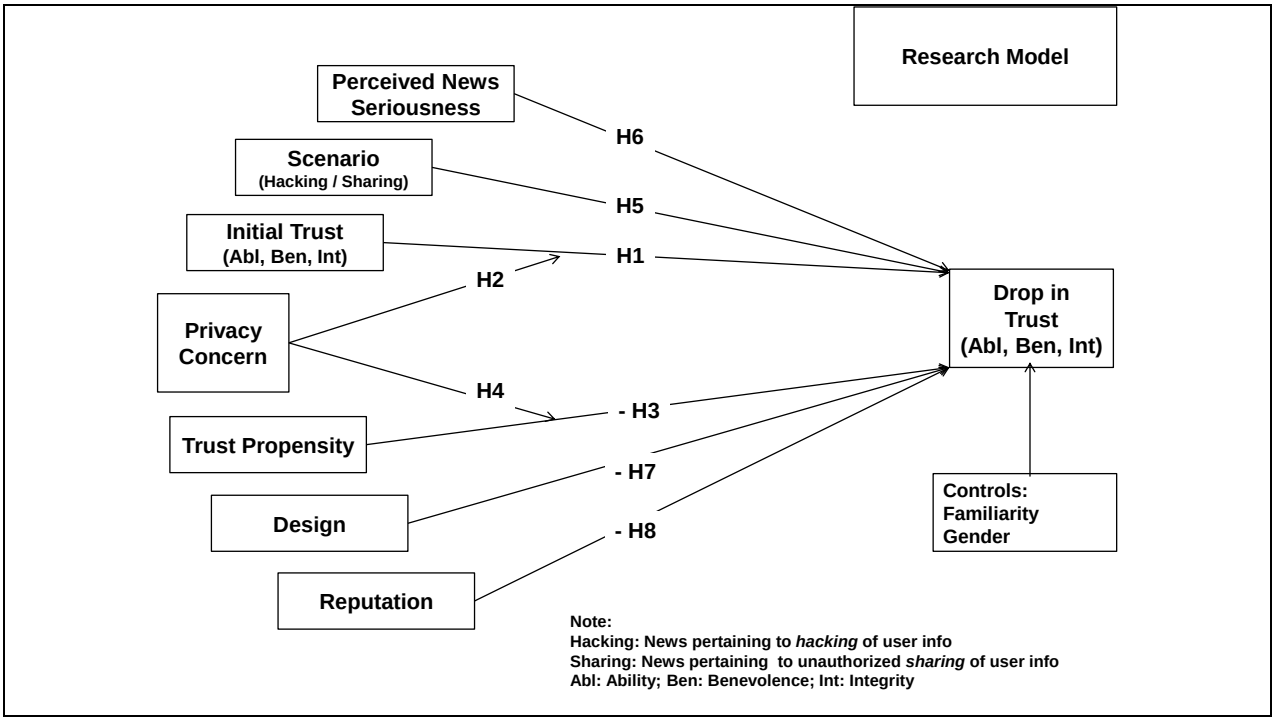

Figure 1. Research Model

RESEARCH METHODOLOGY

Data were collected from students studying in a Midwestern University. Students were shown a website and their initial trust (Trust1) was measured. Later the students were randomly shown one of the two scenarios (Table 1): hacking news or unauthorized information sharing news. Scenario based study is appropriate as it controls for outside factors, moreover the responses to scenarios are known to be accurate and reliable reflections of the actual user decisions and reactions (Elangovan et al. 2007).

Hacking	Sharing
The Website you saw announced late Sunday that criminal hackers broke into its systems and had access to personal information on potentially more than 24 million customer accounts. This sheer size is quite similar to the number of accounts Sony's PlayStation Network reported stolen in April 2011 i.e. 77 million.	The Website you saw has been alleged to sharing unauthorized personal information on potentially more than 24 million customer accounts with a data mining company. This sheer size is quite similar to the number of accounts Sony's PlayStation Network reported stolen in April 2011 i.e. 77 million.

