Effects of Information Privacy Policies on Customers’ Willingness to transact with Online Vendors

Submission Type: Full Papers

Joseph S. Mollick
Texas A&M University – Corpus Christi
joseph.mollick@tamucc.edu

Abstract

Organizations operating in the information age need to refine their understanding of the effects of organizational policies regarding personal information management on customers’ willingness to transact with online vendors. This research employed a 2x2x2 within-subjects experimental design to test the effects of three organizational information management strategy variables on customers’ willingness to transact with online vendors. The three strategy variables presented to customers through privacy policies are: (1) seeking customers’ informed consent, (2) giving customers the ability to limit data sharing, and (3) giving customers the ability to limit secondary use of data. Analyses of data collected from customers support the three hypothesized main effects which are all positive.

Keywords
Privacy policies, Customers, Information, e-commerce

Introduction

Ever since information and communications technology (ICT) started enabling data flows within and between organizations, individuals’ concerns for security and privacy of personal data have been increasing, and companies are facing the challenge of responding to individuals’ information privacy concerns with effective policies and practices. The Internet and the Web have enabled companies to collect data from and about customers, employees and other entities through the use of methods and tools that can be used openly or through secret, covert monitoring of individuals. Web-based businesses have the technological capability to bypass the need to seek individuals’ consent before making them subjects of data collection. Once collected, data about customers can be shared with others within or outside an organization’s boundary for purposes that may or may not have been explicitly authorized by customers. Thus, there is a concern about data collection from or about customers without customers’ informed consent. Moreover, there is a concern about the extent of data sharing from databases and there is a concern that data may be used for unauthorized, secondary purposes. To strategically respond to customers’ concerns about personal information privacy, organizations need to be proactive in formulating and implementing strategies and policies that are perceived by customers as fair and just. The perception that an organization is fair in the way it collects and uses personal information about customers can help build and maintain customers’ trust in online vendors that is necessary to encourage customers to visit a company’s website, safely purchase online, develop loyalty and make referrals to other customers.

Many organizations are combining database and network technologies to implement marketing strategies that depend on the use of customer transaction data that are personal and can pose threats to individual privacy. For example, certain organizational attempts at personalization as part of a relationship marketing program may be perceived by customers as offensive, unfair and contrary to trustworthiness. Fear of threats against information privacy and security has been found to be one of the reasons Internet surfers are afraid of Internet-based exchange of information and monetary transactions.
vendors that depend for their very existence on the combination of databases and networks are interested in finding out how Internet users’ or potential users’ trust can be earned and how surfers can be converted into customers.

The simple thesis underlying this research is the belief that by adopting customer-centered privacy policies, firms that want to transact with customers over the Internet can satisfy customers’ criteria of fairness and qualify for customers’ cooperation in transactional relationship strategies. So, the research question we investigate is do online vendors’ policies regarding management of personal information about customers positively affect customers’ willingness to transact with online vendors?

**Literature review**

**Privacy policies and customers’ willingness to transact with online vendors (Y)**

Organizations and individuals that engage in transactions involving goods, services, money and information have been trying to use the Internet’s virtually limitless potential for members of the global economy. Concern about online vendors’ willingness and ability to secure customers’ personal information privacy has been identified as one of the important challenges facing parties that want to engage in information-intensive transactions online. The belief that an organization is fair in how it handles customers’ personal information can reduce customers’ Internet-anxiety and motivate them to engage in transactions carried out online. A question of trust in and willingness to transact with online vendors includes a question concerning fairness of vendors’ information management policies. Will vendors do what is necessary to protect private information from the hackers and others inside and outside an organization who can harm individual customers?

**Organization theory and organizational policies about information privacy**

In light of a resource-based view of electronic commerce (Barney 1991, Zhuang and Lederer, 2006) it can be argued that information and knowledge about customers is a critical resource for organizations operating in the cyberspace. One of the most important resources that electronic commerce allows organizations to easily collect and use is information about customers and their behavior such as click-stream behavior. Often, this resource is shared with strategic alliance partners and members in the supply chain. However, when organizations do not respect customers’ rights and preferences in the way they collect, store, use, share and disseminate customers’ private information, customers can feel powerless, even violated, and they may cease to cooperate or refuse to engage in transactions with online firms.

