

Association for Information Systems AIS Electronic Library (AISeL)

SIGHCI 2007 Proceedings

Special Interest Group on Human-Computer
Interaction

2007

Antecedents of the Intention to Disclose Personal Information on the Internet: A Review and Model Extension

Horst Treiblmaier

Vienna University of Economics and Business Administration, Horst.Treiblmaier@wu-wien.ac.at

Sandy Chong

Curtin University of Technology, chongS@cbs.curtin.edu.au

Follow this and additional works at: <http://aisel.aisnet.org/sighci2007>

Recommended Citation

Treiblmaier, Horst and Chong, Sandy, "Antecedents of the Intention to Disclose Personal Information on the Internet: A Review and Model Extension" (2007). *SIGHCI 2007 Proceedings*. 19.
<http://aisel.aisnet.org/sighci2007/19>

This material is brought to you by the Special Interest Group on Human-Computer Interaction at AIS Electronic Library (AISeL). It has been accepted for inclusion in SIGHCI 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Antecedents of the Intention to Disclose Personal Information on the Internet: A Review and Model Extension

Horst Treiblmaier

Vienna University of Economics and
Business Administration
Horst.Treiblmaier@wu-wien.ac.at

Sandy Chong

Curtin University of Technology
chongs@cbs.curtin.edu.au

ABSTRACT

In order to reap the benefits which the Internet offers, users often have to provide personal information over the Web. Data types that are frequently required by online vendors include names, mailing and e-mail addresses, telephone numbers or credit card numbers. Previous research has identified several antecedents which influence users' decisions on providing personal details over the Web. This paper adds to the existing research by scrutinizing the concept of personal information and positing an individual's perceived risk of personal information as an antecedent of information disclosure. The results of an empirical survey show that users differentiate between various types of personal data according to the risk of privacy intrusion. Perceived risk of personal information turns out to be a stronger predictor for the intention to provide personal information online than trust in the Internet or in the online vendor.

Keywords

Data Sensitivity, Trust, Privacy, Information Disclosure, Partial Least Squares.

INTRODUCTION

With its potential for multimedia applications, the World Wide Web has significantly influenced the way consumers and businesses conduct commercial transactions in this day and age. Correspondingly, users' privacy concerns have become the focus of attention for practitioners and scholars alike. Communicating with companies or completing transactions online requires personally identifying information which might impose a risk for consumers in the case of data misuse (Shih, Dedrick and Kraemer, 2005). Even if their private data is used correctly, users inevitably have to forfeit parts of their privacy when interacting with businesses online (Culnan and Armstrong, 1999). Accordingly, previous research has identified a number of antecedents for the disclosure of personal information and doing business online, such as trust in the vendor (Pavlou, Liang and Xue, 2007) or trust in the Internet (Dinev, 2006).

In this paper we extend previous models by arguing that "personal information" is a complex rather than a homogeneous construct. By taking into account that a

multitude of data types exist which have varying levels of perceived sensitivity, we analyze the importance Internet users attach to their personal information in more detail. We achieve this by introducing the construct "perceived risk of personal information".

A GENERIC FRAMEWORK FOR THE DISCLOSURE OF PERSONAL INFORMATION

The adoption of Business-to-Consumer (B2C) E-Commerce has been one of the outstanding research topics in recent years. Trust (Gefen, Karahanna and Straub, 2003) and privacy (Liu, Marchewka and Ku, 2004) turned out to be of utmost importance for consumers to start purchasing online. More recent research identified the willingness to provide personal information online as an important antecedent of E-Commerce (Dinev, 2006), that plays a mediating role between privacy, trust and the adoption of E-Commerce. A minimum level of trust in the online vendor and the Internet must be given to induce users to forfeit parts of their privacy. By trading off the benefits of online transactions and potential privacy losses, customers are constantly conducting a "cost-benefit analysis" or "privacy calculus" (Laufer and Wolfe, 1977).

In order to keep our model parsimonious, we only integrated trust in the online vendor and trust in the Internet. When conducting transactions online, consumers in the first instance interact with a specific company and trust that it will protect their privacy. However, the Internet imposes a factor of its own, since many users are well aware that, even if the company is trustworthy, there is a certain amount of risk that data is captured during transmission, e.g. by hacking databases or by spoofing identities (Dinev 2006). In addition to these factors, which are specific to a buying situation, we argue that a general attitude toward personal information exists, which is comparatively invariant over time. Additionally, we include Internet experience in our analysis, since we argue that experienced users are more capable of assessing potential threats caused by online vendors and the Internet.

