J. Basic. Appl. Sci. Res., 3(3)571-577, 2013
© 2013, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspective

Mahmood H Shah[1], Ramanus Okeke[1], Rizwan Ahmed[2]

[1]Lancashire Business School University of Central Lancashire
[2]Faculty of Management Studies, University of Central Punjab

ABSTRACT

Despite rapid growth in e-commerce, many of the privacy and trust issues concerns remain unaddressed. We report a qualitative study on customers' concerns over privacy and trust in online purchasing. A number of issues such as data privacy, data security and safety, data disclosure and sharing by the seller with third parties have been explored with regular internet shoppers. The findings suggest that trusted/branded websites, secured websites, websites with clearly stated data protection/privacy policies makes people more comfortable in online shopping and decreases their data privacy concern. While unsecured websites, vague data protection/privacy policy, disclosure of data to the third parties; in turn discourage the users from releasing their personal data while shopping online.
KEYWORDS: trust and privacy, online shopping, issues in e-commerce

1. INTRODUCTION

This paper reports a preliminary investigation of a research project aiming an in depth study of customers' concerns about privacy and trust in online purchasing.

The rapid growth of electronic commerce has created tremendous opportunities for economic gains for businesses as well as consumers. Online merchants handle and store personal data of millions of customers every year. Impersonal nature of online purchasing gives rise to the questions about the users' data privacy and trust; which in turn has led to the growing privacy concerns amongst the customers. Thus, the need to investigate data privacy concern of customers is imperative; which would assist online merchants and marketers to understand customers' perspective of privacy and trust and enable them develop and modify policies and processes to boost up confidence of their customers (Fienberg, 2006).

Several empirical studies report the growing privacy concerns amongst internet customers (Acquisti & Grossklags, 2005); suggesting that there should be a mechanism that enables customers to manage the privacy of their personal data online. But empirical research argues that most customers may not be capable of making privacy decision and are sometimes likely to trade off long-term privacy for short term benefits (Spiekermann & Cranor, 2009). Therefore major responsibilities rest with online merchants to provide a reliable mechanism to protect customers privacy and gain their trust.

While most researches focus on attitudes or actual behaviour of the users in shopping online with little interests to their concern about personal data privacy (Monsuwe et al., 2004, Shah et al., 2005); this research aims to examine the extent of the users' concern about data privacy by investigating users' perceptions about data privacy in online purchasing.

1. Customers' Concerns over Personal Data Privacy

Lanier (2008) argues that customer's data privacy issues have not been understood very well; further research is needed understand data privacy issues which will enable better management of customer-merchant relationship. Luo (2002) notes that if the issues of data privacy in e-commerce are dealt more effectively, customers may have fewer concerns over merchants' access to their private data.

Mineta (2000) identifies data privacy amongst the major problems affecting users' confidence in any online business transaction. The requirement of personal data in online business transactions instigates an anxiety in customers regarding their personal privacy. It is important to investigate both the causes and effects of such concerns and anxieties. Researchers identify data usage, user awareness, data sensitivity, compensation, and familiarity with firms as five major influences on the users' privacy concerns. Lanier (2008) says that customers get particularly concerned about their private data if they learn that some online merchant has used their personal data without their consent.

***Corresponding Author:** Rizwan Ahmed, Faculty of Management Studies, University of Central Punjab, 1-Khayaban-e-Jinnah Road, Johart Town, Lahore, Pakistan. E-mail: drrizwan@ucp.edu.pk Tel/Fax/Mob: +92-321-4405445

Looking at privacy concern from the context of compensation, Free (2006) points out that the users will only disclose their personal data if the benefits they receive outweigh the cost of the disclosure. Earlier, Westin (1967) had argued that the heart of user's privacy concern is the trade-off between the benefit and cost of disclosure of their personal data. In terms of data usage, users are much concerned about their data privacy if they do not know how their data are being used. There is anxiety on the part of users if the personal data supplied online is used for the purposes other than the particular online transaction (Phelps *et al.*, 2001).

Besides compensation and data usage, sensitivity of personal data has impact on the user's privacy (Sheehan, 2000). Data or information sensitivity is the degree to which users feel that their personal data or information, if shared with other, can harm them (Gandy, 1993). More sensitive the data is, more concerned the users will be about its privacy. Wang *et al.* (2004) found that customers' familiarity with the online merchant, in general, reduces their privacy concerns.

