5-2012

Not All Privacy Losses Cost the Same: Examining the Relative Perceived Trust Violation in a Hacking Versus Unauthorized Information Sharing Scenario

Gaurav Bansal
University of Wisconsin - Green Bay, bansaig@uwgb.edu

Ellyn Hansen
University of Wisconsin - Green Bay, hansem30@uwgb.edu

Lijun Chen
University of Wisconsin - Green Bay, chenl10@uwgb.edu

Not All Privacy Losses Cost the Same: Examining the Relative Perceived Trust Violation in a Hacking Versus Unauthorized Information Sharing Scenario

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

Ellyn Hansen
University of Wisconsin – Green Bay
hansem30@uwgb.edu

Lijun Chen
University of Wisconsin – Green Bay
chenl10@uwgb.edu

ABSTRACT

Using the attribution Theory, the study examines the relative trust loss in a hacking versus unauthorized information sharing by a Website. An experiment was conducted in which the respondents were asked to view a website and answer questions related to their trust, at two different phases both before and after reading the news scenario. The results of the study show that users experience significantly higher degree of trust drop when the website intentionally and unethically share the user data with other companies for data mining or other unauthorized purposes as opposed to information hacking by unknown hackers. The findings suggest that there is more to privacy than just exposure. Both the scenarios entailed exposure of the same number of user accounts, still the trust lost was greater for unauthorized sharing instead of hacking. It suggests that privacy is important, no doubt, however, the way it is lost, is important as well.

Keywords

Trust Violation, Drop, Privacy Concern, Sharing, Hacking

INTRODUCTION

Trust is so important for e-commerce, that it will not be inappropriate to say that trust *empowers* an e-commerce website more than its web server. Hacking and unauthorized information sharing are serious problems that shake up the users' trust in e-commerce, in general, and a website in particular. The study examines the relative trust loss in a hacking versus unauthorized information sharing by a website. Marketing researchers have long known that it is more expensive to attract a new customer, than to retain the existing customer (Johnson 2003). Perceived Trust violation often keeps the existing customers at bay. These customers can be wooed over by repairing the broken trust. Researchers have recently started to delve deeper into this area of winning back the trust (e.g., Elangovan et al. 2007; Goles et al. 2009; Liao et al. 2008; Kim et al. 2009). However, till date there is little knowledge about the trust lost related to unauthorized sharing and hacking. Examining the relative trust lost not only furthers our insight about these issues, but could also help in devising the appropriate trust repair program for these scenarios.

THEORY AND THE RESEARCH MODEL

Trust violation

Trust violation has been defined by Bies and Tripp's (1996) as "unmet expectations concerning another's behavior or when the person [or the trustee] does not act consistent with one's values" (p. 248).

Initial trust

Mayer et al. (1995) argued that "outcomes of trusting behaviors will lead to updating of prior perceptions of the trust in the trustee. The initial trust is primarily an assumption based trust (Kim et al. 2009; McKnight et al. 1998), and hence would

decline as the assumptions seem to be invalid. Initial trust comprises of primarily two things trusting intentions meaning that the trustor is willing to depend upon the trustee in a given situation; and trusting beliefs, meaning that the trustor believes that the trustee possesses the ability, benevolence and integrity in the given situation (McKnight et al. 1998).

Trust Beliefs	**General Definition (Mayer et al. 1995)**	**Definition as applied to e-commerce context (Bhattacherjee et al. 2002)**	**Keywords**
Ability	Group of skills, competencies, and characteristics that enable a party to have influence within some specific domain (p. 717)	In e-commerce contexts, user perceptions of firm's ability are based on two related beliefs: (1) whether the firm is competent (expert or skilled) enough to perform the intended behavior, and (2) whether the firm has access to the knowledge required to perform the behavior appropriately (p.217)	Skills
Benevolence	Extent to which a trustee is believed to want to do good to the trustor, aside from an egocentric profit motive. It suggests that that the trustee has some specific attachment to the trustor (p.718)	Benevolent firms should at the very least: (1) demonstrate receptivity and empathy toward users' concerns and needs, and (2) proactively make good-faith efforts to resolve user concerns. (p.219)	Empathy
Integrity	Trustor' s perception that the trustee adheres to a set of principles that the trustor finds acceptable (p.719)	In e-commerce contexts, rules of integrity refer to: (1) conduct of online transactions, (2) customer service policies following a transaction, and (3) firm's use of private user information. (p.219)	Honesty

Table 1. Trust Dimensions

As the assumptions related to the trusting beliefs are shaken, the trust which was formed easily would also be lost easily. By willfully sharing the user information with unauthorized entities, the website downplays all of the trusting beliefs: ability, benevolence, and integrity. Table 1 lists the general- and the corresponding contextual-definitions of these terms. Moreover, trust declines 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). Hence:

H1: Users with high initial trust will experience more trust drop.