In the following sections we explicitly concentrate on the influence of trust (both in the online vendor and the Internet), the perceived risk of personal information, and the willingness to disclose personal information. Other

than previous research we differentiate between various data types, i.e. the perceived level of risk a person associates with a given piece of data. Most previous studies have tried to capture individuals' attitude toward their personal data without taking into account that the perceived risk may vary according to the respective data type.

RESEARCH MODEL

Our hypothesized research model can be found in Figure 1. The scales to measure trust in the Internet and the online vendor were taken from Dinev and Hart (2006) and Gefen et al. (2003). In order to measure users' perceived risk of personal information and their willingness to disclose them to online vendors, we used the perceived risk of various data items (name, home address, credit card number) as formative indicators. Experience with online data disclosure and general Internet experience were used as grouping variables.

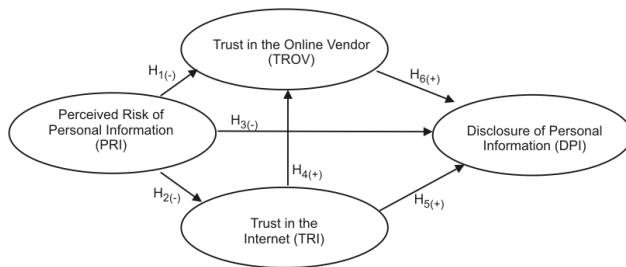


Figure 1: Research Model

In this study, we expect that the perceived level of risk associated with the disclosure of the data is related to the perception of the online company which collects data. While some consumers have an open attitude toward personal information, others take a more protective approach by refusing access or disclosure of information to any parties (Culnan, 1993). Thus, it is proposed that perceived risk in personal information to be related to trust in data collecting companies online.

H1: A higher level of perceived risk attached to personal information leads to a lower level of trust in the online vendor

An individual's perceived risk of personal information is likely to have significant effects on trust in the Internet. Some consumers may have a more relaxed attitude about personal information than others. Previous research has shown that considerable differences exist as to how users perceive the Internet's potential of privacy intrusion (Yao, Rice and Wallis, 2007) and causing them financial losses (Cunningham, Gerlach and Harper, 2005). This level of confidence or detachment toward personal information may be due to the cultural and social upbringing which determines how individuals perceive themselves to be part of a society, how open their attitude is when it comes to human interaction, and how important privacy is to them (Mitchell, 2003). It is therefore proposed that the

individual's perception of personal information to be related to level of trust one has about the Internet.

H2: A higher level of perceived risk attached to personal information leads to a lower level of trust in the Internet

In this study, we focus on individuals' perceived risk of personal information as the antecedent to disclose personal information. The study of these attitudes proposes that the higher risk one attaches to his or her own personal information, the lower the likelihood to disclose the details over the Web (Nam, Song, Lee and Park, 2006). Once one believes that there is little or no risk attached to personal information, perceived uncertainty is being reduced, confidence improves, and therefore the willingness to disclose this information is increased.

H3: A higher level of perceived risk attached to personal information leads to a lower level of willingness to disclose personal information

For the purpose of this study, the following definition of trust is adopted: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another" (Rousseau, Sitkin, Burt and Camerer, 1998, p. 395). Intrinsically, it implies an individual's willingness to accept vulnerability but with an expectation or confidence that it can rely on the other party. When an individual shops in an offline store, trust is often based on the interaction the individual experiences with the store – its products, salesmanship, and continued service after the purchase. The object of trust tends to expand from the company alone to the virtual environment in which it operates from – the Web site, the Internet, or the technology that enables the interaction and transaction online. An individual's perception of the capabilities and risks of the Internet contribute to the perception of confidence and positive expectation one would have in the online company. Therefore, it is hypothesized that when an individual generally possesses trust in the Internet, it is likely that the individual would trust the online vendor it interacts with.