1.1. Data Privacy and Trust

Data privacy and trust are noted by the researchers as the major challenge for online businesses. E-trust as termed in some recent studies remains the most important factor to boost e-commerce (Brynjolfsson & Smith, 2002). It was found that trust is amongst the factors that have the greatest impact on the attitude of users in e-commerce (Korgaonkar, *et al*., 2006). This report calls for further research to ascertain the extent at which customers' privacy concerns relates to trust in online business. Campbell, *et al.*, (1997) suggest that building and enhancing online trust could be a better way to address the customers' data privacy concerns in e-commerce. Since privacy and trust are directly related, establishing procedures to enhance user's trust may lessen customers' privacy concern. It was noted that many online firms have successfully implemented various procedures to comply with fair data and information practices (Chang, *et al*., 2005). Among the commonest of the practices is customer opt-out choice. With this practice the customers could remove their name from any unfriendly mailing lists.

The Internet Society Report (2008) noted that in many cases business on the internet suffers due lack of trust. It is also noted that lack of trust on the web is the basic reason many users choose not to engage in online transactions (Akin, *et al.*, 2005).

1.2. Data Privacy and online security

Online security is a major barrier to effective utilization of internet as marketing tool (Bush, *et al*, 2000). Jones (2004) noted that many customers are unwilling to engage in e-commerce because of uncertainty regarding issues of security and privacy of the data transaction. Researchers have also noted that the perception of system security was the biggest fear for the online users while threat of data interception by the third party follows (Miyazaki & Fernandez 2001).

1.3. Data Protection Policies

A survey of the top 100 e-commerce sites by the Electronic Privacy Information Centre in 2005, found that some online users often perceive most privacy policies to be confusing, inconsistent, incomplete, and sometimes misleading. Such policies may end up frustrating the customers who attempt to understand how well their personal privacy is protected as per policy. This may in turn has negative impact upon the customers' attitude. Although there are some robust examples of online seal programs such as TRUSTe, MasterCard, Visa, and BBBOnLine used by the e-commerce industry to build users' confidence, many online businesses tend not to adhere to such robust privacy principles.

Berendt et al (2005) claim that about 75% of the German users surveyed in their study are afraid that their data privacy might be compromised while shopping online; 60% tend to avoid providing personal information to websites; while 47% provide fake personal data online. It is obvious many users have doubt about the integrity and efficiency of commercial websites' data protection measures.

1.4. Sharing and Selling Personal Data

In the field of Internet marketing, invasion of data privacy is specifically interpreted as the unauthorized collection, disclosure, or other use of personal data such as sharing or selling it to third party or other marketers (Korgaonkar, *et al*. 2006). From the economic viewpoint, such practices have negative impact in e-commerce and web users. Since unauthorized disclosure of personal information may result in inconvenience and wastage of time due to spam and unsolicited emails, this may consequently lead to online customers' reluctance to engage in electronic commerce (Udo, 2001).

A report by University of California – Los Angeles Center for Communication Policy (2001) suggests that about 94.5% of both internet users in America are concerned about privacy of their personal information trading

online; and a similar report covering European online market suggests that 58% of the respondents surveyed considered data privacy concerns as restraining factor to their online business interests (Clickz, 2010).
Table 1 summarizes the collated literature review of the personal data privacy. This review suggests that most of the past research works focused on the interests of the online businesses with little attention paid towards customers' interests, perceptions, concerns over their personal data privacy. This research aims to cover this gap and also foster the ground for further research in privacy related issues.

Table 1: Adapted from Lanier & Saini, (2008).

Publication	Focus of the Literature	Key Concepts/Issues	Proposals and Findings
Spiekerman & Cranor (2009)	Three layer model of users' privacy concerns on the users' behavior.	Development of guidelines for building privacy-friendly systems.	The effect of the users' privacy approach depends on the principle and practices of the system in use. While the privacy by policy focuses on implementation, the privacy by architecture minimizes the collection of identifiable personal data.
Lanier & Saini (2008)	Review of an understanding of general concept of users' privacy.	Provision of the general concept of consumer privacy and suggestion of future research.	Users show concern when they become aware that the firm has used their personal data without their consent.
Lwin, Williams & Wirtz (2007)	Examination of Online privacy concerns and policy responses.	Development of the Power-Responsibility Equilibruim (PRE)	The higher the degree of privacy concern and protective plans the weaker the perceived company privacy policy
Eastlick, Lotz & Warrington (2006)	Consumers' privacy concerns examination based on trust, commitment, and purchase intention	Application of model of information privacy in examination of the hypotheses that consumers' privacy concerns directly and indirectly impact their online purchase intentions.	The consumers' purchase intentions are influenced by privacy concerns with strong negative effects directly and indirectly through trust.
Pollach (2005)	Determination of whether privacy policies from a linguistic perspective adequately enable informed consent	This involves examination and exploration of key stakeholders in online privacy and presentation of privacy policies based on findings of critical linguistic analysis.	Corporate privacy policies of the company use persuasive appeals to influence consumers trust. There is need for privacy policies to be written in clear manner.
Milne & Culnan (2004)	Examination of why consumer do not read or read online privacy notices	Examination of the role of trust, concern, experience, demographics, etc. on reading of online privacy notices.	Privacy concern and positive perceptions about notice comprehension influence reading online privacy notices.
Dommeyer & Gross (2003)	Examination of knowledge of consumers about privacy related laws and protection strategies.	Development of scales for awareness, knowledge and protection.	It was found that consumers have fairly little knowledge of direct marketing regulations and practices.
Kannan, Peng, & Rust (2002)	An economic model development for the projection of erosion of consumer privacy.	Based on some assumptions such as: consumers have an ideal level of privacy, technology is advancing, etc.; the economic model of privacy was developed.	It was found that the amount of privacy will decline over time as the cost of processing information decreases, which would in turn increase the cost of maintenance of privacy.

