

Would Regulation of Web Site Privacy Policy Statements Increase Consumer Trust?

David B. Meinert and Dane K. Peterson
Missouri State University, Springfield, Missouri USA

davidmeinert@missouristate.edu danepeterson@missouristate.edu

John R. Criswell II
Shelter Insurance. Columbia,
Missouri USA

jrcriswell@ccis.edu

Martin D. Crossland
Oklahoma State University,
Tulsa, Oklahoma USA

martin.crossland@okstate.edu

Abstract

Proponents of e-commerce have known for some time that limited participation by consumers partially reflects their concern over the privacy of personal information. To address consumer concerns, web site operators have employed security mechanisms, including privacy policy statements to increase their perceived trustworthiness. While empirical evidence is limited, there is some question regarding the ability of privacy policy statements to engender significantly greater levels of trust. The limited effectiveness of such statements may reflect their voluntary implementation, self-enforcement, and/or significant variance (protection and enforcement) from one web site to another. One possible remedy would be the imposition of legally mandated statements. This study examined the efficacy of legally mandated privacy policies vis-à-vis both voluntary statements of varying degrees of protection and the absence of any such statement. The results were mixed, as legally mandated privacy policy statements were found to be comparable to strong voluntary statements, but superior to none, weak or moderate policies. Perhaps more important, the nature of the privacy policy statement interacted with type of information requested.

Keywords: e-commerce privacy; electronic commerce trust; Internet privacy; Internet trust; online privacy; privacy policy statements

Introduction

The past decade has witnessed rapid growth in e-commerce, particularly with respect to business-

Material published as part of this publication, either on-line or in print, is copyrighted by the Informing Science Institute. Permission to make digital or paper copy of part or all of these works for personal or classroom use is granted without fee provided that the copies are not made or distributed for profit or commercial advantage AND that copies 1) bear this notice in full and 2) give the full citation on the first page. It is permissible to abstract these works so long as credit is given. To copy in all other cases or to republish or to post on a server or to redistribute to lists requires specific permission and payment of a fee. Contact Publisher@InformingScience.org to request redistribution permission.

to-consumer (B2C) transactions. Both established and new vendors have sought to leverage the diffusion of the Internet to expand their markets. The Internet has allowed established firms to expand their marketplace, but at the same time it has eliminated many of the traditional barriers of entry for new entrants to compete for these same consumers. Consumers once accustomed to limited and known vendors are now af-

forded more choices, but are often concerned about privacy and trust as many of the vendors are “unknowns” (Pennington, Wilcox & Grover, 2003). Given that consumers are now presented with vendors with whom they have little or no familiarity it comes as no surprise that recent research on e-commerce has found that privacy and trust issues are a key determinant in whether consumers’ engage in on-line transactions (Hoffman, Novak, & Peralta 1999).

Recognizing that privacy and trust of the vendor is a critical antecedent to increased participation in B2C e-commerce, researchers have examined several “trust mechanisms” employed by vendors to enhance consumer trust and concomitantly their predisposition to purchase on-line. One mechanism that has garnered considerable interest are privacy policy statements, voluntary, self-reported statements displayed on web sites that convey established policies for the use and distribution of personal information.

Use of privacy policy statements to increase perceived trustworthiness is a relatively new phenomenon, and examination of their use and implications is just beginning to be explored (Criswell & Meinert, 2003; Culnan, 1999; Grewal, Munger, Iyer, & Levy, 2003; Liu & Arnett, 2002; Luo & Najdawi, 2004; Meinert, Peterson, Criswell & Crossland, 2006; Miyazaki & Fernandez, 2000; Pennington et al., 2003; Ranganathan & Ganapathy, 2002). While much of the research to date on this topic has focused on chronicling rates of utilization and variability in content, a few studies have examined the efficacy of privacy statements. Pennington, Wilcox and Grover (2003) found evidence via an experimental design that self-reported guarantees can influence system trust and indirectly influence consumer purchase intentions. In an exploratory study, Criswell and Meinert (2003) found that self-reported privacy policy statements increased consumer willingness to provide personal information on-line. That study and a more comprehensive study by Meinert, Peterson, Criswell and Crossland (2006) also affirmed that not only the presence, but the strength, or level of protection guaranteed by the privacy policy statement influences consumer trust as measured by willingness to provide personal information on-line. These results, while preliminary, seem to suggest that voluntary privacy policy statements have a positive, but relatively limited impact on consumer trust. Only a strong privacy policy statement was found to induce a willingness to provide contact, biographical and financial information and in each case respondents were only “slightly likely”. It should be further noted that respondents in these studies were required to read the description of the privacy policy statements. In many instances, potential customers may not read any policies regarding the web site’s stated privacy standards.

Given the widespread use of privacy policy statements it’s somewhat surprising to find that they have minimal impact on consumer trust. Determining whether the effectiveness of privacy policy statements can be improved would contribute to the knowledge and understanding of what, if any, role they can play in influencing consumer trust of on-line vendors. While the literature offers no insight into why such statements are ineffective, one plausible explanation is that consumers place little faith in privacy policies that lack regulatory oversight. The aim of this exploratory study was to examine whether legally mandated web site privacy policies would be more effective than either no policy or voluntary policies affording varying degrees of protection. This study was intended to provide a preliminary understanding of the extent to which regulation of privacy standards might increase the efficacy of web site privacy policy statements in order to increase consumer trust. As an exploratory study, four specific research questions were examined:

- How willing are consumers to provide various types of information via the Internet when a legally mandated privacy policy is in place?
- Are legally mandated privacy policy statements more effective in engendering trust than either no policy or voluntary policies affording varying degrees of protection?
- Are consumers generally aware of privacy policy statements?

- Are consumers reading privacy policy statements?

By addressing these questions, this study aims to contribute to the body of knowledge related to web site privacy policy statements. The findings should be of interest to practitioners, public policy makers and academicians. The findings provide additional insight into the influence of alternative forms of privacy policy statements and the extent to which regulatory oversight might influence consumer behavior.