H4: A higher level of trust in the Internet leads to a higher level of trust in online vendors

Given the level of sophistication in data mining, customer relationship management (CRM) software, and database marketing tools, consumers are increasingly becoming concerned about access to their personal information. Most of these concerns are related to privacy and security issues associated with the Internet being a huge cyberspace of uncertainty and unpredictability. The greater the uncertainty of access and use, the greater the concerns (Culnan, 1999). According to Dinev and Hart (2006), individuals who perceive the Internet as an environment in which there is a risk of other parties' opportunistic behaviors, also have concerns about who has access to personal information which they disclose. We posit that this concern about who has access to

information may influence an individual's willingness to disclose personal information over the Web. Thus, it is expected that trust in the Internet is related to the behavioral act on giving information online.

H5: A higher level of trust in the Internet leads to a higher level of willingness to disclose personal information

A high level of trust in the online vendor's competence, reputation, reliability, safekeeping of the data and goodwill has been shown to be related to consumers' decisions to purchase from the vendor (Chau, Hu, Lee and Au, 2007). Additionally, Xie, Teo and Wan (2006) found that a company's reputation is positively related to online users' provision of personal information. Nam et al. (2006) showed that the perceived convenience of a Website significantly influences users' privacy concerns, which in turn leads to a higher willingness to disclose personal information.

H6: A higher level of trust in the online vendor leads to a higher level of willingness to disclose personal information

It is expected that a low level of perceived risk of personal information disclosure may result from prior hassle-free or satisfactory experience with online and offline companies. This is anticipated to influence the perception of trust in a more 'risky' transaction context such as the Internet. Similarly, it has been shown that users' preferences for online versus offline purchasing are moderated by their Internet experience (Frambach, Roest, and Krishnan, 2007). We therefore consider Internet experience and experience with data disclosure as moderating variables in our analyses.

RESEARCH METHODOLOGY AND RESULTS

Descriptive Analysis

Our data sample consisted of 618 students (Austria: 298, Australia: 135, Hong Kong: 185). No significant differences between the countries can be found according to gender ($\chi^2=4.32$, $df = 2$, $p = .115$). However, we found differences according to age ($F = 16.50$, $df = 2$, $p < .01$) and Internet experience ($\chi^2=49.52$, $df = 4$, $p < .01$). A post hoc Tukey HSD test revealed that the sample from Hong Kong, which had a higher age mean (26.40 as opposed to 23.34 in Austria and 24.12 in Australia) has contributed to the significant deviation. Since only a total of four users classified themselves as being Internet beginners, we added them to the "basic knowledge" group. A higher proportion of students in Austria and Australia classify themselves as being "advanced users" and "experts" than in Hong Kong.

Figure 2 shows the perceived amount of risk which users associate with the disclosure of certain data types, which was measured on a 7-point Likert scale from 1-"not risky" to 7-"very risky". Comparable to the results from Xie, Teo et al. (2006), the credit card number stands out as those data type users see as most risky, followed by the home address and the telephone number (both of which allow

for being contacted in the offline world), the e-mail address and the name. In all but one category (e-mail address), users from Hong Kong were most risk-averse, followed by users from Austria, whereas Australian respondents consistently gave the lowest rankings. An ANOVA analysis revealed that all differences were significant at the 5% level.

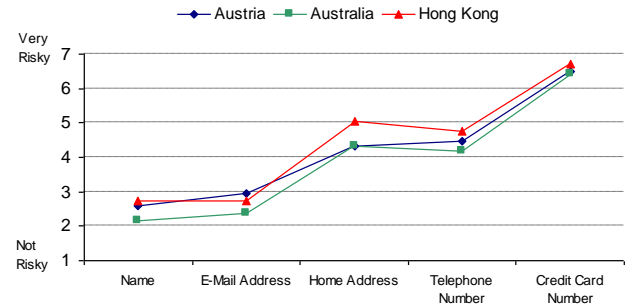


Figure 2: Perceived Sensitivity of Data

The intention to disclose personal information online, which is shown in Figure 3, mirrors the perceived sensitivity of the data (1-"not likely" to 7-"very likely"). Accordingly, users are most skeptical when it comes to the disclosure of the credit card number, followed by the telephone number and the home address. Contrariwise, they are much more likely to disclose their name and the e-mail address. Again, an analysis of variance showed that all differences were significant at the 5% level.

