December 2004

Consumer Empowerment and Its Impact on Information Privacy Concerns and Trust: A Theoretical Model

Vishal Midha
University of North Carolina at Greensboro

Hamid Nemati
University of North Carolina at Greensboro

Consumer Empowerment and Its Impact on Information Privacy Concerns and Trust: A Theoretical Model

Vishal Midha
University of North Carolina at Greensboro
v_midha@uncg.edu

Hamid Nemati
University of North Carolina at Greensboro
nemati@uncg.edu

ABSTRACT

This paper proposes a theoretical model incorporating information privacy concerns and consumers' options and rights as the two antecedents for trust in an organization. We posit that by providing the users with choice and access to the information collected about them, an organization can help reduce the tensions that arise due to consumer's information privacy concerns while increasing the trust in that organization, which is a critical factor in stimulating purchases over internet, especially at this early stage of commercial development (Quelch and Klein 1996).

Keywords

Trust, Privacy, Privacy concern, Consumer/User rights

INTRODUCTION

Even though the technology is approaching towards mobile-commerce (m-commerce) and universal-commerce (u-commerce), still a decade old electronic commerce (e-commerce) has not achieved its full potential. Individuals are willing to participate in diverse activities online – from emailing friends and family to looking up personal medical information. While consumers benefit from their activities online, businesses also benefit from information gained while consumers browse. Past research shows that "many individuals are unaware of the extent of the personal data stored by government and private corporations" (Roddick, 2001). Furthermore, numerous studies have shown that Internet users display incongruities between concern for privacy online and the type of online activities in which they are will to participate. If individuals were educated regarding this collection of information and the ways in which the information is used, would they still demand mass customization? Would an Internet user's level of concern be heightened by this knowledge?

One of the crucial reasons cited for this is the lack of consumer's confidence in confidentiality and privacy in online transactions (Hemphill 2002).

But, what is this privacy and its invasion? - The term privacy is defined as 'the right to be let alone', 'the state of being free from unsanctioned intrusion (www.dictionary.com)' and is related to solitude, secrecy, and autonomy. Whereas in the arena of the electronic marketplace, privacy is usually referred to as 'personal information' and the invasion of privacy is usually interpreted as 'the unauthorized collection, disclosure, or other use of personal information as a direct result of electronic commerce transactions' (Wang et al 1998). It is the ability of the individual (consumer) to control the terms under which personal information is acquired and used (Westin 1967).

Imagine that while shopping at a traditional supermarket, you are continuously followed by sales representative. You notice that the sales representative is making a complete log of everything that you purchase or even look at. And when you remove something from your cart that you don't feel like purchasing at that moment, the sales representative offers you a discount on the items that you are putting back on the shelf. By doing so, the customer representative is acquiring the data about your interests and likings without your permission. Or in other words, he is invading your privacy. And this is exactly what happens when you are shopping online. The online companies are keeping track of each and every move that you are making and you may not even be aware of this collection of the information. In most of the cases, users do not become aware that information about them was collected until after the information is collected. Consumers generally become aware when they receive some type of marketing communication from an entity that has collected information about them. According to Kakalik and Wright (1996), a normal consumer is on more than 100 mailing lists and at least 50 databases. The variety of information collected on consumers via cookies can be gainfully utilized or can be misused by bombarding people with advertising (Buckler 1998).

Are the consumers really bothered by it? - Consumers' privacy concerns are likely to increase as they become aware that marketers have somehow obtained information about them without their awareness or permission (Cespedes and Smith 1993). Studies have shown that fear and distrust regarding the loss of personal privacy associated with the emerging electronic commerce marketplace has been identified as the most crucial issue that Internet consumers face (Wang et al 1998). A survey of 10,000 Web users conducted by the Georgia Institute of Technology concludes that "Privacy now overshadows censorship as the No. 1 most important issue facing the Internet" (Machlis 1997). A study by CommerceNet also shows that privacy is online consumers' biggest concern (Tweney 1998). A survey undertaken by Equifax and Harris Associates determined that over two-thirds of Internet consumers considered the privacy concern to be very important Kakalik and Wright 1996). Of Internet users 81 percent and of people who buy products and services on the Internet 79 percent are concerned about threats to their personal privacy according to a Price Waterhouse survey (Merrick 1998; Joachim 1998).

