Journal of International Technology and Information Management

Volume 16 | Issue 1 Article 2

2007

Personal Data Collection via the Internet: The Role of Privacy Sensitivity and Technology Trust

Susan K. Lippert
Drexel University

Paul Michael Swiercz
The George Washington University

Personal Data Collection via the Internet: The Role of Privacy Sensitivity and Technology Trust

Susan K. Lippert
Drexel University

Paul Michael Swiercz
The George Washington University

ABSTRACT

Policy makers and researchers from a wide range of perspectives have expressed concern about the interplay between privacy rights and information exchanges via the Internet. Of particular interest has been the challenge of protecting sensitive personal information. In this paper, we assert that user willingness to share sensitive data is an area of critical concern and requires additional investigation. In an effort to enrich the dialogue on the question of voluntary sharing of sensitive personal data via the Internet, we present a model showcasing the relationship between personal data sharing, privacy sensitivity, and technology trust and discuss how organizations can apply these insights.

INTRODUCTION

Communication is an essential business process because it is only through the effective exchange of ideas that successful transactions are realized. Effective communication in the form of personal face-to-face exchanges remains the richest form of interaction. Yet, the use of various technologies to facilitate communication presents challenges for its users since the technology mediates the transmission of the message. In the contemporary organization, telephones continue as a dominant form of technology-mediated communication but a growing proportion of business communication occurs through electronic mail, text messaging, video conferences and computer-mediated group discussions.

In the United States alone, email volume is projected to nearly double from 1.5 trillion in 2003 to 2.7 trillion in 2007 (Hallerman, 2005). In the United Kingdom, it is estimated that businesses are loosing over £68,000 per day or £1 billion a year in business due to firms lacking e-mail services (“Email Costs”, 2005). Worldwide, Internet usage estimates have increased by 146.2% between 2000 and 2005 indicating that almost 14% of the world’s estimated 6 billion people are using the Internet (“Internet Usage”, 2005). The growth and penetration of these communication media are distinguishable from face-to-face or telephone channels by the unprecedented ability to collect, store, and share sensitive private information. Severson (1997) reported that ⅓ of Americans are concerned about privacy issues particularly since personal information about each person is transferred between computers on average of five times per day (Eder, 1994).

In 1890, Samuel Warren and Louis Brandeis published an article entitled *The Right to Privacy*. In this article, Warren and Brandeis (1890) defined privacy as “the right to be let alone” and indicated that individuals should receive full protection of person and property. Protection of person represents the individual’s protection from physical interference while protection of property means the protection of an individual’s property, feelings, and intellect. The Warren-Brandeis article profoundly shaped the development of privacy laws. An individual’s or company’s right to know or need to know must always be balanced against the individual’s right or need for privacy (Buchanan, Paine, Joinson, & Reips, (2007). For purposes of this paper, we accept this definition of privacy as ‘the right to be let alone’ and suggest that privacy is a limitation of others’ access to personal information (Gavison, 1995). Information privacy involves the compilation, use, and dissemination of information about individuals (Spinello, 2000). The right to maintain informational privacy concerns the right to control the disclosure of and access to personal information (Spinello, 2000). Technology enables the collection and exchange of personal information through computing and communication technologies (Association for Computing Machinery, 1992). Individuals’ privacy has become particularly vulnerable with the recent developments in technology (Earp, Anton, Aiman-Smith, & Stufflebeam, 2005; Mollick & Pearson, 2006; Velasquez, 1998). Privacy sensitivity is the "attitudinal disposition describing an individual's willingness to share information of a personal and private nature" (Hamilton, 2005, 7).

Caudill and Murphy (2000) provide a general definition of personal information and claim that personal information is "data not otherwise available via public sources." Personal information may include an individual's social security number, mother's maiden name, health history, salary history, or financial records. These data are generally considered sensitive since most people do want others to have knowledge of or access to this information without expressed consent (Pollach, 2005). Personal privacy is the explicit protection of personal data through structural and regulatory procedures. Nissenbaum (1997) argues for the extension of a privacy definition that encompasses all information including that which is considered to be public. She suggests that the power of computers to synthesize repositories of data contained in organizational databases exposes individuals to potential privacy violations resulting in invasion of privacy. Elgesem (2001) suggests that there are two types of privacy violations: (1) when information that is personal is disseminated to another without consent; and (2) when information is used to make decisions concerning the individual. Either type of privacy violation can have negative consequences on the individual.