2. RESEARCH METHODOLOGY

We used face-to-face semi-structured interviews as the as the data collection instrument mainly consisting of open ended questions. A set of four pilot interviews was conducted using an initial set of questions to evaluate their appropriateness and relevance and to judge the appropriateness of interview duration. All the interviews were recorded using Sony® Digital Voice Editor 2 and transcribed on MS Word.

Interviewees consisted of university students, faculty and staff who were regular online shoppers. In the main set of interviews 9 participants were interviewed and each interview lasted for about 15 to 20 minutes. A list of the participants' and their background is provided in Table 2.

Interviews with the students were conducted in the university library while those of faculty and staff were conducted in their offices. The consent of these participants was sought in time before the interview appointment through e-mail and interviews were recorded with their permission.

Literature review facilitated the formulation of our theoretical framework and a set of relevant questions. The key questions revolved around following themes:

- Any experience where their privacy was violated after engaging in online shopping
- Their key concerns before releasing personal information in online shopping

- What factors raise their concerns over their data privacy?
- Do they believe that they have the rights and/or control over their personal data in the hand of online marketer?

The collected data from the nine interviewees was transcribed verbatim for analysis. The following section presents findings of the data analyzed.

Table 2: A list of the interview participant with their respective roles

Interviewee Code	Participant Profession
P1	Faculty
P2	IT Staff
P3	Student MSc – Computing
P4	Student PhD – Business
P5	Student Undergrad - Software Engineering
P6	Faculty
P7	Student Undergrad - Business Management
P8	Staff
P9	IT Staff

3. FINDINGS & DISCUSSION

From the nine interviewees, the following themes were extracted from the interview transcripts. The discussion of these key themes with references to the interviewee statements are further analysed to understand the user's belief, perception over their data privacy. The commonest themes from the interview statements are: awareness of data usage, websites trust and branding, data disclosure to third parties, data protection/privacy policy, and data and internet security.

The general finding from the data analysis suggest that trusted/branded websites, secured websites, and websites with clearly stated data protection/privacy policies decreases the data privacy concern of the customers while shopping online (shown in figure 1 below). On the other hand, unsecured websites, website with vague data protection/privacy policy, disclosure of data to the third discourage customers from releasing their personal data while shopping online. Following we discuss the findings in detail.

3.1. Awareness of Data Usage

The views of our participants suggest that if online merchants clearly state that how their personal data is going to used, they will feel comfortable in providing their personal details for online shopping. In the words of P1

"Yes, it is discouraging because when you see those e-mails, yes it em, it signal you that they… your details (personal data) are not secure, yes, em its makes you to be aware of how you put your details when you shop online or when you do some other online transaction,… yes… but for me personally, it makes me uncomfortable, but if the there is prior notification or awareness on how my data is going to be used, I think many users not only myself would be comfortable to supply their personal data".

This finding supports a earlier finding Monsuwe *et al,(2004.*) that if customers are aware and understand how their data is going to be used, their bar of concerns are lowered. Therefore, we can suggest that that educating the customers on how the information the supply online will be used opens ways for better cooperation by the customers.

3.2. Brand/Trusted Websites

Our data finding suggests that a website or company brand name plays the most important role in building trust amongst online customers; brand name recognition is the most is one of the most emphasised themes by our participants. As P3 says

"I think if you talk to anybody of most issues online, they can not mention any other site without mentioning Amazon. Yes that is why I said that there is this kind of trust there from the users"

Similarly one other respondent states:

"for me personally I think, how to deal with them is that I don't disclose my personal information regularly online, so I would only disclosed them to those well known websites"

This suggests that online customers frequently shop from those websites which are regarded as 'well known and trusted' shops. This is also in support the work of Lauer and Deng (2007) Hence, there will be an increase in the privacy concerns amongst customers if an online shop is not well known and recognized.