To address these research questions, this article reports the results of a survey designed to measure the impact of both voluntary/self-regulated and legally mandated privacy policy statements. First, the article examines related research to develop a basis for this investigation. This literature review necessarily examines findings related to consumer trust and its role in e-commerce and methods employed to increase consumer trust. Likewise the review explores both the protection provided by privacy policy statements and the types of information typically requested by web sites. The literature review concludes with a brief description of existing federal privacy standards that may influence consumer perceptions and/or expectations regarding the government's role in privacy protection. Next, the purpose of the study is outlined in the context of the literature review. This is followed by a methods section that describes the data collection, sample, and results. Following a discussion of the results, limitations of the study and opportunities for future research are addressed. The article concludes with a brief summary of the implications of the study.

Literature Review

An antecedent to virtually all business transactions is consumer trust. When consumers feel vulnerable or at risk they are generally hesitant or unwilling to place orders or provide personal information. Recognizing the importance of consumer trust, individual organizations, industries and public policy makers have sought to identify and implement mechanisms to reduce perceived risks. While concern about consumer trust in e-commerce is a relatively new phenomenon, there are four categories of literature that provide a foundation for this study. The first explores the general basis for trust and its role in e-commerce models. The second chronicles methods for increasing consumer trust. The third examines the strength of privacy policy statements (i.e., level of protection afforded) and the nature of information collected via the web site. The fourth and final category pertains to existing federal privacy standards that demonstrate the viability of legally mandated privacy policies for web sites.

Consumer Trust and its Role in E-Commerce

Numerous studies have demonstrated that many potential customers are reluctant to engage in e-commerce transactions because of concerns about providing personal information through the Internet (Kolsaker & Payne, 2002; Miyazaki & Fernandez, 2001; Suh & Han, 2003). It has been estimated that \$15 billion in e-commerce revenues for 2001 were unrealized due to a lack of consumer trust in either the ability or the intent of web merchants to ensure that personal information would only be used in an acceptable manner (Sipior, Ward, & Rongione, 2004).

Definition of trust

A number of definitions of trust have been suggested specifically with regards to e-commerce (e.g., Gefen, 2002; Lee & Turban, 2001; McKnight & Chervany, 2001). Most of the definitions of trust proposed within the realm of e-commerce share a number of common elements. For example, trust has been defined as a consumer's willingness to rely on the seller and take action in circumstances where such action makes the consumer vulnerable to the seller (Jarvenpaa, Tractinsky, Saarinen & Vitale, 1999). As in most definitions of trust there is an element of risk associ-

ated with the information submitted through the Internet. Consumers are vulnerable because they are dependent on web merchants to use information in an acceptable manner. The definition also implies that consumers make their own subjective assessment of the risks involved in a particular e-commerce transaction. Finally, a consumer's actions are assumed to be the result of a rational decision making process.

Models of consumer trust in e-commerce

A variety of models on consumer trust in e-commerce have recently been proposed (Jarvenpaa, et al., 1999; Lee & Turban, 2001; Limayem, Khalifa, & Frini, 2000; Liu, Marchewka, & Ku, 2004; McKnight & Chervany, 2001; Suh & Han, 2003; Tan & Thoen, 2001). For the most part, these models share a number of common elements. For example, most models recognize that individual differences among consumers play a vital role in e-commerce trust. In general, consumers are assumed to differ in terms of their propensity to trust or their disposition to trust (Lee & Turban, 2001; McKnight & Chervany, 2001). The disposition or propensity to trust is likely influenced by consumers' awareness of Internet fraud and their past experiences regarding both the Internet and other situations involving risk. In addition to past experiences, individual differences in the willingness to engage in e-commerce transactions could also be the result of inherent differences in the inclination of individuals to take risks, such as a tendency to be risk averse or a risk seeker (Tan, 1999; Tan & Thoen, 2001).

The assumption that individuals differ in terms of their trust in e-commerce is supported by studies demonstrating individual differences with respect to gender (Kolsaker & Payne, 2002), amount of experience with the Internet (Corbitt, Thanasankit, & Han, 2003; Miyazaki & Fernandez, 2001), and cultural background (Jarvenpaa et al. 1999; Liu et al., 2004). In an attempt to examine the extent of individual differences, Sheehan (2002) developed a four category typology based on concerns about submitting personal information to web sites. This study, based on 889 responses to an e-mail survey, indicated that only a small percentage of individuals could be classified in the extreme groups, "unconcerned" (16%) and "alarmed" (3%). The majority of individuals were classified in the middle two categories, "circumspect" (38%) and "wary" (43%). These results seem to imply that most individuals do not already have strong preconceived notions about the level of risk involved in providing personal information to web sites. Rather the results suggest that the specific attributes of a given web site or web merchant is likely to influence the decisions of most potential customers.

Another component that is common to most models on e-commerce trust is trust in the Internet system (Lee & Turban, 2001; McKnight & Chervany, 2001). It has been proposed that consumer trust in the Internet system is influenced by the perceived technical competence of the system, perceived performance level of the system, and the degree to which the consumer understands the Internet system (Lee & Turban, 2001). These perceptions of the trustworthiness of the Internet system are likely to be highly influenced by media reports. For instance, one frequently reported study conducted jointly by the Computer Security Institute and the FBI estimated the cost of system penetration by outsiders at over seven billion dollars annually (cited in Tribunella, 2002).

The third and most investigated component of most models on e-commerce trust is trust in the web merchant. Studies have shown that the size and reputation of a web merchant greatly influences consumer trust (Jarvenpaa, et al. 1999). It has also been demonstrated that the perceived ability, integrity, and benevolence of a web merchant influences consumer trust (Lee & Turban, 2001). This finding emphasizes that web merchants must not only have good intentions, but also the perceived ability to protect personal information. Strength of authentication, nonrepudiation, confidentiality, privacy protection, and data integrity all have an impact consumer trust in Internet Banking (Suh & Han, 2003).

Methods for Increasing Consumer Trust

To gain consumer trust, web merchants must convince potential consumers that personal information obtained through e-commerce transactions will remain secure. To this end, web merchants have employed a variety of security mechanisms to increase their perceived trustworthiness. These methods include seals of approval or third party certifications, quality and normalcy of web site design, ratings or customer testimonials, endorsements by reference groups, and money-back guarantees (Ba & Pavlou, 2002; Corbitt et al. 2003; Grewal et al. 2003; Lee & Turban, 2001; Liu et al. 2004; Pennington et al. 2003; Ranganathan & Ganapathy, 2002; Suh & Han, 2003; Tan, 1999).