Table 1. Scenario Description

Both news scenarios involved the same magnitude of number of user accounts affected. Trust in the website was measured again (Trust2). In order to ensure that the participants had given the website some serious consideration, they were later asked to identify the correct name of the website shown to them from a list of five options. They were also asked to correctly identify its specialization. Those who failed these two questions were not considered in the analysis. 378 students completed the study. After removing the students who failed the "quiz" only 364 were included in the analysis. The average age of the respondents is shown in Table 2 below.

	Male	**Female**	**N**	**Age Mean (Std_dev)**	**Internet experience Mean (Std_dev)**
High PC	70	108	181	22.51 (5.79)	11.33 (3.34)
Low PC	83	90	174	21.45 (4.07)	10.55 (3.03)

Table 2. Demographics

Operationalization of variables

To ensure construct validity we used items from existing scales wherever possible. We converted the items to semantic differential (0-10), so as to minimize common method bias (Song and Zahedi 2005).

Construct	**Adapted from**	**Construct**	**Adapted from**
Trust Propensity	Zahedi and Song (2008)	Trust	Gefen et al. (2003)
Reputation		Design Quality	Bansal et al. (2008)
Ability		PC	Malhotra et al. (2004)
Benevolence		Familiarity	Self-developed
Integrity		Perceived Seriousness of News (PSN)	Self-developed

Table 3. Operationalization of Variables

Data analysis and Results

Data analysis was performed using OLS Regression. We first performed the EFA analysis separately for each model (ability, benevolence, and integrity). EFA factor loadings were all above .70 for all constructs in all of the models except for PC Error Concern which ranged from .67 to .68. Reliability was measured by computing Cronbach alphas. They ranged between .746 and .96. The EFA factor loadings provided confidence in the discriminant and convergent validity of the constructs. Cronbach alpha scores confirmed the reliability of the constructs. We used four factors of PC (collection, secondary use, unauthorized access and errors) and created a second order factor as suggested by Stewart and Segars (2002). To examine the moderating role of PC we split the second order PC such that negative factors were assigned to the low PC group and positive factor scores were assigned to the high PC group. We subtracted the sum of Trust2 items from the sum of Trust1 items to compute the trust lost. We computed one factor each for initial trust, PSN, familiarity, trust propensity, reputation, and design. Gender and news scenario were used as categorical variables. Hypothesis 1, 3, 5, 6, 7 and 8 were analyzed by computing the regression coefficients separately for ability, benevolence and integrity based trust. We examined the moderating hypotheses (H2 and H4) using the formula (Cohen 1983) shown below. The formula should be considered appropriate since the sample sizes across the two groups are roughly equal:

$$Z = \frac{(b_1 - b_2)}{\sqrt{\frac{V_1(SEb_1^2) + V_2(SEb_2^2)}{V_1 + V_2}}}$$

Here, V_1, and V_2, are the degrees of freedom and SE_{b1} and SE_{b2}; are the standard errors associated with the first (high PC) and second groups (low PC) respectively.

The results from the three models: ability, benevolence and integrity are presented in Figures 2-4. The R squares for the six regression models (three trust types x two PC levels) ranged from .26 to .42. VIFs for all regression models were less than 3, indicating that multicolinearity is not affecting the analysis. To examine the presence of common method variance in the data set, we carried out the Harman one factor test. The first factor explained the following percentage variations in the various models: Ability: 22.35%, Benevolence: 21.65%, and Integrity: 20.76%. It seems that the variance is probably not large enough to signal the existence of common method bias.

Hypothesis 9 was examined by using pairwise t-tests utilizing normalized mean differences for loss of trust in integrity, benevolence and ability separately for sharing and hacking scenarios. The results of Hypothesis 9 are explained in Table 5. Normalized mean differences were obtained by dividing the drop in trust by initial trust: (Trust1-Trust2)/Trust1. The descriptive analysis of the normalized means is shown in Table 4.