The basic proposition behind the three information privacy and security strategy variables in this study is that organizations, in order to win and retain customers, should evaluate the effects of their information privacy policies on customers’ willingness to transact with online vendors. In so doing, an organization can improve its chances of gaining a relationship advantage over competitors who are perceived as less fair and trustworthy and, therefore, less worthy of customers’ transactional patronage. To this end, organizational policy makers can adopt information management policies that empower and respect customers. One way to empower customers is to ask them for their permission or authorization before collecting any information about them. A second way is to allow them to restrict the release, access or sharing of personal information with sub-units, branches, affiliates, alliance partners and others outside an organizational boundary. A third way is to restrict the use of personal information to only the primary purpose that was stated at the time data were collected. The three strategy variables have been collected from prior research about individuals’ information privacy concerns and attitudes as they relate to organizational information privacy practices and policies.

**Policy of seeking individual customers’ consent before data collection (S1)**

Researchers (Smith, Milberg and Burk 1996) identified individuals’ concern about the collection of data as one of the four dimensions of an individual’s information privacy concern. Concern about collection of data can be broken down into two sub-categories: concern about the content of data collected and concern
about the tools, methods and procedures used to collect the data. In the first independent variable of this study, we focus on one aspect of the methods of data collection used by online vendors. This variable relates to methods of information acquisition for competitive intelligence. The variable, informed consent, is based on prior research related to the fairness of methods of data collection. It has been reported (Milne and Culnan 2002) that privacy notices are an important means for reducing customers’ privacy concerns by providing consumers with information about the organization’s information practices. Also, it has been reported that roughly 60% of a sample of consumers said they decided not to use a website or not to purchase something from a website because they were not sure about the collection and use of their personal information (Shepard 2004). Security disclosures and awards from neutral sources were found to enhance cue-based trust which, in turn, positively influenced two behavioral intentions regarding Internet shopping, bookmarking intentions and willingness to provide personal information (Siju, Beatty and Fox 2004). Third party seals of approval were also found to have positive effects on those two behavioral responses. Effects of Internet monitoring on job attitudes can be compared to the effects of online customer surveillance and monitoring on customers’ attitude toward an organization (Alder, Noel and Ambrose, 2006).

Policy of limiting data sharing: within an organization’s boundary (S2)

Much research has been published in the last thirty years that documented individuals’ concern about access to data in organizational computer databases. An important research article identified access control or data sharing as one of the legal and ethical liabilities facing organizations as they computerize different business processes using databases and network tools (Straub and Collins 1991). More recently, another survey research indicated that information security professionals rated access control as their number one objective in securing data (Ma and Pearson 2004). Sandhu and Samarati (1996) found that authentication, access control and auditing together provide the foundation for information and system security. Thus, concern about access to data is shared by professionals and scholars in the domains of information security and privacy management, information ethics and strategy as well as by individuals about whom data are collected and stored by organizations.

It can be said that customers’ concern about data sharing reflects the extent to which they believe that their privacy and security is being compromised or violated because of ignorance, incompetence, negligence, malice or criminal intent on the part of information managers and knowledge workers. Hagel and Singer (1999) examined how consumers’ right to privacy in the United States may be undermined by retailers’ practice of sharing of consumer information and the advent of information technology. A business strategy of deliberately sharing customer data with entities outside an organization’s boundary is likely to negatively impact customers’ perception of an organization’s fairness with regard to privacy protection. Mollick (2006) found that the more concerned students are about access to their records stored in university databases, the more they feel alienated from the university.

Policy concerning secondary use of data about customers (S3)

Privacy is the ability of the individual to control the terms under which personal information is acquired and used (Westin 1967). Concern about unauthorized secondary use of data has been identified as one of the four core dimensions of individuals’ information privacy concerns regarding organizational practices. This dimension of individuals’ information privacy concern can be defined as the fear that information is collected from individuals for one purpose but is used for another, secondary purpose (Linowes 1989). The secondary purpose could be an internal use within a single organization but without authorization from the individuals, or it could be the disclosure of information to an external party other than the collecting organization.

In the online environment, loyalty and reward schemes are one of the tools being used in customer relationship management. Consumers who register as loyalty scheme members allow businesses to record purchase transactions, and thereby grant implicit permission for businesses to use that data in exchange for modest rewards such as enrollment in lotteries. Cookies are software tools used, often covertly, to collect data about individuals using computers connected to the Internet. Terms such as ‘cookies’ that
may remind customers of something sweet may actually refer to monsters (Morse and Morse 2002) that ruin personal privacy because of covert collection and secondary use of personal information. Secondary uses of customer data can easily cross the limits of the contractual agreement, if any such agreement exists, and span into uses from which a company can profit substantially at the expense of customers’ privacy, while customers remain in the dark about the uses of data.