Scenario: Sharing vs. hacking

Attribution Theory suggests that in the context of negative news, the degree of attribution primarily depends upon three things; whether the cause of the violation is perceived to be internal or external, perceived likelihood of recurrence, and the extent to which the user perceives that the violator could have controlled the outcome (Wang and Huff 2007; Weiner 1985). 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 integrity belief would decline when the user perceive the website to be using the user information in an unethical way; the benevolence belief would decline when the user perceives that the website has little empathy for them and is willing to compromise their privacy for its own gains; similarly, the ability belief would decline as well when the user perceives that the website is not skilled and competent enough to be profitable on its own, and is thus resorting to tactics like sharing user information in an unauthorized way to gain business advantage. In hacking scenarios, users, for the most part if not completely, will exempt the website from any wrong doing and would in turn shift the majority of the blame externally on to the unknown hacker. The users might also associate the trustee has having less control over hacking event.

In unauthorized sharing based scenarios, decline in all three trusting beliefs would exert a downward push on the trust, more than the downward push for hacking based scenarios. Moreover, high initial trust users may feel even more downward pressure on their trust as opposed to low initial trust users for unauthorized sharing. High initial trust users would feel more wronged by unauthorized sharing, than low initial trust users. We as humans get more offended by the loved ones than by the strangers (Fitzpatrick and Winke 1979). Extending the above line of reasoning to trust domain, it could be argued that the high initial trust of the users will give them more reasons to feel offended by unauthorized sharing. Hence,

H2: Users will experience bigger trust drop for sharing scenario as opposed to hacking scenario.

H3: Initial trust level will moderate the trust drop associated with a negative news scenario in such a way that there will be bigger drop in trust for high initial trust users for unauthorized sharing news.

The research model is explained in Figure 1.

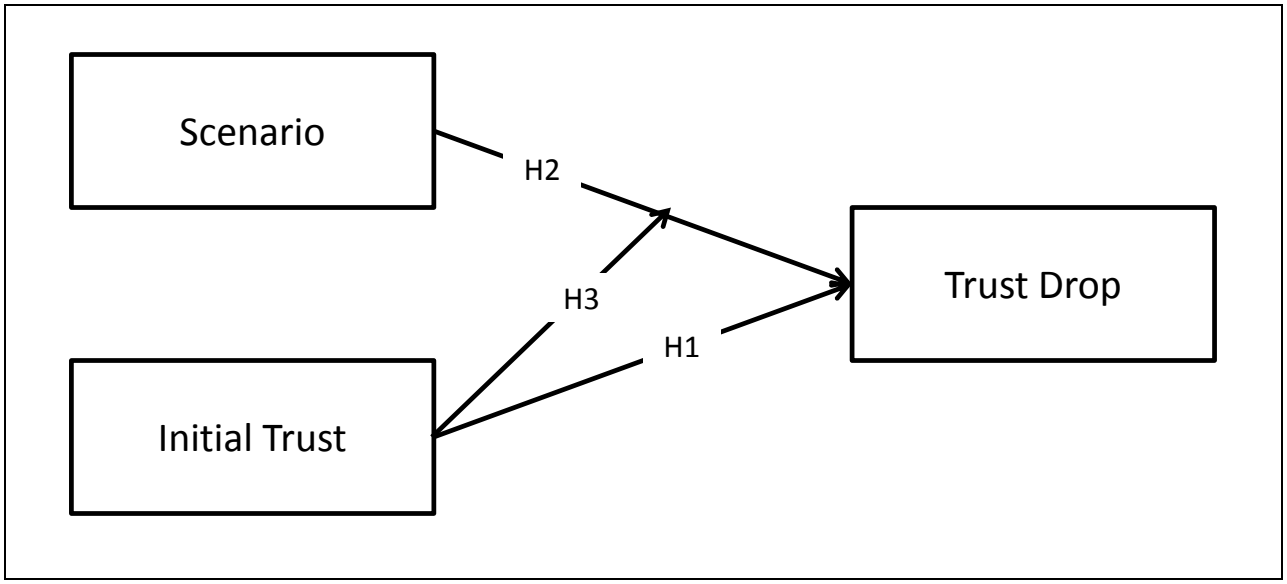

Figure 1. Research Model

RESEARCH METHODOLOGY

Data were collected from students studying in a Midwestern University. A total of 364 usable responses are included in this analysis. Students were shown a website and their initial trust (Trust1) was measured. Later the students were randomly shown one of the two scenarios (Table2): hacking news or unauthorized information sharing news.