Since the effectiveness of these procedures has been reviewed in previous articles, a detailed review will not be presented in this paper (Liu & Arnett, 2000; Ngai & Wat, 2002). Briefly, the results of these studies have provided positive support for the inclusion of many security mechanism, including money back guarantees, warranties, partnerships with established organizations (Corbitt et al. 2003; Grewal et al. 2003), non-online methods of payment (Ranganathan & Ganapathy, 2002) privacy protection guarantees, nonrepudiation (Suh & Han, 2003), approval from reference groups and warranties (Tan, 1999). However, seals, ratings (Pennington et al. 2003) and third party endorsements (Lee & Turban, 2001) have not been found to significantly increase consumer trust.

One of the most widely used security mechanisms by web merchants is a self-reported guarantee or a privacy policy statement. A privacy policy statement is a contractual commitment to consumers outlining how their personal information will be treated. Privacy policy statements represent one of the simpler and less expensive methods of increasing consumer confidence, which may account for their widespread use. The evidence suggests that posting a self-reported guarantee of compliance with e-commerce standards is an effective means of increasing consumer trust (Pennington et al., 2003; Ranganathan & Ganapathy, 2002). Privacy policy statements appear to be most beneficial to the web merchants that have the greatest need to increase consumer trust (Grewal et al., 2003). That is, privacy policy statements were found to be much more useful for web merchants that lacked name recognition than those with an established reputation.

Privacy Policy Statements

Previous research has examined various aspects of privacy policy statements including: levels of protection, enforcement, and interaction with information types.

Levels of protection

Studies examining the content of web sites have found a remarkable amount of variability in the nature and types of privacy policy statements (Liu & Arnett, 2002; Luo & Najdawi, 2004; Miyazaki & Fernandez, 2000). These studies have reported that privacy policy statements vary in terms of their placement, length, and ease of reading. Most importantly, the statements vary in terms of the level of protection guaranteed (Liu & Arnett, 2002). Some privacy policy statements are highly restrictive while others offer no real assurance of privacy. An example of a highly restrictive privacy policy statement might include a statement such as: "Under no circumstances will any information you provide to us over the Internet be released to any third party for any reason whatsoever" (4321net, 2002).

A less restrictive privacy policy statement might include language similar to the following excerpt from the Sun Microsystems privacy policy statement, "If you choose to provide us with your Personal Information on the web, we may transfer that information, within Sun or to Sun's third party service providers, across borders and from your country or jurisdiction to other countries or jurisdictions around the world" (Sun Microsystems, 2001).

A third and least restrictive level of privacy statement does not provide any protection of personal information. In this scenario, the term privacy policy statement is a misnomer as the statement simply indicates that it is the intention of the web merchant to share information collected on individuals with other organizations. Thus, these types of statements serve primarily as a means of protecting the web site with respect to liability issues, as it is the intent of the web site to share information on customers with other sources.

Enforcement. Differences in web site privacy policy statements are not limited to the level of protection afforded as enforcement also varies. Enforcement generally falls into three categories: self-regulation, third-party validation/audits and regulatory oversight. Although the Federal Trade Commission has been concerned about on-line privacy for some time they have “actively supported self-regulation” (Federal Trade Commission, 2000, p. 20). Hence, the absence of any reference to third party or regulatory oversight in a privacy policy implies self-enforcement. To address consumer concerns related to self-regulation, third-party seal programs have been developed (Liu and Arnett, 2002). Seal programs such as TRUSTe, BBBOnline (Better Business Bureau Online Seal), MutiCheck and WebTrust (offered by American Institute of CPAs) allow licensees who abide by posted privacy policies and/or allow compliance monitoring to display the granting organizations seal of approval on their web site. Privacy seals are intended to provide a simple means for addressing consumer privacy concerns. The standards for achieving certification vary and at present there are no fewer than nine services offering seal programs (Higgins, 1998). The least common form of enforcement is regulatory, which reflects in large part the federal government’s attempts to rely on self-regulation rather than legal standards. Laws and regulations at both the state and federal level in the United States have been enacted to establish privacy standards for web sites operated by the government. For example, policy set forth by the White House Office of Management and Budget requires federal government web sites to post privacy statements and eliminate the use of covert methods of collecting information, such as cookies (Swire et al., 1999). On a broader scale, laws have been enacted that apply to all web sites, private or public such as the Children’s Online Privacy Protection Act (COPPA) of 1998 (SEC. 1301-1308). COPPA requires commercial web sites to obtain parental consent before collecting, using, or disclosing personal information of children under the age of 13.

Types of Information Requested

Much of the research on e-commerce trust has focused on measures of consumers’ beliefs, attitudes, and purchase intentions, without consideration for the types of information requested by the web sites. As noted earlier, the inherent risk is associated with the type of information required. Thus, it seems likely that the type of information requested could affect beliefs concerning risk and thus the willingness or intentions of consumers to engage in e-commerce transactions. That is, consumers are apt to engage in e-commerce transactions when a certain threshold of trust is achieved or the level of perceived risk is acceptable. Most theories on risk take into account not only the perceived level of risk involved in a transaction or gamble, but also the stakes involved in the gamble (Tversky, 1995). Thus, it might be reasonable to assume that the trust threshold for engaging in e-commerce transactions varies depending on the potential loss or harm that could result from engaging in a specific transaction. Individuals may be likely to engage in e-commerce transactions when there is little to lose even if the level of trust is low. Conversely, if (1) the perceived level of risk is high or (2) the potential loss or harm is substantial, there may be a reluctance to engage in e-commerce. It is likely that the perceived potential for loss or harm in e-commerce is dependent upon the type of personal information requested. Thus, whether a consumer engages in an e-commerce transaction is apt to depend not only on the level of trust, but also the potential loss associated with the type of personal information required.

There is enormous variability in the types of information requested by web sites. Some web sites require contact information before consumers are even allowed to access a web site and extensive personal information must be provided in order to complete a transaction (Sipior et al. 2004). At the other extreme, some web sites make it possible for consumers to conduct transactions based on a limited amount of personal information submitted to the web site using such techniques as buyer's authentication, confirmation and payment assurance, or non-repudiation (Hoffman, Novak, & Peralta, 1999). Other web sites may permit consumers to browse potential products and services and then printout order forms that can be submitted using other modes of communication (e.g., telephone, conventional mail, or fax) (Miyazaki & Fernandez, 2000).