Nemati *et al* showed that knowledge about data collection can have negative influence on the customer's trust and confidence level online. If the consumers are made aware about the policies which let the corporations collect the personal information about the users, their willingness to share the information reduces. This decrease was more prominent in the case of more educated people. If collecting data reduces consumers trust in the firms, which is leading to decrease in business, then a question arises- What can the companies do to collect the data and not lose the trust of the consumers?

On the other hand, Gillmor (1998) points out that the fundamental problem in Internet privacy is not the disclosure of sensitive information by itself. People will not object to companies gathering and analyzing data about their consumers with the intent of serving their consumers better. As long as the consumers give that information voluntarily and are made fully aware as to how it is going to be used, their privacy is not being violated. The concern is, when that information is merged with several other databases owned by companies other than the one they are doing business with (Gillmor 1998), and then the consumer totally loses control over how that information is being used. If information is used only for the purpose of the original transaction, consumers tend to be unconcerned about privacy. However, if marketers use information beyond the original transaction, consumers become increasingly concerned with privacy (Cranor 1998; Foxman and Kilcoyne 1998; Goodwin 1991).

One must ponder what actually happens when companies collect the information? – E-commerce is weighted on the scale of perceived risks versus the perceived benefits to the consumers. The perceived benefits include economic benefits, ease of use, ease of comparison etc whereas the perceived risks include perceived security, and perceived privacy.

In a survey conducted by AT&T Research Labs they found that 87% of their respondents felt that tracking web sites people visit and using the information collected improperly was very serious (Ackerman, 1999). The study also revealed that 52% of respondents were concerned about cookies, but another 12% were unaware of what a cookie is. "The security of personal data and subsequent misuse or wrongful use without prior permission of an individual raise privacy concerns and often end up in questioning the intent behind collecting private information in the first place" (Gurpreet, 2001). The most crucial factor that internet users have identified is fear and distrust regarding to loss of personal privacy in the e-commerce markets (Wang et al 1998). When the perceived risks outweigh the perceived benefits, consumers may think twice before dealing in an online environment.

The issues that arise between the collection and use of consumer's personal information have been studied. Empirical evidence has been provided to show that companies can gain competitive advantage by behaving ethically, i.e. by letting users know what information they will collect, how they will collect, and for what purposes they will use that information (Culnan 1999). But it's a human tendency to believe what he sees on his own. We take a different approach to solve the issues arising between the collection and use of the data. This research work proposes that if consumers, along with the opt in or opt out option, are given the access to the company database, such that they can edit, delete, or restrict the use of all or any part of the data, the consumer's trust and confidence in privacy & confidentiality will increase.

CONCEPTUALIZING TRUST

Several social disciplines, including, social psychology, marketing, economics, organizational behavior have studied trust. Mayer et al defined trust as "the willingness of a party [trustor] to be vulnerable to the actions of another party [trustee] based on the expectation that the other [trustee] will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party [trustee]" (Mayer et al 1995). This definition well suits the consumers' concerns of privacy. When companies use consumer's personal information (vulnerable act), the consumer's trust in that particular firm tends to decrease.

Many researchers have studied trust and privacy concerns. But most of the studies, so far conducted, have treated privacy and trust as two separate issues. In our model we propose information privacy are deeply related to trust in a company and are antecedent for trust. Although it cannot be denied that initial trust is required for customers to provide their private information. But once the information has been provided, it is the level to which their information is kept private controls their trust in the company. That is, when a customer initially trusts a company, he feels secure in providing his private information. "Developmentally, relationship between parties who have had no prior association is expected to emerge incrementally and to begin with small actions that initially require little reliance on trust" (Jarvenpaa et al, 2000). But more importantly, the trust of the consumer in that company increases if the same company keeps that private information private. In other words, trust as an antecedent to privacy is just a catalyst to the whole process of trust relationship. But the privacy concern acts as an antecedent for the entire relationship afterwards.

The required initial trust can originate form four studied antecedents – characteristic based, process based, institution based, and economic incentive based.

Characteristic based trust

Characteristic oriented (personality oriented), refers to a consumer's personality traits. It is defined as consumer's propensity or consumer's disposition to trust. These traits are stable within-party factors (Cheung and Lee 2003) that lead to generalized expectations about trustworthiness, which is a consumer-specific (Kim et al 2003). Since consumers have different cultural backgrounds, personality types, and developmental experiences, they differ in their inherent propensity to trust (Hofstede 1980, Gefen 2000). In other words, some people trust almost everybody and some trust almost nobody. Consumers that trust more will be more willing to provide their information for the first time, whereas the customers that do not trust anybody will be very reluctant in providing their personal information.