THE VALUE OF PRIVACY

Privacy is valued at different levels for different circumstances. Usually, the first issue of privacy value is the potential economic consequences of privacy data disclosure. Recently, the issue of identity theft has been exposed as the use of computer technology has dramatically increased. The economic consequences of identity theft have been widely discussed and new procedures or practices to prevent the disclosure of privacy information continue to be developed. A second consideration in the value of privacy is related to the cultural norms within a context or society. For example, some cultures and political systems see limited privacy for individuals while other cultures, such as the American culture, have traditionally valued individual protection of information as a strong and distinguishing cultural norm.

Privacy may have a different meaning from society to society (Hamilton, 2005). Sheehan and Hoy (1999) suggest that new technological capabilities provide opportunities for individuals and organizations to violate consumers' privacy in an online arena (Sheehan & Hoy, 1999). In a recent study, the Federal Trade Commission (1998) indicated that more than 92% of Web sites collect personal information. Straub and Collins (1990) suggest that organizations should place greater attention on developing strategies designed to collect and disseminate customer information while simultaneously respecting their right to privacy. The importance or value of privacy is variable in that what one person values may be slightly different from what another individual deems sensitive (Stalder, 2002). This variability in sensitivity belies a fundamental premise to the diversity of individual privacy preferences. An individual's right to privacy can be undermined by others' interest and access to their personal and private information (Britz, 1999).

The purpose of this paper is to explore the question of individual willingness to share sensitive information on a voluntary basis via the Internet. We argue that user willingness to share personal sensitive information, as distinguished from the broader topic of user privacy rights and expectations, is an area of critical concern requiring additional investigation. Toward the goal of encouraging dialogue and empirical research on the question of voluntary sharing of sensitive personal data via the Internet, we present a model showcasing the relationship between personal data sharing, privacy sensitivity, and technology trust. In addition, we discuss how organizations can apply these insights in support of improved user interactive system design and implementation.

COMPUTER-MEDIATED-COMMUNICATION AND PERSONAL IDENTITY

In the past decade, the term Computer-Mediated-Communication (CMC) has emerged to differentiate computerized exchanges from other forms of technology-mediated-communication. Not surprisingly, different definitions of this construct exist. Ebersole (1999, p. 1) defines CMC as "the study of human communication using the medium of networked computer technology". Rice (1992b, p. 438) defines CMC as "media that facilitates the exchange of semantic content, transmitted through telecommunications networks, and processed through one or more computers, between individuals and among groups who in one way or another can be identified as such". Similarly, Walther (1992, p. 52) defines CMC as "synchronous or asynchronous electronic mail and computer conferencing, by which senders encode in text messages that are relayed from the senders' computers to receivers'". For purposes of this paper, these definitions are sufficient providing the addition of one characteristic. Namely, computer-mediated-communication is distinguished by the degree to which private information can be captured, manipulated, and used in ways not intended by the sender.

The most dramatic expression of this characteristic is the phenomenon of identity theft. Identify theft occurs when personal information, such as an individual's name, social security number, credit card number or other identifying information, is used by someone without permission to commit fraud or other crimes (Federal Trade Commission, 2005). This type of theft can occur within an organization when an individual steals records or information while at work, by bribing an employee who has access to sensitive data, by hacking into a database, or by conning information out of employees (Federal Trade Commission, 2005). The effects of such activities can be devastating since identity theft creates an average loss of $10,000 per victim per event, affects approximately 4.7% of the U.S. population, and costs Americans over $5 billion a year ("Effects Identity", 2005). Additionally, personal information obtained through an Internet site may be sold or disclosed to third parties, acquired through the use of cookies, gained from information in an email, or secured through surveys, forms or online questionnaires. In a survey conducted by the Ponemon Institute and TRUSTe of 6,300 consumers, 76% of the respondents indicated that identity theft was their greatest concern regarding the misuse of their personal information (Greenspan, 2004).

Given these alarming statistics and potential negative outcomes, it raises the question: why would people want to share personal information? We suggest that people share personal information for at least four reasons: (1) to fulfill the requirements of an economic transaction; (2) to make an emotional connection; (3) to signal trust; and, (4) to reduce ambiguity.