	Hacking			**Sharing**		
	N	**Normalized Mean Difference**	**Std. Dev.**	**N**	**Normalized Mean Difference**	**Std. Dev.**
Drop in Ability	181	.20	.26	181	.33	.34
Drop in Benevolence	179	.21	.26	179	.45	.31
Drop in Integrity	177	.25	.27	178	.45	.39

Table 4. Descriptive Analysis of the Trust Drop across three types of Trusts

Pairwise Comparison (T-test)	**Hacking**	**Sharing**
Drop in Integrity > Drop in Benevolence	Yes (p value <.01)	
Drop in Integrity > Drop in Ability	Yes (p value < .01)	Yes (p value <.001)
Drop in Benevolence > Drop in Ability		Yes (p value < .001)

Table 5. Comparison of Drop in Ability, Benevolence and Integrity based Trust (Using Normalized Mean Differences)

The results are summarized in Table 7 and shown in Figures 2-4. Hypotheses H1, H4, H5, and H6 found strong support. H2 was supported for integrity based trust, H3 was supported for low PC individuals only, H7 was supported for ability based trust in low PC individuals, and H8 was supported for integrity based trust in high PC individuals. The results show that high and low PC users rely to varying degrees on different mechanisms for the three trust dimensions when setting their attribution. The findings show that high initial trust acts as a dual-edged sword. It was known to be positively associated with positive trust revision (Zahedi and Song 2008), but is now (controlling for familiarity and gender) known to be associated with a bigger drop in response to negative news. High PC users drop more trust than low PC users, when they encounter negative evidence. We find that trust propensity and design act as cushions which lower the trust drop across all trust dimensions. Gender played no strong role. We found that low PC females dropped more benevolence based trust. It appears that familiarity provided more cushion to low PC people as opposed to high PC people, the difference however is not statistically significant.

We found that the drop in integrity was more than the drop in ability based trust. However, the drop in benevolence was less than the drop in integrity for the hacking scenario and was more than the drop in ability for the sharing scenario. So it seems that in the sharing scenario benevolence gets battered to the same degree as integrity. In the hacking scenario, benevolence gets some relief, and is not discounted to the same extent as integrity is.