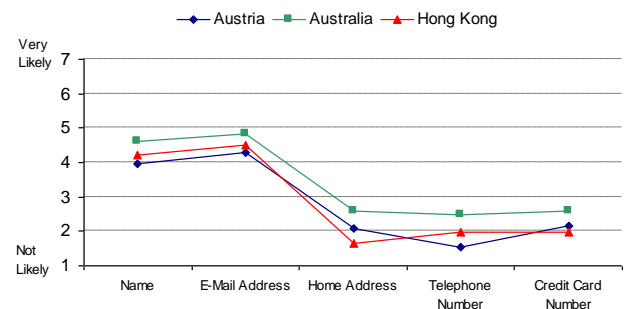


Figure 3: Intention to Disclose Private Data

Apparently, users differentiate between different data types according to their perceived risk. A factor analysis revealed three different dimensions, with (a) the name and the e-mail address, (b) the home address and the telephone number, and (c) the credit card number loading on one factor, respectively. Since our indicators are defining the characteristics of the construct, they are not interchangeable and they do not necessarily covary with each other (which may be the case when e.g. a limitation of liability is introduced for credit card fraud), we used three formative indicators (name, home address, credit card number) to measure the perceived risk of personal information and the intention for its disclosure (Jarvis, 2001). We used a two-step approach which first assessed

the quality of the measurement model before testing our hypotheses through the structural model.

Measurement Validation

Prior to testing our model with PLS (Partial Least Squares), we assessed the quality of the measurement model. The two reflective constructs (trust in the Internet, trust in the online vendor) possess significant levels of reliability (Cronbach's Alpha and Composite Reliability > .7). In order to assure factorial validity, we conducted a confirmatory factor analysis with the results indicating sufficient levels of convergent and discriminant validity.

The structural model is depicted in Figure 4. It can be seen that both the influence of perceived risk of personal information on trust in the online vendor (H1) and on trust in the Internet (H2) are significant at $p < .05$. However, the most important relationship in our model is between perceived risk of personal information and the intention to disclose personal information (H3, $p < .01$). We also found a significant influence of trust in the Internet on trust in the online vendor (H4, $p < .01$), whereas the influence of trust in the Internet (H5) and trust in the online vendor (H6) on the willingness to disclose personal information turned out to be not significant for the disclosure of personal information.

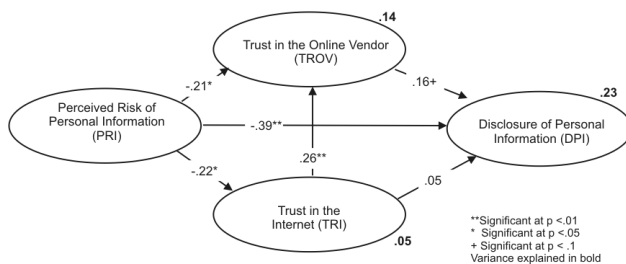


Figure 4: PLS Results for Disclosure of Personal Information

Group Comparisons

We split our data set according to culture, Internet experience and frequency of Internet usage (see Table 1). It is found that the impact of perceived risk of personal information (PRI) on disclosure of personal information (DPI) is the most important relationship across all different national groups, experienced and inexperienced users and Internet users who frequently disclose personal data as opposed to user who infrequently give away their data. Experienced users exhibit a significant influence of perceived risk of personal information on trust in the

online vendor and trust in the Internet, whereas for inexperienced users these path coefficients are nonsignificant. The same situation applies for frequent vs. infrequent Internet users, with significant relationships between perceived risk and trust for the former group.

CONCLUSIONS AND LIMITATIONS

In this paper we have shown that Internet users clearly differentiate between different data types. Although the level of perceived risk was significantly different between users from three different countries, the relative assessment was strikingly similar. Generally speaking, data types such as name and e-mail address were seen as less sensitive compared to personal details such as home address and telephone number. Credit card number was by far the most sensitive data type in all three surveys. Based on these results, we created a construct which used three data types (name, home address and credit card number) as formative indicators. The results of a PLS analysis show that the perceived risk of personal information is the best predictor for an individual's willingness to provide personal information online. Our research has strong implications for organizations which want to establish B2C-E-Commerce online. In spite of the substantial growth rates of E-Commerce during recent years, many users still refrain from disclosing personal information online. While in the long term it may be possible to change users' risk perception for the disclosure of private data (e.g. by establishing a relationship based on trust), in the short run there seem to be less options for companies.

One viable solution might be to concentrate on collecting only those data types which are perceived as being less sensitive or to use trusted intermediaries, such as PayPal.