A preliminary review of web sites suggests that most of the information requested by web merchants can be broadly classified as contact, biographical, or financial. Contact information includes such items as e-mail address, name, mailing address, and telephone numbers. Contact information is of value to web merchants for several reasons including creating mailing lists to publicize special promotions, products, or services offered by the web merchant. However, contact information may also be sold by web merchants to third parties. Consequently, many individuals are often reluctant to provide contact information to web sites (Greiner, 2003).

Biographical information includes demographic data such as income, personal preferences, interests, and hobbies. Web merchants may use biographical information to profile customers, target future communications for marketing purposes, and customize web pages for individual customers. Web sites may also use biographical information to market their site to advertisers by providing detailed information on visitors to their web site (Liu et al., 2004). Because consumers are concerned that personal information may be sold to third parties, most individuals (over 90 %) have refused to provide biographical information to a web site on at least one occasion and many (approximately 40%) admitted in some instances to providing false information (Hoffman et al. 1999). A recent review of the literature suggests that privacy concerns regarding how web sites use biographical information remains "a most formidable barrier to people engaging in e-commerce" (Wang & Emurian, 2005).

Financial information includes such items as credit card numbers and bank account numbers. Although consumers are obviously reluctant to provide financial information, this information is often viewed as necessary to complete an e-commerce transaction. However, numerous techniques such as buyer's authentication, confirmation and payment assurance, cryptography, digital signatures, non-repudiation, and alternative payment methods can reduce the perceived risks associated with financial transactions (Hoffman, et al. 1999; Kolsker & Payne, 2002; Miyazaki & Fernandez, 2000). While such techniques may complicate the processing of orders for web merchants, these procedures may reduce the perceived risk and increase consumer willingness to engage in e-commerce transactions.

Existing Federal Privacy Standards

Government involvement in the regulation of information privacy on the Internet varies greatly among nations with the degree of government involvement highly associated with the level of privacy concerns among citizens of a particular country (Smith, 1994). Many countries like the U.S., and until recently, Canada and Australia, have not been highly involved in the regulation of privacy standards, leaving it to the internet industry to regulate itself (Bellman, Johnson, Korbin, & Loshe, 2004). These countries have primarily targeted government regulation in certain areas, such as the public sector. This voluntary or *sectoral* approach contrasts with the omnibus approach, to both public and private sectors, used by the European Union (Bellman et al. 2004). Since the present study was conducted within the U.S. and for the most part examined the views of U.S. citizens, the focus of the present study is on the federal privacy standards existing in the U.S.

In recent years within the U.S., consumers have been inundated with notifications of federal privacy requirements when dealing with health care and financial institutions (e.g., loans, financial/investment advice, or insurance). In health care settings, patient privacy protection is mandated by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), while privacy of consumer information held by financial institutions is governed by the Gramm-Leach-Bliley Financial Modernization Act of 1999. Periodic (annual) and episodic notification of these acts and the respective institution's privacy policies have certainly contributed to an increased consumer awareness regarding not only privacy issues, but the existence of federal standards and enforcement in select industries. In these settings consumers have grown accustomed to uniformity in both format and content of privacy policies. This is in severe contrast to the Internet where consumers are confronted by a myriad of differences including placement, length, level of protection, and enforcement. Internet users must determine to what extent, if any, personal data will be utilized internally and/or shared for external or secondary purposes. Further, consumers must for the most part rely on self-policing and/or 3rd parties (seal programs) to insure compliance with stated policies.

Purpose of the Study

The fundamental purpose of this study is to determine whether the imposition of legally mandated privacy policy statements would significantly increase consumer trust and thus willingness to engage in e-commerce. Attempts to estimate the efficacy of regulation would seem prudent given calls for such regulation and the limited impact of voluntary privacy policy statements and self-regulation. Therefore, this study examined the effects of legally mandated versus voluntary privacy policy statements on consumer willingness to provide personal information.

Recognizing that consumer privacy concerns are determined to some extent by what information is requested (Cespedes & Smith, 1993) and level of protection promised (Meinert et. al, 2006), it is necessary to examine the efficacy of privacy policy statements in the context of both the information at risk and strength of protection afforded by the privacy policy. While information sensitivity varies from individual to individual, some information items or categories generate more privacy concerns than others. Therefore, a second objective of this study was to examine the main and interaction effects of types of information requested. To address this objective, when presenting the alternative privacy policy scenarios the effects of three information categories, contact, biographical, and financial, were examined.

Although privacy policy statements have become common, there is evidence suggesting that consumers may not be familiar with these statements (Westin & Maurici, 1998). It might be expected that with the increased popularity of e-commerce and the growing prevalence of privacy policy statements that more consumers at the present time would be aware of such statements. However, even though consumers may be aware of privacy policy statements, there is no guarantee that they read such statements. Research in the area of consumer behavior has demonstrated that customers frequently fail to read important and relevant information regarding transactions such as product warranties (Adler, 1994) or guarantees (Gore, 1995). Thus, although privacy policy statements are intended to increase consumer trust, if consumers are unaware or do not read the privacy policy statements, then the statements provide dubious benefits. Therefore, this study also examined whether consumers were generally aware of privacy policy statements and whether they had read a privacy policy statement prior to participation in this study.

Method

Data Collection

Given the exploratory nature of this research and the need to present respondents with multiple scenarios (5 scenarios of privacy policy statements x 3 types of information) a survey was selected over interviews, mall intercepts, quasi-experimental or experimental design. A survey approach also allows for detailed and consistent presentation of the descriptions for both privacy policy statements and information types. With this research procedure, respondents could compare and contrast descriptions, if necessary, to differentiate between the scenarios presented. Subjects were asked on the survey to indicate a willingness to provide various types of information to hypothetical web sites possessing dissimilar privacy policy statements. Concise descriptions of the alternative privacy policies were used to clearly differentiate between the types. Concise descriptions were selected over actual privacy policy statements, as the later are often very lengthy, difficult to read and contain information regarding other aspects of privacy and security. The questions from the survey relevant to the present study are presented in A. As can be seen in the appendix, subjects were not provided with any specific information concerning the nature of the hypothetical web site.