A continuing ethical debate exists concerning what constitutes socially acceptable practice in data sharing and access. In particular, there are a number of ethical considerations in the use of computer technology. These considerations include: (1) the propriety nature of information sharing; (2) the degree of access; (3) the qualifications for individuals or organizations to be privy to privacy data; (4) standardization of practices and procedures within the computer information systems profession; and, (5) agreed upon sanctions for ethical violations. The two sides of the debate include increased protection of privacy along with additional threats to privacy while the other side of the debate suggests that privacy is never protected (Gavison, 1995). Despite the underlying disagreement in terms of what constitutes privacy and how privacy issues should be addressed, the two sides agree that privacy is a legal right (Gavison, 1995).

FULFILLING THE REQUIREMENT OF AN ECONOMIC TRANSITION

Economists have developed a wide variety of tools in an effort to model the economic behavior of people and firms; a well known example of this effort is Transaction Cost Economics (TCE) (Coase, 1937). According to TCE, a transaction involves costs and occurs whenever a good or service passes a technological barrier. Within the firm, this may include coordination and organizational costs; outside the firm, these costs may include contracting fees and contract fulfillment expenditures between two organizations. From this perspective, one of the great advantages of Internet commerce is the ability to dramatically reduce transaction costs. The airline industry, for example, has fully embraced Internet reservation and ticketing services to exploit transaction cost efficiencies. Online travel is continually the largest online shopping category with total online purchases of U.S. leisure and business travel projected to triple in the next five years from $18 billion in 2000 to $63 billion in 2006 ("Online Travel Market", 2001). The online travel industry routinely completes 64% of transactions online compared to other product categories that transact only 30-40% of revenues through the online interface ("Online Travel", 2001). In fact, online transactions have become so embedded into practices of the airline industry that consumers now face extra charges for services (paper tickets) that were once included in the ticketing process.

One of the byproducts of this economically efficient transaction mechanism is a dramatic increase in the demand and use of personal information. Companies not only consistently require personal information as part of the formal transaction but sophisticated technology now enables them to use recorded historical data to construct a highly personalized profile of the customer. And as a consequence of this profile, companies now have the capacity to predict, with great accuracy, everything from vacation preferences to voting behavior. How these data are used becomes an issue of personal privacy and a concern for those individuals who provide the information.

MAKING AN EMOTIONAL CONNECTION

In a recent *Harvard Business Review* article, Hallowell (1999) suggested that in a world of high-paced technology, executives need to rethink how information is communicated within organizations. Hallowell (1999, p. 59) argues that executives need to experience "the human moment" which he describes as an "authentic psychological encounter that can happen only when two people share the same space…and share their emotional and intellectual attention".

Although no research has focused exclusively on the concept of the "human moment", interpersonal communication dynamics are being explored through various media selection theories (e.g., Daft & Lengel, 1986; Carlson, 1995). These theories suggest that face-to-face communication allows for an emotionally rich exchange since message transmission occurs without interference from a secondary communication medium. The existence of eye contact enables immediate assurance and feedback between individuals (Argyle & Dean, 1965). Eye contact also creates a feeling of intimacy, which leads to increased trust between people. In terms of organizational communication, Adams, Todd & Nelson (1993) found that in an environment where face-to-face communication is primarily used, horizontal communication amongst employees is far more frequent than vertical communication between subordinates and supervisors.

Email enables more uninhibited communication content resulting from a sense of anonymity (Marchewka, Liu, & Petersen, 2003). The speed of message creation and distribution facilitated by email reduces the user's emotional awareness of the message content (Kiesler, Zubrow, Moses & Geller, 1985). The combination of reduced inhibition and a lack of emotional awareness places certain limitations and constraints on the use of email. Phillips (1989) contends that individuals use email to persuade others through indirectness, impoliteness, assertiveness, and manipulation. Phillips' (1989) work contradicts other studies that claim email is an ineffective method of communicating complex information (e.g., Kiesler et al., 1985; Golden, Beauclair & Sussman, 1992). When communication occurs through computer-mediated media such as email, personal identifies such as race, gender, physical condition, economic level, age, and social status of senders and receivers are less apparent than through other communication media (Donovan, 1995).

SIGNALING TRUST

In the face of increased competition and reduced pricing flexibility, virtually all members of the business sector have committed themselves to the task of cultivating stronger customer relationships. Typically, strong relationships are based on a high degree of personal contact and the persistence of trustworthy behavior exhibited by both parties. Trust enables individuals to reasonably predict how another will behave and enables the establishment and testing of expectations (Deutsch, 1960). Developing interpersonal trust relationships is important for sustaining individual and organizational effectiveness (McAllister, 1995). However, when communication is mediated through a technology, the personal interaction can potentially be impacted by the technology's presence.