Theoretical integration of the independent variables

One of the theoretical lenses that is relevant to the three privacy strategy variables is Herzberg’s two-factor theory of motivation (Herzberg 1966), which has been used to explain behavioral intentions, especially in the domain of organizational behavior or employees’ motivation to work. Herzberg developed the motivation-hygiene theory to explain human motivation to work. He found that factors causing job satisfaction, which he called motivators, were different from factors causing job dissatisfaction, which he called hygiene factors. The theory can be used to explain individual customers’ motivation to sign up or join an online organization to engage in information intensive transactional relationships. Organizational privacy policy can be viewed as one of the hygiene factors that can determine the level of dissatisfaction a customer develops with any specific firm or with the cyberspace or computer networks and database driven environments in general. This level of dissatisfaction can reduce customers’ motivation to engage in transactions with firms online. Use of spying to collect data from or about customers, secondary use of data, or sharing customer data with entities outside an organization’s boundary can be perceived as poor organizational hygiene, unhealthy and unsafe for customers committed to protect their well being. Customers’ negative attitude toward secondary use of data can be viewed in light of Herzberg’s hygiene factors. Likewise, findings that concerns about collection and secondary use of data directly correlate with students’ feeling of alienation from their university (Mollick and Pearson 2006) can also be viewed in light of Herzberg’s hygiene factors.

Development of the research model and hypotheses

In light of the discussion this far, the research model is presented in Figure 1, and the hypotheses follow. We hypothesize about the main effects of three privacy policy variables on customers’ willingness to transact with online vendors.

Figure 1: The Research Model
Effect of seeking customer consent before data collection (S1) on customers’ willingness to transact with online vendors (Y)

By seeking customers’ permission, authorization or informed consent before subjecting them to data collection, a business empowers customers and presents itself as an entity that respects customers’ free will and autonomy. Right to privacy is the right to control information about oneself (Westin 1967). Control is the key issue. A policy of seeking customers’ permission recognizes and honors the privacy rights of individuals. By seeking customers’ informed consent, an organization that collects data about customers reduces customers’ inequity. It is also probable that by putting in place a policy of seeking informed consent, an organization reduces the risk and uncertainty faced by customers in the face of informational asymmetry (Ackerlof 1970). It can be argued that the power relationship between the data collecting organization and the subjects of data collection is perceived by customers as more in equilibrium or in balance when informed consent is sought as a precondition for subjecting an individual to data collection procedures. Thus, the relationship between an organizational policy of seeking customers’ informed consent and customers’ willingness to transact with online vendors (Y) can be hypothesized as follows.

H1: Vendors with organizational policies that allow customers to authorize or give informed consent to data collection will have a higher average score on customers’ willingness to transact with online vendors (Y).

Effects of a policy of restricting data sharing (S2) on customers’ willingness to transact with online vendors (Y)

Information confers power on those who possess it or can control its flow in a way that enables them to achieve their own goals. Customers are increasingly becoming aware that this power, which can be enormous, unfortunately, can be abused. Consequently, customers expect organizations to make judicious use of information power (Mason, Mason and Culnan 1995). An organizational policy that restricts data sharing to be limited within an organizational boundary is likely to be interpreted by customers as a responsible organization’s attempt to protect customers from abuse of personal information, a judicious use of power.

A policy that restricts data sharing within organizational boundary creates an impression that the company, in its role as a custodian of customers’ personal information, is concerned about procedural fairness and justice. These arguments lead to the following hypothesis:

H2: Vendors with organizational policies that allow customers to control and limit data sharing within an organizational boundary will have higher average score on customers’ willingness to transact with online vendors (Y)

Effects of a policy of restricting secondary use of data (S3) on customers’ willingness to transact with online vendors (Y)

Individuals’ negative attitude toward secondary use of data stems from the fact that if information is given to an entity for one stated purpose, then the providers of the information expect the use of that information to be restricted to that stated purpose. Customers expect to enjoy the benefits of efficient placement and execution of transactions in exchange for sacrificing some personal privacy. Any use of the data for a subsequent purpose violates the contract. The violation of the contract may not always be a legal violation, but it will be a breach of a psychological (Rousseau and Parks, 1992) and social contract (Rousseau, 1947). Unauthorized secondary use of data goes contrary to customers’ expectations and thus contributes to customers’ perception that the vendor who uses data for a secondary purpose deviates from norms of fairness and trustworthiness. In light of the arguments based on breach of social and psychological contracts, the effect of secondary use of data on an organization’s perceived worthiness for customers’ patronage can be hypothesized as follows:
H₃: Vendors with organizational policies that allow customers to restrict an organization’s use of customers’ personal information for secondary purposes will have a higher average score on customers’ willingness to transact with online vendors (Y)

**Research methodology**

In this section, we describe the target population and sample selection, the research procedures, and manipulation of the three independent variables.