The survey provided the following definition of privacy policy statements. "A privacy policy statement explains a web site's policy regarding the information that is provided online by users." Following the definition of a privacy policy statement, respondents were given examples of three levels of privacy (strong, moderate, and weak) that seem to typify many of the statements presented on web sites. These examples were based on an examination of policy statements on over 75 web sites. Table 1 contains the descriptions presented to respondents to differentiate between strong, moderate, and weak privacy policy statements. Abbreviated descriptions for the three types of privacy policy statements were utilized to minimize the risk of respondents misinterpreting lengthy or technically written statements. Although the hypothetical privacy statements used in this study were considerably more concise than those usually found on the Internet, they captured the essence (i.e., level of protection) of what was found in the review of 75 such privacy statements.

Table 1: Descriptions of Privacy Policy Statements Examined

Type of Statement	Description Presented to Respondents
STRONG	A strong privacy policy statement explains a web vendor's policy concerning information that is provided by web users and makes an explicit guarantee that they will not under any circumstances share the user's information with any other organization, company, or individual
MODERATE	A moderate privacy policy statement explains a web vendor's policy concerning information that is provided by the web users and also ensures that the information that is provided will remain confidential. It also provides limited sharing of information when the web vendor believes that it is in the best interest of the customer, the web vendor, or both.
WEAK	A weak privacy policy statement explains a web vendor's policy concerning information that is provided by the web users, but does not offer any guarantee with respect to protecting personal information.
LEGALLY MANDATED	A legal privacy policy statement indicates that federal, state or local laws mandate the presentation and content of the privacy policy statement and use of information collected online.

The survey then provided respondents with a description of legally mandated privacy policy statements noting that "Some web sites indicate that federal, state or local laws legally mandate their privacy policy statement and use of information collected online." Thus, respondents were also asked their willingness to provide personal information IF a web site displayed a legally mandated privacy policy statement.

Following the definition of each example of a privacy policy statement, respondents were asked to indicate their willingness to provide various types of information on a six point Likert scale, ranging from (1) "extremely unlikely" to (6) "extremely likely". The types of information requested were defined in the following manner for the respondents on the survey.

- **Contact Information:** Request for e-mail address, name, mailing address and telephone number
- **Biographical Information:** Request for demographic data, such as annual income, personal preferences, hobbies, and interests.
- **Financial Information:** Request for credit card numbers, expiration date, bank account numbers, etc.

The decision to utilize broad information types reflected the breadth of information that can, and often is collected via the Internet and the desire to avoid a lengthy survey instrument that could easily compromise the quality of responses and/or response rate.

Sample

The sample consisted of 374 students enrolled in graduate courses or non-credit professional courses offered through the Colleges of Business at one of two Midwestern state universities. To achieve a high response rate, the survey was administered during regularly scheduled class periods. Although participation was voluntary, nearly 100% of the enrolled students participated. While the validity of using students in behavioral research has been questioned (Alpert, 1967; Gordon, Slade & Schmitt, 1986; Levitt, 1965), there are instances where they (students) are either good substitutes or surrogates for another population (Khera & Benson, 1970; LaTour, Champagne & Behling, 1990; Remus, 1986) or by virtue of demographic profile are representative of the target population under investigation. The latter instance was the primary justification for the use of graduate business students, specifically working professionals, in the present study. From its inception the Internet and to a large extent e-commerce has attracted substantially larger numbers of well-educated and affluent consumers (Guglielmo, 1999). Consumers with more education and above average incomes continue to be more likely to use the web and shop online (Enos, 2000; Kolettis, 2001). More recent research, has suggested that e-commerce has attracted a more diverse consumer group, however, the younger, more affluent and highly educated individuals still represent the vast majority of internet users (Savage & Waldman, 2005).

The present study relied on graduate students associated with business programs that have historically attracted working professionals. The profile of these students was consistent with the profile described above as on average they are more educated and earn more than the general population. The average age of the graduate students was also very close to the median age (36 years old) of Internet users (Kolettis, 2001). While this convenience sample is not representative of all Internet users it does represent a large segment of Internet users, one that is generally perceived to be more inclined to participate in e-commerce.

Findings

Table 2 summarizes the characteristics of the respondents. As illustrated in Table 2 most respondents connected to the Internet on a daily basis (86.4%). This compares favorably to national

norms for Internet users as Kolettis (2001) reported that 72 percent of women use the Internet every day, while 87 percent of men are daily users. Almost the same percent had provided an e-mail address to a web site (88.2%). Overall, the sample were somewhat younger and more educated than the general population, uses the Internet frequently and most have previously provided personal information to a web site. Consequently, the results must be generalized with caution. However, the sample would seem appropriate for a study aimed at determining the impact of privacy policy statements on the willingness of consumers to provide personal information to web merchants.

As shown in Table 2, 79.4 percent of the 374 respondents had reported seeing a privacy policy statement. However, only 170 or 45.5 percent indicated that they were familiar, or more specifically, had read a web site's privacy policy statement prior to the study.

Table 2: Respondent profile: Demographics (n = 374)

Demographic Characteristic		
Age (years)		
Mean	32.9	
S	14.3	
Gender		
Male	216	(57.6%)
Female	157	(41.9%)
No Response	1	
Connect to Internet		
Daily	324	(86.4%)
Twice a Week	19	(5.1%)
Weekly	9	(2.4%)
Monthly	2	(0.5%)
Never	15	(4.0%)
No Response	4	(1.4%)
Provided An Email Address		
Yes	330	(88.2%)
No	27	(7.2%)
No Response	17	(4.6%)
Awareness (Seen a Privacy Policy Statement)		
Yes	297	(79.4%)
No	73	(19.5%)
Familiarity (Read a Privacy Policy Statement)		
Yes	170	(45.5%)
No	154	(41.2%)

The mean willingness to provide the various types of information for each type of privacy statement is presented in Table 3 along with grand means. A 3 (Types of Information) X 5 (Type of Privacy Policy Statement) within subject ANOVA was conducted on the data. The last row of

Table 3 illustrates the differences in willingness to provide each of the three types of information requested. The overall mean willingness to provide personal information ranged from 3.74 for contact information to 2.70 for financial information. It is noteworthy that only the grand mean for contact (3.74) exceeded the scale midpoint, thus reflecting a “likeliness” to provide data. The ANOVA results indicated the difference between types of information was significant ($F=188.67$, $p = 0.000$). The results further revealed that all three possible pairwise comparisons were significant ($p < .05$). Respondents are least likely to provide financial, and most likely to provide contact.