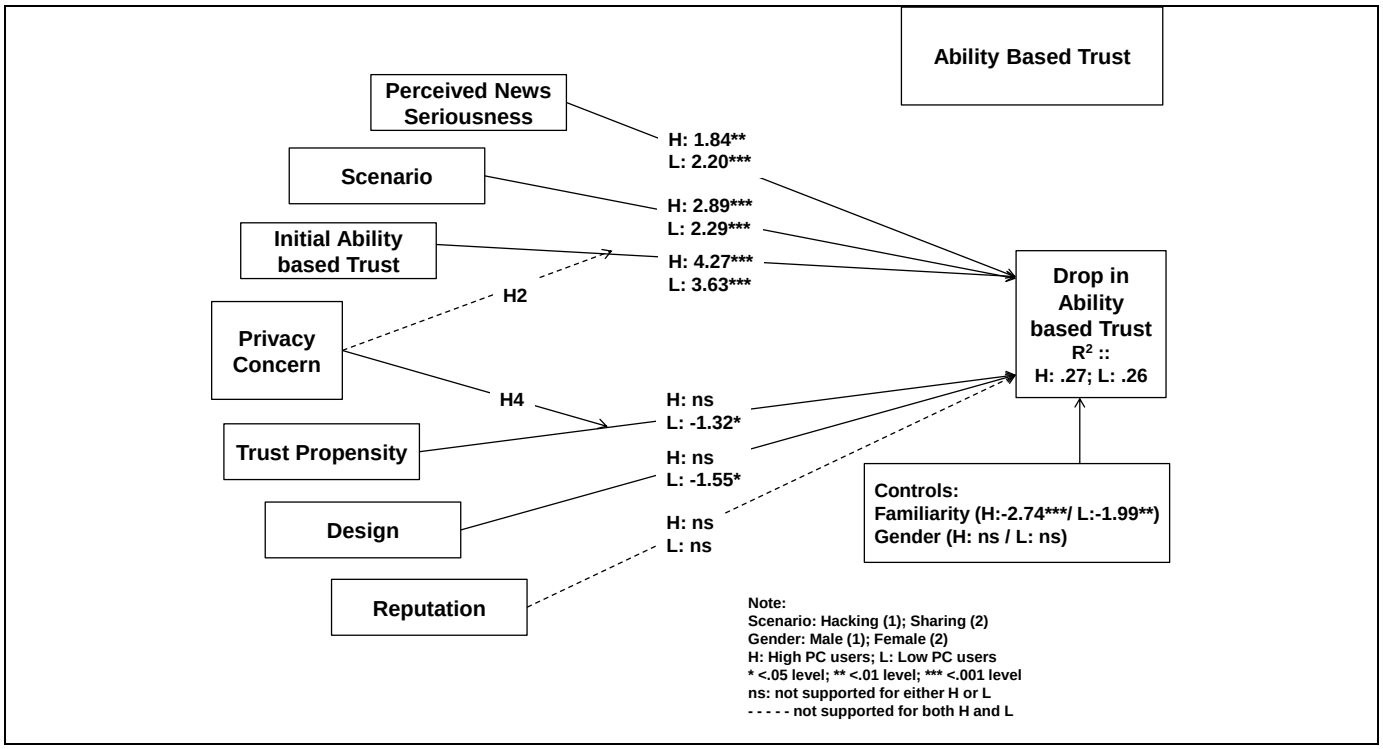

Figure 2. Results (Ability)

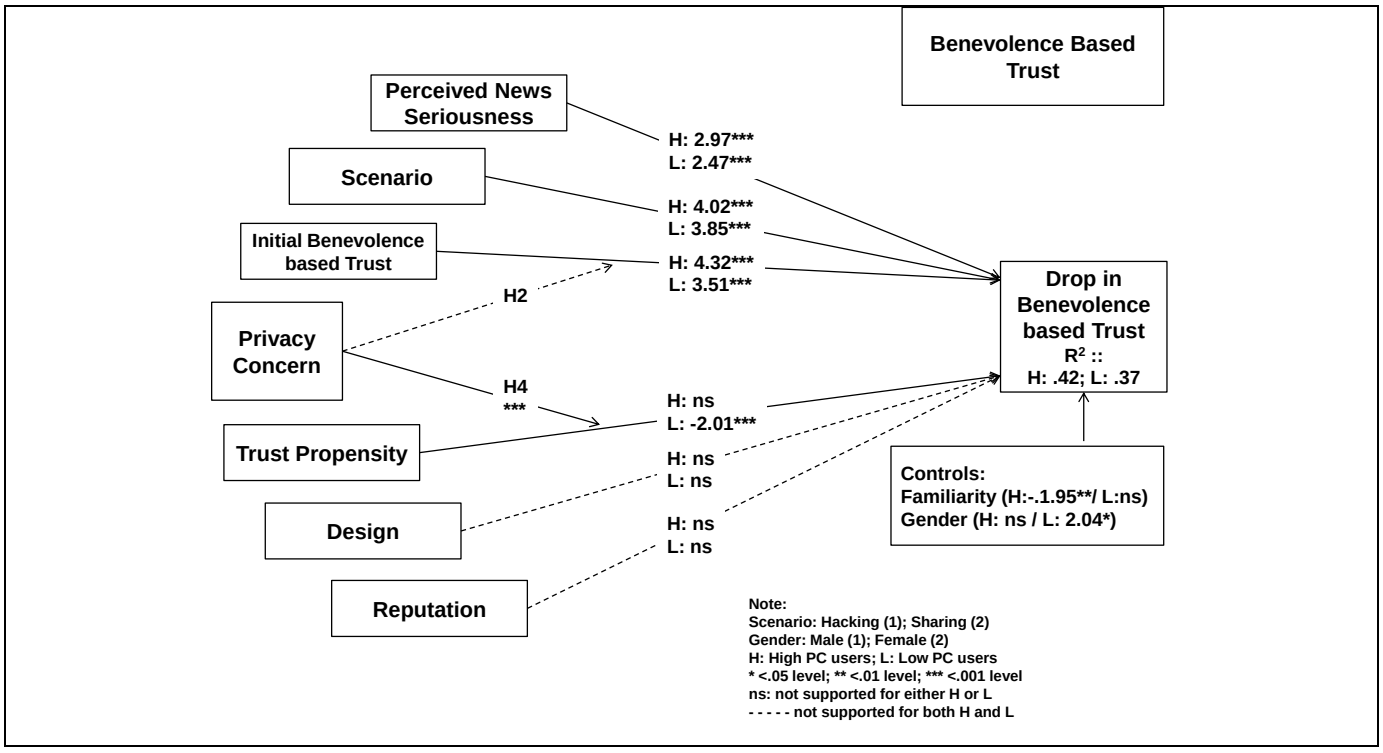

Figure 3. Results (Benevolence)