3.3. Data Disclosure to Third Parties

The fear of the users' personal data being shared or sold to the third parties is found to increase the data privacy concerns. In some cases, even if the users are assured that their data would not be revealed to the third parties after, but customers may be concerned about what happens in an event online shops are sold to another company or forced by law enforcement agencies to share their data. For example, P4 states:

"*these days some companies that are using a bit of formulation strategy to get on some customers. Like for instance Amazon there something they put on their agreement where you click. Clicking on it means that you are accepting that your information would be distributed to the third party, but this does not mean that em.. online shop owners do not give out information to the third party. Like at the moment, it is understood that information are being giving out to the law enforcement bodies for crime fighting. Even when they told you that this information would not be given out, they at least give the information to the law enforcement bodies. Because of the fact that they can't stop law enforcement body from doing their investigation, the online shop owner has restructured their terms of agreement. They have now included that you data could be sent to the third party if it has to do with crime fighting. This also they have used in the structure of their agreement that your information could be given out but just on specific reasons…., so how do you deal with the situation like this?"*

Some customers may perceive this as a case of data sharing on the positive ground, but many customers may consider it a breach of their privacy. This could discourage some customer from trading online in order to save themselves from unwanted disclosure personal data.

3.4. Data Protection/Privacy Policies

Our participants suggest that an online shop without clearly stated data protection/privacy policy increases the data privacy concern of the users. Most respondents said that they tend not to purchase without having privacy policies certified law enforcement bodies. This finding somewhat contradicts with the Reagle *et al*. (1999) research study which notes that privacy policy is one of the least factor that influences the users data privacy concern. Our study suggests that most of our participants pay absolute attention while reading these policy statements before shopping in any intended websites.

From example P7, who always reads the privacy/protection policies before shopping on the internet, states that:

"*Yes, if it is websites that I have not shopped on before then I do read the terms and policies to make sure I got the terms and conditions, then if I am not happy with what they send to me and I can send it back again and search for the websites with certified policy statements*".

Similarly P8 says:

"*the Apple privacy violation case in 2008 of which Apple's privacy policy says that personal information will be shared by Apple to improve services and advertising but that it won't be shared with third parties for their marketing purposes…, but in the this case Apple was charged from invasion of privacy to violation of the stored communication act*".

This incidence suggests that there are growing concerns amongst online customers over privacy protection policies and people are getting more conscious about the privacy policies of online merchants.

3.5. Data/Internet Security

Most of our participants are show concern about unsecured websites. They say that they are keen to find out how well an online shop is secured before making a purchase. This finding supports Jones (2004) finding, where he noted that many users are unwilling to engage in e-commerce because of uncertainty over their personal data security. As P5 affirms:

"*the key things you worry about is security, yes security of my data…, I care about the security of my data, you never know, some might be watching! These days I am watchful of this security logo of padlock on the websites, which was not used to happen before. This makes the user to feel extra safe…, but like I said before, it is all about trust, if it is a website I don't trust, I can use a fake name…… yes… for security reasons.. I might put the correct address but I will put wrong name… You know you don't really know who to trust…yes sometimes you do sometime like that for security reasons…, as for the trusted known companies like e-bay, Amazon, putting in your data in their websites would be more secure because you are one of their customer. Also when you look at this being a large website they have many people working on their security".*

4. Conclusion

In summary, the finding suggest that trusted/branded websites, secured websites, websites with clearly stated data protection/privacy policies makes people more comfortable in online shopping and decreases their data privacy concern. While unsecured websites, vague data protection/privacy policy, disclosure of data to the third parties; in turn discourage the users from releasing their personal data while shopping online.

This result of this paper is based on a limited convenience sample of the university community who engages in electronic commerce and needed to be confirmed by larger sample size. Our study does not take into account some demographic factors such as the influence gender, age, literacy and technology awareness on privacy concerns. In future we plan to conduct a large scale survey study and confirm the findings of the survey study through empirical methods such as controlled experiment or ethnography. This will help generalizing the results of our study and the studies previously conducted by other researchers.

The outcome of such studies can be used by stakeholders in policy making and management of e-commerce in order to boost the consumers' confidence in electronic marketplace. It can also foster further research on software technology for controlling and monitoring user's data online and further understand the impact of privacy on business organisations.