Strategies that companies have used for establishing and maintaining trust to the benefit of longer-term relationships include: (1) reducing perceived risk; (2) offering contractual safeguards; (3) building customer confidence interaction by interaction; (4) emphasizing competence; and, (5) resolving conflicts in a timely manner (Harrison, 2003).

All of these tools can be effective but the test of their success is the user's signal that he is responding in a manner consistent with the firm's aspirations. What this means in practical terms is that the customer responds by sharing more personal information (McCarthy, Aronson, & Petrausch, 2004). For example, customers of a bank signal trust each time they transfer more control of their financial well-being to the bank. Each time they use the bank for a new financial service – checking, saving, financial planning, auto loans, mortgage services, or brokerage services – they signal trust by providing more personal information.

REDUCING AMBIGUITY

Within the domain of information systems and communication research, a substantial theoretical literature base has been generated as part of an effort to understand why and how managers select a particular communication channel. Carlson and Zmud (1999, p. 153) identified eight interrelated theories used to study organizational communication, table 1.

Table 1: Communication Theories.

Theory	Source
Media Richness Theory	Daft & Lengel, 1986
Social Influence Model of Technology Use Theory	Fulk, 1993; Fulk, Steinfield, Schmitz & Power, 1987
Channel Expansion Theory	Carlson & Zmud, 1999, 1994; Carlson, 1995
Media Symbolism	Trevino, Lengel, & Daft, 1987
Situational Factors	Trevino et al., 1987; Rice, 1992a
Social Presence	Short, Williams & Christie, 1976
Critical Mass	Markus, 1987
Communication Genres	Yates & Orlikowski, 1992

Of these eight, Media Richness Theory (MRT) offers the greatest promise for shedding light on the question of voluntary information sharing. MRT asserts that individuals within organizations use media selection to reduce ambiguity in communication. Richness, in this context, refers to the capacity of the communication channel to not only transfer data but also to impart meaning. Richness is achieved by sending equivocal information which is intended to provide nuance and modify the receiver's understanding of the message. Understanding occurs when different conceptual frames of reference converge or ambiguous issues are resolved. If a particular medium provides new understanding or carries equivocal information effectively, the medium is deemed rich.

Communication media vary in their ability to reduce ambiguity in communication. According to Media Richness Theory, ambiguity is reduced through a blending on four criteria based on the communication medium's ability to: (1) facilitate feedback; (2) convey meaning through multiple cues; (3) use a variety of language; and, (4) present personalized messages. Thus, since organizational tasks differ in terms of ambiguity, the selection of an appropriate communication media to transmit the message becomes an important criterion to reduce uncertainty in meaning.

Computer-mediated interactions lack non-verbal queues that exist in face-to-face exchanges that are used to inform understanding between the individuals (Kiesler, 1986; Rice & Love, 1987). As a communication medium, CMC provides the possibility to create new identities not present in face-to-face situations. These challenges, coupled with the fact that people share personal information to facilitate the requirements of an economic transaction, to make an emotional connection, to signal trust, and to reduce ambiguity, make understanding why individuals share personal information more compelling.

THE NATURE OF PERSONAL DATA COLLECTION

One of the major challenges associated with the implementation of an Internet-based communication network concerns the nature of the data to be collected. One simple way to approach this challenge is to categorize prospective data into two broad categories: (1) data owned by the sender (person specific); and, (2) data owned by the organization (organization specific).

Person specific information owned by individuals includes data such as educational background, career history, family status, health status, political beliefs, personal preferences, ethical standards, and performance motivation. Some of this data is relatively benign and most individuals share it without much consideration. However, within the category of person specific information, there are facts that many people would aggressively define as being *sensitive* and therefore beyond the legitimate domain of information to be captured and shared in an Internet database.

In contrast, organization specific (i.e., transaction) data is composed of artifacts derived as a byproduct of the interaction between the individual and the organization. Consider, for example, the employment relationship. As the relationship progresses over time, the employee engages in a process of progressive data sharing with the firm. During the pre-hire process, the prospective employee completes a variety of application and data release forms. The data contained on these forms may be collected from a range of different sources. Standard application documents provide the initial data for career history, skills, and educational background. Release for reference checks provides information concerning the employees' performance ratings, technical and functional skills as observed by previous employers, and character references provided by others. Background checks reveal information on domestic relations, credit history, military service, criminal history, personal habits such as use of illegal substances and abuse of alcohol, standing within the community, psychological problems, trustworthiness, and reliability.