Process/ Familiarity based trust

This portion of trust develops from the experience, in other words, familiarity with the other companies (not the one in question). Customer's prior experiences govern this trust process. If the customer had a good experience with the other companies and their privacy policies, then it lead the consumer to create concrete ideas of future expectations (Kim et al 2003). Such expectations lead consumers to trust the companies in providing their private information.

Institution based trust

Pavlou et al described two dimensions of institution based trust as– Third party institution based trust and Bilateral institutionalized trust. Third party institution based trust refers to the presence of a third party's assurance among the two dealing party's. Bilateral institutionalized trust is defined as 'the subjective belief or confidence that there are fair, stable, and predictable shared routines, processes, and norms to enable successful transactions' (Dyer 2000).

Economic Incentive based trust

In e-commerce field, despite of so many involved risks in e-commerce privacy issues, consumers still provide their privacy information to the companies. As consumer finds low price goods/services of comparable quality, the perceived economic gain leads consumers to share their information. A group based in Singapore is currently working on studying the monetary value at which the consumers are willing to share their private information.

Trust has been proposed as a precursor to a potential consumer's willingness to make online purchases (Jarvenpaa 2000). Cheung and Lee proposed that an Internet user perceives privacy control as the ability of Internet vendors in protecting user's personal information collected during its electronic transactions from unauthorized use or disclosure and they also proved that the perceived privacy control of an Internet vendor positively affects the consumer's trust in Internet shopping (Cheung and Lee 2000). Hoffman et al argues that the lack of consumer's trust in e-commerce is engendered primarily by the industry's documented failure to respond satisfactorily to mounting consumers' concerns over the information privacy in electronic, networked world (Hoffman 1999). McGraw III (1999) noticed that if consumers trust that the personal information remains private, they will flock to e-commerce in droves.

CONCEPTUALIZING INFORMATION PRIVACY CONCERN

Various studies (Stone and Stone 1990, Smith et all 1996, Cespedes and Smith 1993) revealed several dimensions of individuals' concern about organizational information privacy practices: collection, errors, secondary use/ improper access to the information, unauthorized access.

Collection

"Individuals often perceive that great quantities of data regarding their personalities, background, and actions are being accumulated, and they often resent it" (Smith et al 1996). So what data is collected about the consumer is a big concern to the consumer. Who is collecting data, what data are they collecting, how are they collecting data, and who will use this collected data are the few of the concerns that consumers are worried about.

Errors

Concern that protections against deliberate (e.g. a disgruntled employee maliciously falsifies the data) and accidental errors in personal data are inadequate. What if they put wrong data about me, what if that wrong data becomes the reason for the denial of my loan application becomes the major concerns for consumers.

Secondary use

In literature, secondary use has been divided into internal and external secondary use. Internal secondary use is referred to as when the collected data is used for another purpose, without the user's authorization, than it was intended to be used for. External secondary use is referred to as when the collected data is shared with some other third party. The most commonly cited examples of this concern are the usage of collected data for marketing purposes whereas the original intent for that data was to be used for research purposes, sale of consumer personally identifiable data, including names, addresses, purchasing histories.

Unauthorized access

It refers to a concern about who accesses the collected data. Even within an organization who is allowed to access the user's data. For example, in a hospital, is it only the doctor who is supposed to have the access to the data or can other doctors and staff members also accesses the healthcare data of the patients.

Control of unauthorized access, which becomes more of a security issue than an information privacy issue, cannot be handled by users. It needs to be seriously undertaken by legal and governmental involvement. Other three concerns to a certain extent can be handled by users' involvement. Next sections talk about this type of users involvement needed to alleviate the privacy concerns.

RESEARCH MODEL

This paper proposes a theoretical model incorporating information privacy concerns and consumers' options and rights as the two antecedents for trust in an organization. We posit that by providing the users with choice and access to the information collected about them, an organization can help reduce the tensions that arise due to consumer's information privacy concerns while increasing the trust in that organization, which is a critical factor in stimulating purchases over internet, especially at this early stage of commercial development (Quelch and Klein 1996). Figure 1 summarizes the proposed model in which information privacy concerns and consumer empowerment are viewed as the two antecedents in company trust.