REFERENCES

ACQUISTI, A, and GROSSKLAGS, J., (2005). Privacy and Rationality in Individual Decision Making, *Security & Privacy, IEEE*, 4 (1), pp. 26 – 33, ISSN: 1540-7993

BETTINNA, B., (2005). Privacy in E-Commerce: Stated Preferences vs Actual Behaviour, Institute of Information Systems, *Communications of ACM*, 48(4), pp. 101-106.

BRYNJOLFSSON, E., & SMITH, M. D., (2002). A comparison of Internet and conventional retailers. *Working paper, MIT*, Available at www.ecommerce.mit.edu/papers/friction, [Accessed: 27/08/2010]

CHANG , L., *et al*, (2005). A privacy trust behavioral intention model of electronic commerce. *Journal of Information and Management*, 42(2), pp. 289-30

DOMMEYER, C. J., & GROSS, B. L., (2003). What Consumers Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing*, 17 (2), pp. 30-51.

EASTLICK, M. A, LOTZ, S. L., WARRINGTON, P. (2006). An integrated model of privacy concerns, trust and commitment. *Journal of Business Research*, 59(8), pp. 870-880.

FIENBERG, S. E. (2006). Privacy and Confidentiality in an e –Commerce World: Data Mining, Data Warehousing, Matching and Disclosure Limitation, *Institute of Mathematical Statistics*, 21 (2), pp. 143-154.

FREE C., and ASHWORTH, L. (2006). Digital Privacy & Marketing Dataveillance: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics*, 67 (2), pp. 107 – 123.

GANDY, O., (1993). *The Panoptic Sort: A Political Economy of Personal Information*. New York: Westview.

JONES, E., *et al*, (2004). Organisational communication. *Journal of Communication*, 54 (4), pp. 722-750.

KANNAN, P. K., RUST, R. T., PENG, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science*, 30 (4), pp. 450-464.

KORGAONKAR, P. K & WOLIN, L. D., (2006). A multivariate Analysis of Web Usage. *Journal of Advertising Research*, pp. 53– 68.

LANIER, C. D., (2008). Understanding Consumer Privacy: A Review for Future Directions, *Academic Marketing Science Review*, 12 (2).

LUO, X., (2002). Trust Production and Privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*. 31 (2), pp. 111-118.

LWIN, M., WIRTZ, J. & WILLIAMS, J. D., (2007). Consumer online privacy concerns and responses. *The Journal of Consumer Affair*, 35 (4), pp. 570-587.

MARSHALL, C. and ROSSMAN, G. B. (1999). *Designing qualitative research*, 3rd ed. Sage Publications.

MILNE, G. R., ANDREW, J. R.,and SHALINI, B. (2004). Consumer Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 38 (2), pp. 215-232.

MONSUWE, T., BENEDICT, G.C., and KO, R. (2004). What drives consumers to shop online? International Journal of Service, 15 (1), pp. 102-121.PHELPS, J. E., GILES, D., AND GLEN, J.

N, (2001). An empirical investigation - Antecedents and consequences of consumer privacyconcerns, *Journal of Interactive Marketing*, 15 (4), pp. 2-17.

POLLACH, I. (2005). A Topology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics*, 62 (3), pp. 223-230.

REAGLE, J., ACKERMAN, M. S., and CRANOR, L. F. (1999). Privacy in E-Commerce:

Examining User Scenarios and Privacy Preferences, *ACM Conference on Electronic Commerce Publications*, pp. 1-8.

SHAH, M. A. A., & SINGH, R., (2005*). BUILDING CONSUMER TRUST. An ONLINE perspective. Social Science and Business Administration Programmes*. ISSN: 1653 – 0187.

SHEEHAN, K. B., (2005). An assessment of privacy policies at direct to consumer websites. *Journal of Public Policy & Marketing*, 24 (3), pp. 273-283.

SOLOVE, D. J. (2006*). The Digital Person: Technology and Privacy in the Information Age*. New York University Press.

SPIEKERMANN, S. and CRANOR, L. F., (2009). Engineering Privacy. *IEEE Transactions on Software Engineering*, 35 (1).

UDO, G. J., (2001). *Privacy and Security Concerns as a Major Barriers for E-Commerce: A Survey study*, 9 (4), pp. 165-174, ISSN:0968-5227

WANG, H., LEE, M. K & WANG, C., (2003). Consumer privacy concerns about Internet marketing. *Communication of ACM*, 41, pp. 63–70.

WESTIN, A., (1967). *Privacy and Freedom*, New York: Atheneum.