**Target population and sample selection**

The target population of interest in this study was defined as individual consumers with at least a high school education, between 19-25 years in age, at least moderately internet-savvy, and with limited experience of carrying out transactions online. As such, the findings of this study should be more useful for online firms interested in obtaining new customers at an early stage of their professional life.

As a representative of the target population, a sample of eighty-four students enrolled in the College of Business at a large, public university in the southern USA were chosen to participate in the research. Subjects were enrolled in different courses and were given the chance to earn extra credit points for the class in exchange for their participation. All subjects had completed at least one introductory level course in Management Information Systems and were familiar with computers, the Internet and e-commerce.

**Procedures**

The 84 subjects participated in a repeated measures design. Subjects participated in the experiment in a 35-person computer lab; accordingly, subjects were randomly assigned to participate at different times since the lab was unable to accommodate all subjects at once. The treatment order assigned to each subject was randomized to equally distribute and neutralize order effects.

The three privacy policy factors concerning seeking customers’ informed consent before data collection (S1), limiting data sharing within an organizational boundary (S2) and limiting unauthorized secondary use of data (S3) produced eight factor level combinations or cells which represented eight hypothetical organizations. Privacy policy characteristics of these eight hypothetical organizations are summarized in Table 1. Each of the eight hypothetical organizations represented by a website were presented to study participants as being identical with regard to all other aspects that might influence customers’ willingness to transact with online vendors (Y). Table 1 presents the eight combinations for the three independent privacy policy variables. In Table 1 “Y” is yes; “N” is no for the strategy variable.

<table>
<thead>
<tr>
<th>Strategy Variable/ Websites</th>
<th>DotCom1</th>
<th>DotCom2</th>
<th>DotCom3</th>
<th>DotCom4</th>
<th>DotCom5</th>
<th>DotCom6</th>
<th>DotCom7</th>
<th>DotCom8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Informed Consent?</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Limit Sharing of Customer Data?</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Limit Secondary Use of Data?</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Table 1: Combinations of privacy policy variables within the eight DotCom websites
Results

Results of testing hypotheses, statistical significance and power

Testing hypothesized effects involves comparing the means of the dependent variable at different levels of the independent variables. The mean scores on customers’ willingness to transact for the eight hypothetical DotComs, defined with three privacy policy variables in Table 1, are presented in Figure 2.

![Figure 2: Mean 'Willingness to Transact' scores for eight hypothetical DotComs](image)

Table 2 provides summary results showing that each of the beta coefficients is found to be statistically significant with p-values less than .001, which support H1, H2 and H3.

<table>
<thead>
<tr>
<th>Regression Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple R</td>
</tr>
<tr>
<td>R Square</td>
</tr>
<tr>
<td>Adjusted R Square</td>
</tr>
<tr>
<td>Standard Error</td>
</tr>
<tr>
<td>Observations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ANOVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>df</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Regression</td>
</tr>
<tr>
<td>Residual</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coefficients</th>
<th>Standard Error</th>
<th>t Stat</th>
<th>P-value</th>
<th>Lower 95%</th>
<th>Upper 95%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>1.1967</td>
<td>0.0816</td>
<td>0.0000</td>
<td>1.0758</td>
<td>1.3176</td>
</tr>
<tr>
<td>S1</td>
<td>0.6142</td>
<td>0.0816</td>
<td>9.9761</td>
<td>0.0000</td>
<td>0.4933</td>
</tr>
<tr>
<td>S2</td>
<td>0.6082</td>
<td>0.0816</td>
<td>9.8795</td>
<td>0.0000</td>
<td>0.4873</td>
</tr>
<tr>
<td>S3</td>
<td>0.5087</td>
<td>0.0816</td>
<td>8.2822</td>
<td>0.0000</td>
<td>0.3878</td>
</tr>
</tbody>
</table>

Table 2: Regression Results for Tests of Hypotheses
Each of the three hypotheses has been supported with more than 99% confidence and the statistical power associated with tests of each of the main effects is more than .999. Thus, the evidence is overwhelmingly strong to support each of the three hypothesized main effects.

Conclusion

The findings of the study add to the body of knowledge about the determinants of customers’ willingness to transact with online vendors that embody different privacy policies and related practices. The confirmatory approach implemented through the experimental study using a within-subjects design helps establish a higher degree of confidence in some beliefs and previous findings concerning the effects of organizational information privacy policies on customers’ willingness to transact with online vendors.

REFERENCES

Herzberg, F. Work and the nature of man,T. Y. Crowell, New York