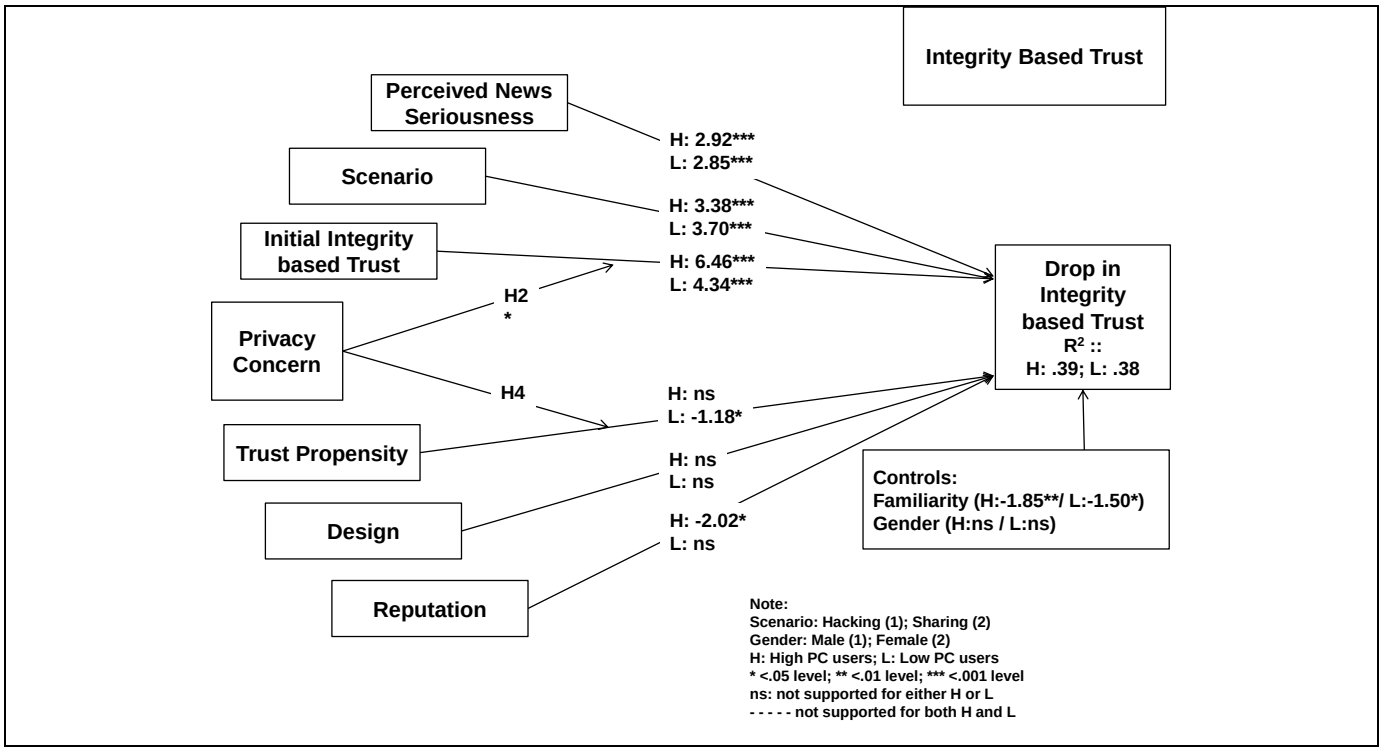

Figure 4. Results (Integrity)

Hypothesis	Construct	Ability	Benevolence	Integrity
H1	Initial trust	S	S	S
H2	Moderation: Initial Trust	ns	ns	S
H3	Trust Propensity	S	S	S
H4	Moderation: Trust Propensity	S (structural)	S (structural)	S (structural)
H5	News Scenario (hacking vs. sharing)	S	S	S
H6	Perceived News Seriousness (PSN)	S	S	S
H7	Design	S	ns	Ns
H8	Reputation	ns	ns	S
H9a	Drop in Integrity > Drop in Ability	S		
H9b	Drop in Benevolence > Drop in Ability	S (supported for sharing scenario)		
H9c	Drop in Integrity > Drop in Benevolence	S (supported for hacking scenario)		
Familiarity		H:-*** L: -**	H:-** L: ns	H:-** L: -*
Gender		H: ns L: ns	H: ns L: *	H: ns L: ns