Smith (2001) provided a comparison on the privacy concerns among US and Europe. In that study, he came up with a 2x2 grid with level of governmental involvement in corporate privacy management and extensiveness of data subjects' rights as two the dimensions of the grid. He postulated that US fits in the lower left corner of the grid compared to Europe, which is placed in upper right corner. In other terms, companies in Europe have higher governmental involvement in privacy management and higher extensiveness of data subjects' rights. In this proposed model, by providing choice and access rights to consumers, companies can move towards right on the grid axis, i.e., higher on data subjects' rights. This leads to a decrease in consumer's concerns about privacy which in turn improves consumer's trust in a company.

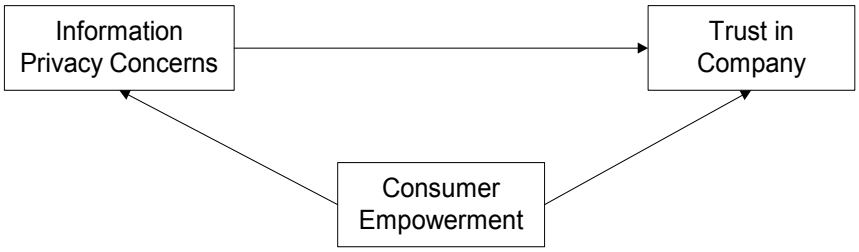

Figure 1. The Theoretical model of consumer empowerment and its impact on information privacy concerns and trust

Consumer Empowerment

Consumer empowerment is achieved by giving customers the options and the rights to control the nature and content of data collected about them. The Federal Trade Commission has also identified five core principles to guide online content providers' development of privacy policy and provide specific instructions as to how online businesses should act to increase online commerce (Sheehan and Hoy 2000; Gillin 2000). These five core principles are

1. Notice: Online consumers should be given notice of an entity's information practices.
2. Choice: Consumers should be given choice with respect to the use and dissemination of information collected from or about them.
3. Access: Consumers should be given access to information about them collected and stored by an entity.
4. Security: Data collectors should take appropriate steps to ensure the security and integrity of information collected.
5. Redress: Enforcement mechanisms, through self-regulation, government regulation, or other means, should be available to ensure compliance

In a recent survey conducted by FTC showed that most websites collect a vast amount of personal information from and about consumers. The results showed that 97% of sites collect email address or other personal information. However, to a great consumer surprise to consumers, only 20% implement the mentioned fair information practice principle. Unfortunately, these numbers are even higher when considering only the most popular websites (2000).

In our study, we concentrate on Choice and Access to consumers as a solution to problem of privacy concerns. Out of the five suggested core principles, choice and access are the issues that can have a direct involvement of the consumers. Security, notice and redress are considered out of the scope of this study. As security and notice principles relate primarily to the company side and redress relates to the required governmental actions. Although these three principles are equally required but our study is focused on the issues in which consumers have a direct dealing.

Choice to Consumers

We suggest that U.S. companies should at least provide an opt-out option. Under this approach, unless the consumer takes an overt action of opting out, it is assumed that the consumer assented to the use of information collected upon him. By providing this option, it at least provides consumer's a right not to be a part of companies' databases. It means that when a consumer requests to be removed from the database, e.g. mass e-mail lists, companies must delete their e-mail addresses and not send them any further messages or face penalties. Now days, many companies are doing so.

To make this process more strong, we suggest that U.S. companies should follow European Union norms. EU has established the opt-in approach to handle this situation. Under this approach, a company cannot assume that the lack of consumer's

objection to the use of information implies consent to use the information. Smith (2001) mentioned that 83% of respondents in a survey conducted in 1996 said that there should be an opt-in procedure for mailing lists.

By this time, an old consumer probably exists in a company's database. The opt-out option can be the only possible solution for already consumers. Whereas for new consumers (new to a certain company database), opt-in approach will provide the best way for not to enter into company's database

Access Rights to Consumers

The Fair Credit Reporting Act of 1970 gives consumers the right to inspect their credit records to find out why they were turned down for a loan or mortgage. However, no such right exists with regard to on-line profiles.

We suggest that if the users are provided with a complete access to the data that has been collected over them. By Access we mean, the complete rights to inspect the collected data, edit the collected (erroneous) data (and not falsifying the data), withhold the permission for the use of all or any particular data, then the consumer's information privacy concerns will reduce considerably. This would keep consumers from being hounded by marketers about products of no interest to them. While there may be some difficulty in doing this, because the information a Web site collects is often strewn among multiple databases, experts suggest that the same kinds of tools these sites use to track consumers could be used to provide at least a partial window into the information that makes up an on-line profile (Green, et al., 2000).