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 2. Scenario Description

Both news scenarios involved the same magnitude of number of user accounts affected i.e. 24 million. Trust in the website was measured again (Trust2). Trust drop was tabulated by subtracting Trust2 from Trust1. We developed two factors for Trust1 and familiarity based on the four trust and two familiarity items, respectively. We split the Trust1 factor into high and low based on positive and negative factor scores. Anova analysis was then performed. Trust drop was used as the dependent variable; trust1: high vs. low, and scenario: sharing vs. hacking was used as the two factors. We controlled for familiarity by

using it as a continuous variable. Prior research has shown that trust bonding increases with prior familiarity (Gefen et al. 2003a), and thus might soften the trust drop.

	Male	**Female**	**N**	**Age Range**	**Age Mean (Std dev)**
Hacking	86	93	181	18-56	21.96(5.320)
Sharing	72	108	183	18-54	22.33(5.780)
Overall	158	201	364	18-56	22.14 (5.551)

Table 3. Demographics

Scenario based research design is appropriate for this study 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). The average age of the respondents is shown in the Table 3. The EFA analysis was performed for sharing and hacking based scenarios separately. EFA analysis is shown in the Table 4. The factor loadings are more than .7, and there are no cross loadings more than .40. The analysis, thus, confirms discriminant and convergent validity of the constructs.

	Hacking			Sharing		
	1	2	3	1	2	3
Initial Trust1	.197	**.864**	.130	.034	**.914**	.133
Initial Trust2	.164	**.837**	.124	-.006	**.890**	.095
Initial Trust3	.178	**.894**	.178	-.034	**.933**	.138
Initial Trust4	.158	**.899**	.119	.023	**.909**	.173
Familiarity1	.181	.203	**.917**	.172	.172	**.925**
Familiarity2	.225	.169	**.913**	.104	.221	**.925**
Final Trust1	**.865**	.250	.118	**.953**	-.038	.081
Final Trust2	**.878**	.268	.173	**.927**	.035	.047
Final Trust3	**.935**	.086	.201	**.956**	.024	.102
Final Trust4	**.907**	.147	.132	**.940**	-.005	.158

Table 4. EFA

Trust items were adapted from Gefen et al. (2003b). The items used are shown in Table 5.

Construct	Code	Item (on a scale of 0 to 10)
Trust		I believe that the website is
	Tr1	*.....not honest at all / very honest*
	Tr2	*.....opportunistic / dependable*
	Tr3	*.....not reliable at all / very reliable*
	Tr4	In general the level of my trust for the website is *(very low / very high)*
Familiarity	Fam1	I believe that the degree of my familiarity with the Website is *(very low / very high)*
	Fam2	I believe that the degree of my prior experience with the Website is *(very low / very high)*

Table 5. Scale

RESULT

The results are shown in Figure2. The left axis represent the trust drop. The horizontal axis represents binary categories of high and low initial trust. All the hypotheses were supported. The users lost more trust for sharing scenario (p value .000).

Users with high initial trust lost more trust (p value .000). The initial trust level played a moderating role such that those who had high initial trust, lost more trust for the sharing scenario than for the hacking scenario (p value .003).