Table 6. Result Summary

Abbreviation: S: Supported; ns: not significant; H: High PC; L: Low PC; * .05 level; ** .01 level; *** .001 level

DISCUSSION

To the best of our knowledge, this study is among the first to examine the moderating role of PC on trust lost. The finding that PC positively moderates the impact of trust antecedents in such a way that high PC users experience greater trust loss for initial integrity based trust, and low PC users experience less trust loss for trust propensity which acted as trust cushion,

provides support to the idea of the moderating role of involvement (reflected in the form of PC) (Bansal et al. 2008) on the level of attribution. The finding that high PC users were more punitive of the fact that the company willingly, unethically and in an unauthorized fashion, shared its users' information for its gain, suggests that that fairness might be a fifth dimension on the slate of Smith et al.'s (2011) four facets of information privacy: control, commodity, right and state.

In order to enrich the trust repair literature, recently Kim, Dirks and Cooper (2009) stressed the need to examine (1) the role of individual differences; (2) the role of situational factors; (3) the role of length of relationship; and (4) the relative role of benevolence based attributions as compared to ability and integrity based attributions with regard to trust violation and repair. In this study, by examining the role of PC as individual personal disposition, the situational role of news pertaining to hacking and unauthorized sharing of user information, the role of familiarity with the website, and the relative role of benevolence vis-à-vis integrity and ability, we attempt to address the future research directions for trust repair research identified by Kim, Dirks and Cooper. The finding that the drop in benevolence is between the drop in integrity and ability based trust supports the proposition advanced by Kim et al. (2009).

There are several other interesting findings from this study. The finding that low PC females dropped more benevolence based trust adds to an ongoing debate of whether degree of forgiveness is the same across gender. It seems familiarity and reputation are cushioning high PC individuals more; and trust propensity & design are cushioning low PC individuals more. Out of these, trust propensity and familiarity play a more consistent role for all three trust types.

There are several key managerial implications as well. Website managers should understand that even though sharing of user information is legally allowed, the users still find it more punitive than hacking. Even though sharing in an unauthorized way is primarily an integrity based issue, it lowers the benevolence and even the ability based trust as well. Website design and reputation might help cushion the effect of the trust drop, but they only go so far, and do little. Out of the two, it seems reputation cushions integrity based trust for high PC individuals, and design cushions ability based trust for low PC individuals.

Limitations and Future research

This study has limited generalizability since the respondents were students studying in a Midwestern university. Even though the study measured trust in two parts, it was not longitudinal. Our study provides answers to some questions, but also opens the door for many hitherto unanswered questions. Future research should look at different demographics, preferably across different cultural settings. Future research could examine different contextual scenarios and measure trust at different time intervals. Integrity is supposed to be relatively more stable than benevolence and ability, these findings however, need to be examined in the context of trust violation and repair. Future research can examine the efficacy of trust repair efforts for any given degree of initial trust as well as loss in trust. It will be interesting to examine the relative efficacy of various trust repair approaches in an attempt to rebuild the trust which was once had and then lost!