As in every empirical research project, there exist limitations which should be addressed in future research. First, there is a gap between users' stated preferences and their actual behavior which is especially pronounced in an online environment (Berendt, Günther and Spiekermann, 2005). Second, we concentrated on student samples to make sure that factors such as age and education are comparable across countries. However, in order to ensure external validity of the results, additional empirical validation with other user segments is recommended.

	Austria	Australia	Hong Kong	Experienced	Inexperienced	Frequent	Infrequent
PRI -> TROV	-.21*	-.13	-.19+	-.19*	-.14	-.22*	-.15
PRI -> TRI	-.24*	-.30**	-.21+	-.27**	-.19	-.23*	-.20+
PRI -> DPI	-.40**	-.47**	-.30*	-.37**	-.49**	-.42**	-.46**
TRI -> TROV	.32**	.26*	.30*	.28**	.29**	.26**	.28**
TRI -> DPI	.07	.08	-.08	.13	-.08	.07	-.05
TROV -> DPI	.12	.25*	.22+	.15+	.11	.11	.18+
R ² TROV	.18	.10	.15	.15	.12	.14	.12
R ² TRI	.06	.09	.04	.07	.04	.05	.04
R ² DPI	.22	.37	.15	.25	.26	.23	.26

Table 1: Group Comparisons (+p < .1, * p < .05, **p < .01)

10. L

REFERENCES

- Berendt, B., Günther, O. and Spiekermann, S. (2005) Privacy in E-Commerce: Stated Preferences vs. Actual Behavior, *Communications of the ACM*, 48, 4, 101-106.
- Chau, P.Y.K., Hu, P.J.-H., Lee, B.L.P. and Au, A.K.K. (2007) Examining Customers' Trust in Online Vendors and their Dropout Decisions: An Empirical Study, *Electronic Commerce Research and Applications*, 6, 2, 171-182.
- Culnan, M.J. (1993) How Did They Get My Name?: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use, *MIS Quarterly*, 17, 3, 341-363.
- Culnan, M.J. (1999) Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission, Georgetown University, Washington D.C.
- Culnan, M.J. and Armstrong, P.K. (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science*, 10, 1, 104-115.
- Cunningham, L.F., Gerlach, J. and Harper, M.D. (2005) Perceived Risk and E-Banking Services: An Analysis from the Perspective of the Consumer, *Journal of Financial Services Marketing*, 10, 2, 165-178.
- Dinev, T. (2006) Why Spoofing is Serious Internet Fraud, *Communications of the ACM*, 49, 10, 76-82.
- Dinev, T. and Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions, *Information Systems Research*, 17, 1, 61-80.
- Frambach, R.T., Roest, H.C.A. and Krishnan, T.V. (2007) The Impact of Consumer Internet Experience on Channel Preference and Usage Intentions Across the Different Stages of the Buying Process, *Journal of Interactive Marketing*, 21, 2, 26-41.
- Gefen, D., Karahanna, E. and Straub, D.W. (2003) Trust and TAM in Online Shopping: An Integrated Model, *MIS Quarterly*, 27, 1, 51-90.
- aufer, R.S. and Wolfe, M. (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory, *Journal of Social Issues*, 33, 3, 22-42.
- Liu, C., Marchewka, J.T. and Ku, C. (2004) American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce, *Journal of Global Information Management*, 12, 1, 18-40.
- Mitchell, S. (2003) The New Age of Direct Marketing, *Journal of Database Marketing*, 10, 3, 219-229.
- Nam, C., Song, C., Lee, E. and Park, C. (2006) Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online, *Advances in Consumer Research*, 33, 1, 212-217.
- Pavlou, P.A., Liang, H. and Xue, Y. (2007) Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective, *MIS Quarterly*, 31, 1, 105-136.
- Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerer, C. (1998) Not So Different After All: A Cross-Discipline View of Trust, *Academy of Management Review*, 23, 3, 393-404.
- Shih, C.-F., Dedrick, J. and Kraemer, K.L. (2005) Rule of Law and the International Diffusion of E-Commerce, *Communications of the ACM*, 48, 11, 57-62.
- Xie, E., Teo, H.-H. and Wan, W. (2006) Volunteering Personal Information on the Internet: Effects of Reputation, Privacy Notices, and Rewards on Online Consumer Behavior, *Marketing Letters*, 17, 1, 61-74.
- Yao, M.Z., Rice, R.E. and Wallis, K. (2007) Predicting User Concerns about Online Privacy, *Journal of the American Society for Information Science and Technology*, 58, 5, 710-722.