Table 3: Mean Willingness to Provide Information to Web Sites

Policy Statement	Type of Information Requested			Grand Means
	Contact	Biographical	Financial	
Legally Mandated Policy	4.73	4.31	4.02	4.36
Strong Policy	4.84	4.33	4.01	4.42
Moderate Policy	3.50	2.89	2.22	2.88
Weak Policy	2.71	2.23	1.61	2.20
No Policy	2.88	2.28	1.51	2.26
Grand Means	3.74	3.22	2.70	

Mean based on 6-Point Likert Scale (1-Extremely Unlikely to 6-Extremely Likely)

The main effect for level of privacy offered by the policy statements is summarized in the last column of Table 3. The overall mean willingness to provide information by type of policy statement ranged from a high of 4.42 for strong policies to 2.20 for weak policies. The ANOVA results indicated the difference between the types of privacy policy statements was significant ($F=576.70$, $p = 0.000$). All possible pairwise comparisons between the conditions were significant except for the difference between a Weak Policy and No Policy. Respondents are significantly more likely to provide information for strong and legally mandated privacy policy statements. The mean response for the remaining privacy policy scenarios (no policy, weak and moderate) fell below the scale midpoint implying reluctance or unwillingness to provide information.

Perhaps the most interesting result was a significant interaction between type of privacy policy statement and type of information ($F = 24.87$, $p = 0.000$). This interaction is illustrated in the main body of Table 3. The type of privacy policy statement had the greatest impact on financial data and the least impact on contact. That is, willingness to provide financial information increased the most as the level of stated privacy increased. The results further indicated that only

three of the possible 30 pairwise comparisons were not significant. These included the difference between mandated and strong policy for biographical data, mandated and strong policy for financial data, and weak and no policy for biographical data.

Discussion

Not surprisingly, this study revealed that the willingness of individuals to provide information to web merchants depends on the type of information requested. Respondents were more willing to provide contact than biographical information and likewise biographical rather than financial information. Given the inherent risk associated with these types of information one would expect differences of this nature. These results suggest that alternative payment methods that do not require the submission of personal financial information may be extremely beneficial in overcoming one of the major obstacles faced by web merchants.

The relative sensitivity of biographical information has implications for organizations that have, or plan to collect such information for purposes of market segmentation or target marketing. The results suggest that consumers concerned about disclosing biographical information may opt to forgo providing any information, including contact, if the former information is a requirement. Future research is needed to demonstrate the necessity and potential value of differentiating between required and optional information either by category (e.g., biographical) or discrete element (e.g., home phone number).

The willingness to provide personal information varied depending on the level of privacy offered by the policy statements. As expected, respondents were more willing to provide information given a strong or legally mandated privacy statement. It was noteworthy that legally mandated policies are unlikely to foster greater trust than strong voluntary policies. Moderate statements proved to be more effective than a weak or no policy statement. On the other hand, a weak privacy statement was no more effective than not providing any policy statement. In summary, it appears that many Internet users, particularly younger and well educated, would be unwilling to provide personal information online, except when offered a strong or legally mandated privacy policy statement (i.e. comparing response means were below the responses with the midpoint of the Likert scale).

The interaction between type of privacy policy statement and type of information has several implications. First, in cases where financial and biographical information are requested strong or legally mandated privacy statements are a necessity. Respondents clearly perceive a difference in sensitivity across information types and are subsequently reluctant to provide more sensitive information in the absence of a strong or legally mandated privacy guarantee. Conversely, the strength of the privacy policy statement is of less importance when soliciting contact information.

A secondary goal of this study was to investigate the degree of prior awareness and familiarity with privacy policy statements. The findings indicate that while respondents were generally aware of privacy policy statements, most do not take the time to read them. This finding is noteworthy given the impact that such statements would purportedly have on consumer trust. If potential consumers do not read privacy policy statements, then even a strong guarantee of privacy will not be effective in terms of increasing confidence. Legally mandated privacy policies would offer the advantage of uniformity and thus a reduced need for consumers to peruse each web sites policy to ascertain the level of protection and enforcement.

However, it should be noted that evidence that consumers frequently do not take the time to read privacy policy statements does not imply that they have no impact on consumer trust. The mere indication that a web site contains a privacy policy statement may increase consumer trust. This would be consistent with studies demonstrating that warranties and guarantees may influence

consumer purchasing decisions, even though the consumer never actually read the warranties or guarantees (Adler, 1994; Gore 1995).

The success and growth of e-commerce is inextricably linked to consumer willingness to provide information to web sites. The findings of this study, while preliminary, suggest that legally mandated privacy policy statements are unlikely to significantly increase consumer trust and concomitantly participation levels in e-commerce. However, the findings suggest that privacy policy statements should have a strong guarantee of privacy in order to be effective. This is especially true in transactions requiring the submission of more sensitive personal information such as biographical and financial

Limitations and Future Research

First, the sample size and target population were limited which brings into question the degree to which the findings can be generalized. As noted above, while the sample is representative of a significant percentage of Internet users, the findings may not be generalized to other distinct segments such as less educated and older consumers that are increasingly utilizing the Internet. Second, the hypothetical nature of the privacy policy statements used in this study may have seemed somewhat artificial to the respondents. Experimental or quasi-experimental research involving actual web sites and privacy policy statements could be useful for replicating the results of this study. Third, the decision to reduce the granularity of the information types into three general categories rather than discrete data elements (e.g., credit card #, year of birth, blood type, social security number) may have impacted the results. Although some significant differences were noted using broad categories, it would be beneficial to extend these findings in a similar study using discrete data elements of varying sensitivity. Such research could potentially identify within category differences as well as validate the across group differences noted herein (e.g., contact vs. financial). Fourth, since the study was based on current U.S. privacy policy practices and was limited to U.S. respondents the findings may not be transferable to other countries with more restrictive data protection laws (e.g., EU countries). Fifth, other variables may play a critical role in creating trust in addition to, or in combination with the privacy policy statement (Grewal et al. 2003). Similarly, further research is clearly needed to ascertain which individual variables might explain why consumers differ with respect to reading privacy policy statements. Also an understanding of the contextual factors relating to the likelihood that a privacy policy statement will be read could have an impact on the placement, text, etc. of privacy policy statements.