REFERENCES

1. Bansal, G., Zahedi, F. M. and Gefen, D. (2008) The Moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation, in the proceedings of the *International Conference on Information Systems*, Paris.
2. Bansal, G., Zahedi, F. M., and Gefen, D. (2010) The impact of personal dispositions on information sensitivity, PC and trust in disclosing health information online, *Decision Support Systems*, 49, 138-150.
3. Bies, R. J., and Tripp, T. M. (1996) Beyond distrust: Getting even and the need for revenge, in R. M. Kramer and T. Tyler, Eds., *Trust in Organizations*, Newbury Park: Sage Publications, 246-260.
4. Burnett, M. F., Williamson, I. O., and Bartol, K. M. (2009) The Moderating effect of personality on employees' reactions to procedural fairness and outcome favorability, *Journal of Business Psychology*, 24, 469–484.
5. Cohen, A. (1983) Comparing regression coefficients across subsamples. A study of the statistical test, *Sociological Methods and Research*, 12, 77-94.
6. Elangovan, A. R., Auer-Rizzi, W., and Szabo, E. (2007) Why don't I trust you now? An Attributional approach to erosion of trust, *Journal of Managerial Psychology*, 22, 1, 4-24.
7. Goles, T., Lee, S., Rao, S. V., and Warren, J. (2009) Trust violation in electronic commerce: Customer concerns and reactions, *The Journal of Computer Information Systems*, 49, 4, 1-9.
8. Jarvenpaa, S. L., Knoll, K., and Leidner, D. E. (1998) Is anybody out there? Antecedents of trust in global virtual teams, *Journal of Management Information Systems*, 14, 4, 29-64.
9. Jones, G., and Geiorge, J. (1998) The experience and evolution of trust: Implications for cooperation and teamwork, *The Academy of Management Review*, 23, 3, 531-546.

10. Junglas, I.A, Johnson, N.A., and Spitzmuller, C. (2008) Personality traits and concern for privacy: An empirical study in the context of location-based services, *European Journal of Information Systems*, 17, 387–402.
11. Kim, P. H., Dirks, K. T., and Cooper, C. D. (2009) The repair of trust: A dynamic bilateral perspective and multilevel conceptualization, *Academy of Management Review*, 34, 3, 401-422.
12. Liao, Q., Luo, X, and Gurung, A. (2008) Rebuilding post-violation trust in B2C electronic commerce, *Journal of Organizational End User Computing*, 21, 1, 60-74.
13. Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004) Internet users' information PCs (IUIPC): The construct, the scale, and a causal model, *Information Systems Research*, 15, 4, 336-355.
14. Mayer R. C., Davis J. H., and Schoorman, F. D. (1995) An integrative model of organizational trust, *Academy of Management Review*, 20, 3, 709–734.
15. McKnight, D. H., Cummings, L. L., and Chervany, N. L. (1998) Initial trust formation in new organizational relationships, *Academy of Management Review*, 23, 3, 473-490.
16. Pavlou, P. A. and Gefen, D. (2005) Psychological contract violations in online marketplaces: Antecedents, consequences, and moderating role, *Information Systems Research*, 16, 4, 372-399.
17. Schoorman, F. D., Mayer, R. C., and Davis, J. H. (2007) An integrative model of organizational trust: Past, present, and future, *Academy of Management Review*, 32, 2, 344-354.
18. Smith, H. J., Dinev, T., and Xu, H. (2011) Information privacy research: An interdisciplinary review, *MIS Quarterly*, 35, 4, 989-1015.
19. Song, J. and Zahedi, F. M. (2005) A theoretical approach to web design in e-commerce: A belief reinforcement model, *Management Science*, 51, 8, 1219-1235.
20. Stewart, K. A., and Segars, A. H. (2002) An empirical examination of the concern for information privacy instrument, *Information Systems Research*, 13, 1, 36-49.
21. Tomlinson, E. C., and Mayer, R. C. (2009) The role of causal attribution dimensions in trust repair, *Academy of Management Review*, 34, 1, 85-104.
22. Trafimow, D., and Trafimow, S. (1999) Mapping perfect and imperfect duties onto hierarchically and partially restrictive trait Dimensions, *Personality and Social Psychology Bulletin*, 25, 687-697.
23. Wang, S., and Huff, L. C. (2007) Explaining buyers' responses to sellers' violation of trust, *European Journal of Marketing*, 41, 9/10, 1033-1052.
24. Weiner, B. (1985) An Attributional theory of achievement motivation and emotion, *Psychological Review*, 92, 548-573.
25. Xie, Yi, and Peng, S. (2009) How to repair customer trust after negative publicity: The roles of competence, integrity, benevolence, and forgiveness, *Psychology & Marketing*, 26, 7, 572-589.
26. Zahedi, F. M., and Song, J. (2008) Dynamics of trust revision: Using health infomediaries, *Journal of Management Information Systems*, 24, 4, 225-248.