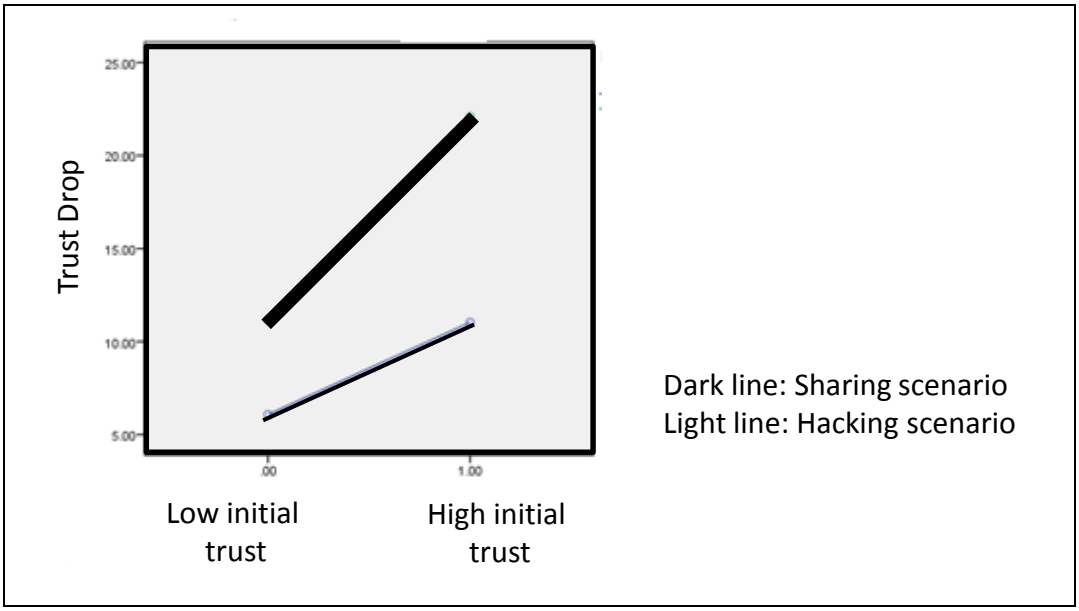

Figure 2. Result

DISCUSSION

The study provides several key theoretical implications. Studying trust lost is a timely issue. Prior trust has been known to be positively associated with trust revision (Zahedi and Song 2008). However, in lieu of negative news we show that the prior trust could also accelerate the trust decline as well. The finding also shows that not all privacy loss is equal. Both the scenarios entailed exposure of the same number of user accounts, still the trust lost was greater for unauthorized sharing instead of hacking. It suggests that privacy is important, no doubt, however, the way it is lost, is important as well. The interaction effect of scenario and initial trust levels provide rich support to the argument that there is more trust decline in the sharing scenario for high initial trust users. This shows that high trusting users feel more wronged by sharing news as compared to hacking news. There are several key managerial implications as well. Initial trust gets developed easily, and our study shows that it can also disappear easily – more easily when the basic assumptions on which it is based seem to be violated. Website managers should understand that even though sharing of user information is legally allowed, the users still find it more punitive than hacking. This study has limited generalizability since the respondents were students studying in a Midwestern university. Future research should look at different demographics, preferably across different cultural settings.

REFERENCES

1. Bhattacherjee, A. (2002) Individual Trust in Online Firms: Scale Development and Initial Test, *Journal of Management Information Systems*, 19, 1, 211-241.
2. Bies, R. J. and Tripp, T.M. (1996) Beyond Distrust: Getting Even and the Need for Revenge, in R. M. Kramer and T. Tyler, e.d., *Trust in Organizations*, Newbury Park: Sage Publications, 246-260.
3. 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.
4. Fitzpatrick, M. A., and Winke, J. (1979) You Always Hurt the One You Love: Strategies and Tactics in Interpersonal Conflict, *Communication Quarterly*, 27, 1, 3-11.
5. Gefen, D., Karahanna, E., and Straub, D. W. (2003a) Inexperience and Experience with Online Stores: The Importance of TAM and Trust, *IEEE Transactions on Engineering Management*, 50, 3, 307-321.

6. Gefen, D., Karahanna, E., and Straub,D. W. (2003b) Trust and TAM in online shopping: An integrated model, *MIS Quarterly*, 27, 1, 51-90.
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. Johnson, M. (2003) Keep The Romance Alive!, *Foodservice Equipment & Supplies*, 56, 12, 17-17.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. Wang, S., and Huff, L. C. (2007) Explaining buyers' responses to sellers' violation of trust, *European Journal of Marketing*, 41, 9/10, 1033-1052.
15. Weiner, B. (1985) An Attributional Theory of Achievement Motivation And Emotion, *Psychological Review*, 92, 548-573.
16. Zahedi, F. M., and Song, J. (2008) Dynamics of Trust Revision: Using Health Infomediaries, *Journal of Management Information Systems*, 24, 4, 225-248.