CONCLUSIONS

We expect this study to contribute in understanding the antecedents of trust, which is the trunk of the e-commerce tree, in a company. This study is expected to suggest the ways for the companies such that they can collect data on the consumers and not lose their trust. An empirical study by Culnan and Armstrong (1999) suggests that companies can gain business advantage through customer retention by observing procedural fairness. Therefore by providing consumers with an option and access to their private information companies can gain the trust of the consumers.

REFERENCES

1. Buckler, G. (1998) Web sites often put the bite on Net cookies, *Computer Dealer News*, 14, 39
2. Cespedes, F. V. and Smith, H. J. (1993) Database Marketing: New Rules for Policy and Practice, *Sloan Management Review*, 34, Summer
3. Cheung, C. and M. Lee (2000) Trust in Internet Shopping: A Proposed Model and Measurement Instrument, *Proceedings of the 2000 America's Conference on Information Systems (AMCIS),* 681-689
4. Cranor, L. F., Reagle, J., and Ackerman, M. S. (1999), Beyond Concern: Understanding Net Users' Attitudes about Online Privacy, AT&T Labs-Research Technical Report TR 99.4.3, [available at http:1/www.research.att.com/library/].
5. Culnan, M. J. and Armstrong, P. K (1999) Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation, *Organization Science*, 10, 1
6. Dyer, J.H. (2000) Collaborative Advantage: Wining Through Extended Enterprise Supplier Networks. Oxford, NY: Oxford University Press.
7. Foxman, E. R. and Kilcoyne, P. (1993) Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues, *Journal of Public Policy & Marketing*, 12, Spring
8. Gillin, D. (2000) How privacy affects us all, *Marketing research*, Summer
9. Gillmor, D. (1998) Violating privacy is bad business, *Computerworld*, 32, 12
10. Goodwin, C. (1991) Privacy: Recognition of a Consumer Right, *Journal of Public Policy & Marketing*, 10, Spring
11. Hemphill, T. (2002) Electronic commerce and Consumer Privacy: Establishing Online Trust in the U.S. Digital Economy, *Business and Society Review*, 107, 2, 221-239
12. Hoffman, D. L., Nowak, T. P. and Peralta, M. A. (1999) Information privacy in the marketspace: Implications for the commercial uses of anonymity on web, *The Information Society*, 15
13. Jarvenpaa, S. L., Tractinsky, N. and Vitale, M. (2000) Consumer Trust in an Internet Store, *Information Technology and Management,* 1
14. Joachim, D. (1998) Internet privacy laws: Hot Capitol Hill topic, *Internetweek*, 721

15. Kakalik, J. S. and Wright, M. S. (1996) Responding to privacy concerns of consumers, *Review of Business*, 18(1) 15-18
16. Machlis, S. (1997) Web sites rush to self-regulate, *Computerworld*, 32, 19
17. Mayer, R. C., Davis J. H. and Schoorman, F.D. (1995) An integrative model of organizational trust, *Academy of Management Review*, 20, 3
18. Merrick, B. (1998) Privacy concerns slow growth of online banking, *Credit Union Magazine*, 64, 11
19. Nemati, H., Tao, W., Gold, J. Understanding tradeoffs: The link between knowledge and privacy concerns
20. Sheehan, K. B. and Hoy, M. G. (2000) Dimensions of Privacy Concern Among Online Consumer, *Journal of Public Policy and Marketing*, Spring, 19, 1
21. Quelch, J.A. and Klein, L. R. (1996) The internet and international marketing, *Sloan Management Review,* Spring, 60-75
22. Smith, H. J. (1996) Information Privacy: Measuring Individuals' Concerns about Organizational Practices, *MIS Quaterly*, 20,2
23. Smith, J. (2001) Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe?*, California Management Review,* Winter, 43, 2
24. Stewarts, K. A., and Segars, A. H. (2002) An Empirical Examination of the Concern for Information Privacy Instrument, *Information Systems Research,* 13, 1
25. Stone, E. F. and Stone, D. L. (1990) Privacy in Organizations: Theoretical Issues, research Findings, and Protection Mechanisms, *Research in Personnel and Human Management*, 8
26. Tweney, D. (1998) The consumer battle over online information privacy has just begun, *InfoWorld*, 20, 25
27. Wang, H., Lee, M. K. O. and Wang, C. (1998) Consumer privacy concerns about Internet marketing, *Association for Computing Machinery. Communications of the ACM* ,41, 3, 63-70
28. Westin, A. F. (1967) Privacy and Freedom, New York: Atheneum