Summary

This study validates earlier findings that type of information and type of privacy policy statement play a role in determining consumer willingness to submit personal information via the Internet. In addition, the findings indicate that legally mandated or imposed privacy policy statements resulting from regulation are unlikely to significantly reduce consumer reluctance to provide personal information on-line. On the contrary, findings from this study suggest that legally mandated privacy statements would be no more effective than strongly worded voluntary policies. This finding clearly contradicts calls for federal legislation to protect consumers and stimulate greater rates of participation in e-commerce. Clearly, more extensive research is needed to fully understand both the limitations and potential of privacy policy to increase consumer trust related to e-commerce.

References

- 4321 Net. (2002, Jan 10). Privacy statement and policy. Retrieved November 20, 2005, from http://4321net.com/privacy_statement.htm
- Adler, R. S. (1994). The last best argument for eliminating reliance from express warranties: "Real-World" consumers don't read warranties. *South Carolina Law Review*, 45(3), 429.
- Alpert, B. (1967). Non-businessmen as surrogates for businessmen in behavioral experiments. *Journal of Business*, 40, 203-7.
- Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly*, 26(3), 243-269.
- Bellman, S., Johnson, E. J., Korbin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, 20, 313-324.
- Cespedes, F.V., & Smith, H.J. (1993). Database marketing: new rules for policy and practice. *Sloan Management Review*. 34(4), 7-22.
- Corbitt, B. J., Thanasankit, T., & Han, Y. (2003). Trust and e-commerce: A study of consumer perceptions. *Electronic Commerce Research & Applications*, 2(3), 203-216.
- Criswell, J., & Meinert, D. (2003). The efficacy of web site privacy policy statements: An exploratory study. *Journal of Business and Behavioral Sciences*, 10(2), 102-117.
- Culnan, M. (1999). Progress report to the Federal Trade Commission (FTC) (funded by the Online Privacy Alliance), Retrieved September 14, 2003, from <http://www.msb.edu/faculty/culnanm/gippshome.html>
- Enos, L. (2000). Net prices no lure for most e-shoppers. *Ecommerce Times*. Retrieved from <http://www.ecommercetimes.com/story/4645.html>
- Federal Trade Commission (2000) Privacy online: Fair information practices in the electronic marketplace: A report To Congress. Retrieved November 20, 2005, from <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>
- Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *DATA BASE for Advances in Information Systems*, 33(3), 38-54.
- Gordon, M. E., Slade, L. A., & Schmitt, N. (1986). The 'science of the sophomore' revisited: from conjecture to empiricism. *Academy of Management Review*, 11(1), 191-277.
- Gore, M. (1995). Read the fine print when selling guarantees. *Best Review*, 95(11), 64-65.
- Grewal, D., Munger, J. L., Iyer, G. R., & Levy, M. (2003). The influence of Internet-retailing factors on price expectations. *Psychology & Marketing*, 20(6), 447-493.
- Greiner, L. (2003). Information requested is none of company's e-business. *Computing Canada*, 29(19), 19.
- Guglielmo, C. (1999). E-Commerce: There to here. *Inter@Active Week*, 6(47), 106.
- Higgins, A. (1998, August 24). Certification aims to calm online buying fears. *The Cincinnati Enquirer*. Retrieved November 20, 2005, from http://www.enquirer.com/editions/1998/08/24/bus_cpaweb24.html
- Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information privacy in the marketplace: Implications for the commercial uses of anonymity on the Web. *The Information Society*, 15, 129-139.
- Jarvenpaa, S.L., Tractinsky, N., Saarinen L., & Vitale, M. (1999). Consumer trust in an Internet store: a cross-cultural validation. *Journal of Computer Mediated Communication*, 15(2), Retrieved March 14, 2003, from <http://www.ascusc.org/jcmc/vol5/issues2/jarvenpaaa.html>
- Khera, I. P., & Benson, J. D. (1970). Are students really poor substitutes for businessmen in behavioral research? *Journal of Marketing Research*, 7, 529-32.

Regulation of Web Site Privacy Policy

- Kolettis, H. (2001). Who's caught in the web? *Security Distributing & Marketing*, 31(11), 14.
- Kolsaker, A., & Payne, C. (2002). Engendering trust in e-commerce: A study of gender-based concerns. *Marketing Intelligence & Planning*, 20, 206-214.
- LaTour, M., Champagne, P. J., & Behling, R. (1990). Do students represent a viable source of data for researching business social responsibility and ethical issues? *The Journal of Computer Information Systems*, 30, 26-29.
- Lee, M. K. O., & Turban, E. (2001). A trust model for consumer Internet shopping. *International Journal of Electronic Commerce*, 6(1), 75-91.
- Levitt, T. (1965). *Industrial purchasing behavior*. Boston: Harvard University.
- Limayem, M., Khalifa, M., & Frini, A. (2000). What makes consumers buy from Internet? A longitudinal study of online shopping. *IEEE Transactions on Systems, Man, and Cybernetics (Part A)*, 30(4), 421-432.
- Liu C., & Arnett, K. (2000). Exploring the factors associated with Web site success in the context of electronic commerce. *Information & Management*, 38, 23-33.
- Liu, C., & Arnett, K. (2002). An examination of privacy policies in Fortune 500 web sites. *Mid-American Journal of Business*, 17(1), 13-22.
- Liu, C., Marchewka, J. T., & 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.
- Luo, W., & Najdawi, M. (2004). Trust-Building Measures: A Review of Consumer Health Portals. *Communications of the ACM*, 47 (1), 109-113.
- McKnight, D. H., & Chervany, N. L. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce*, 6(2), 35-59.
- Meinert, D., Peterson, D., Criswell, J., & Crossland, M. (2006). Privacy policy statements and consumer willingness to provide personal information. *Journal of Electronic Commerce in Organizations*, 4(1), 1-17.
- Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing*, 19(1), 54-61.
- Miyazaki A. D. & Fernandez A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *The Journal of Consumer Affairs*, 35(1), 27-44.
- Ngai, E. W. T., & Wat, F. K. T. (2002). A literature review and classification of electronic commerce research. *Information & Management*, 39, 415-429.
- Pennington, R., Wilcox, H. D., & Grover, V. (2003). The role of system trust in business-to-consumer transactions. *Journal of Management Information Systems*, 20(3), 197-226.
- Ranganathan, C., & Ganapathy, S. (2002). Key dimensions of business-to-consumer web sites. *Information & Management*, 39, 457-465.
- Remus, W. (1986). Graduate students as surrogates for managers in experiments on business decision making. *Journal of Business Research*, 14, 19-25.
- Savage, S.J., & Waldman, D. (2005). Broadband Internet access, awareness, and use: Analysis of United States household data. *Telecommunications Policy*, 29(8), 615-633.
- Sheehan, K.B. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society*, 18(1), 21-32.
- Sipior, J. C., Ward, B. T., & Rongione, N. M. (2004). Ethics of collecting and using consumer Internet data. *Information Systems Management*, 21(1), 58-66.

Smith, H. J. (1994). *Managing privacy: Information technology and corporate America*. Chapel Hill: University of North Carolina Press.

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of Electronic Commerce*, 7(3), 135-161.

Sun Microsystems. (2001, May 22). Sun online privacy policy. Retrieved November 27, 2005, from <http://www.sun.com/privacy/>

Swire, P., Baker, R., Bentivoglio, J., Doerflein, R., Irving, P., Moushegian, V., & Pincus, A. (1999, June 1). Guidance and model language for federal web site privacy policies. M-99-18. Retrieved October 20, 2003, from <http://www.whitehouse.gov/omb/memoranda/m99-18attach.html>

Tan, S. J. (1999). Strategies for reducing consumers' risk aversion in Internet shopping. *Journal of Consumer Marketing*, 16, 163-180.

Tan, Y., & Thoen W. (2001). Toward a generic model of trust for electronic commerce. *International Journal of Electronic Commerce*, 5(2), 61-74.

Tversky, A. (1995). Weighing risk and uncertainty. *Psychological Review*, 102(2), 269-283.

Tribunella, T. (2002). Twenty questions on E-commerce security. *The CPA Journal*, 72(1), 60-63.

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in Human Behavior*, 21(1), 105-125.

Westin, A., & Maurici, D. (1998). *E-commerce and privacy: What net users want*. Price Waterhouse Coopers, p. 15.

Appendix A

Section 3:						
While the type of information collected via web sites varies from site-to-site, there are three basic categories of information collected online:						
Contact Information: Request for a web users e-mail address, name, mailing address or telephone number.						
Financial Information: Request for data sufficient for conducting financial transactions (credit card number, expiration date, bank account number, etc...).						
Biographical Information: Request for information for the purposes of marketing. Includes demographic data, annual income, personal preferences, hobbies, interests, and others.						
To what extent would you be willing to provide the following types of information IF a web site did not provide a privacy policy statement?	Extremely Likely	Quite Likely	Slightly Likely	Slightly unlikely	Quite unlikely	Extremely unlikely
12. Contact Information						
13. Financial Information						
14. Biographical Information						

Section 4: Types of Privacy Policy Statements						
<p>As stated, a web site privacy policy statement is intended to let users know what level of privacy they can expect if they submit information to that site. Unfortunately, not all privacy policy statements promise the same level of protection when it comes to user privacy. For this survey web site privacy policy statements have been categorized in three basic levels:</p> <p>Weak: A weak privacy policy statement explains a web vendor’s policy concerning information that is provided by the web users, but does not offer much if any guarantee when it comes to protecting the information.</p> <p>Moderate: A moderate privacy policy statement explains a web vendor’s policy concerning information that is provided by the web users and also insures that the information that is provided will remain confidential. It also provides limited sharing of information when the web vendor believes that it is in the best interest of the customer, the web vendor, or both.</p> <p>Strong: A strong privacy policy statement explains a web vendors policy concerning information that is provided by web users and makes an iron clad guarantee that that they will not under any circumstances share the user’s information with any other organization, company, or individual.</p>						
To what extent would you be willing to provide the following types of information IF a web site displayed a weak privacy policy statement?	Extremely Likely	Quite Likely	Slightly Likely	Slightly unlikely	Quite unlikely	Extremely unlikely
15. Contact Information						
16. Financial Information						
17. Biographical Information						
To what extent would you be willing to provide the following types of information IF a web site displayed a moderate privacy policy statement?						
18. Contact Information						
19. Financial Information						
20. Biographical Information						
To what extent would you be willing to provide the following types of information IF a web site displayed a strong privacy policy statement?						
21. Contact Information						
22. Financial Information						
23. Biographical Information						

Section 6: Legally Mandated Privacy Policy Statements						
Some web sites indicate that federal, state, or local laws legally mandate their privacy policy statement and use of information collected online.						
To what extent would you be willing to provide the following types of information IF a web site displayed a legally mandated privacy policy statement?	Extremely Likely	Quite Likely	Slightly Likely	Slightly unlikely	Quite unlikely	Extremely unlikely
27. Contact Information						
28. Financial Information						
29. Biographical Information						

Biographies



David B. Meinert is Professor and Director of the MS CIS Program at Missouri State University. Dr. Meinert received his doctorate in management information systems from the University of Mississippi in 1990. His professional background includes software development, systems integration and project management. Dr. Meinert has published in a number of journals, including Journal of Applied Business Research, Journal of Computer Information Systems, Journal of Electronic Commerce in Organizations, Information Strategy: The Executive’s Journal, Information Resource Management Journal, End User Computing Management, Focus on Change Management, and Journal of Marketing Management.



Dane K. Peterson is a Professor of Quantitative Business Analysis at Missouri State University. He received his Ph.D. in Quantitative Methods and Applied Psychology from Southern Illinois University. He has published in numerous journals such as Journal of Applied Psychology, Organizational Behavior and Human Decision Processes, Journal of Electronic Commerce in Organizations, International Journal of Information Management, Business & Society, Information Resources Management Journal, Business & Psychology, Personnel Review, and Information Technology & People.



John R. Criswell II is a senior programmer with Shelter Insurance and adjunct instructor teaching computer information systems at Columbia College in Columbia, Missouri. He received his B.S. (computer information systems), MBA and MS CIS from Missouri State University. His research has appeared in the *Journal of Business and Behavioral Sciences* and *Journal of Electronic Commerce in Organizations*. His current research interests include privacy policy statements, e-commerce and ethics in information systems.



Martin D. "Marty" Crossland is an Associate Professor of Management Science and Information Systems at Oklahoma State University. He earned a Ph.D. in Management Information Systems from Indiana University, an MBA from Oklahoma City University and a BS in Geology from Texas Tech University. His research interests include decision making effectiveness and human factors in decision support system usage, particularly with spatially reference information (geographic information systems), telecommunications and networking, and systems security. His research has been published in various journals, including *MIS Quarterly*, *Decision Support Systems*, *Journal of End User Computing*, and *Technology Studies*.