With increasing tenure in the organization, the distinction between organization specific and person specific information becomes increasingly more ambiguous for the question of ownership. Performance reports written by superiors, for example, are generally considered to be owned by the employer. Likewise, many companies are beginning to treat email as organizational property, which makes its contents available for scrutiny in situations where a chronological history of interactions is required. In contrast, information concerning an employee's decision to pursue advanced training, volunteer at a community organization, become politically active, or enter into a committed personal relationship are all information elements generally thought to be owned by the employee until such time that the employee chooses to share the information with the employer.

A MODEL OF PERSONAL DATA SHARING VIA THE WEB

Figure 1 represents a proposed model of voluntary personal data collection likely to occur via the Internet. In summary, the model identifies two variables – privacy sensitivity and technology trust – that moderate the voluntary decision to share personal person specific data. In addition, the model calls attention to the character of the shared data by acknowledging that individuals may submit incorrect information either intentionally or unintentionally. In other words, accuracy and veracity influence the utility of personal data collected via the Internet. The interconnections between each of the propositions under consideration are the notions of disclosure and accuracy. Disclosure, as the link between assertions, directly addresses either the voluntary offering or withholding of personal data and represents one connection between the propositions. Accuracy represents the conscious or unconscious disclosure of incomplete or inaccurate personal data. The second link between propositions is the notion of accuracy. Specifics regarding the proposed variables and their causal relationships are provided below.

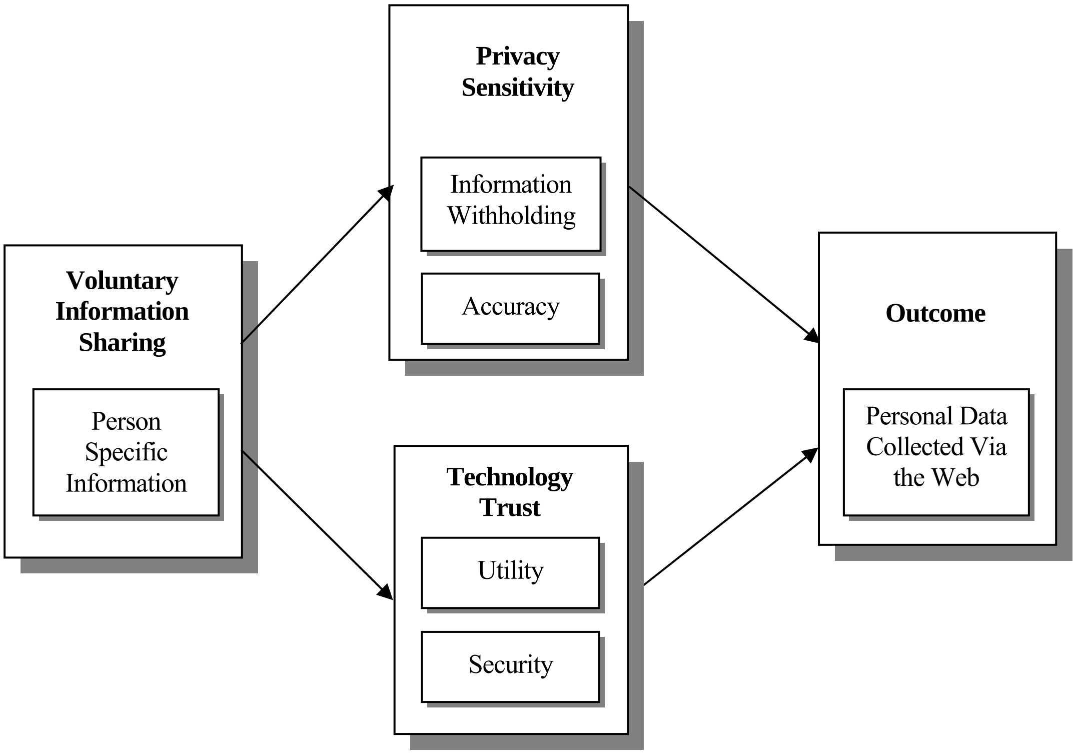
Privacy Sensitivity
Information Withholding
Accuracy
Voluntary Information Sharing
Person Specific Information
Outcome
Personal Data Collected Via the Web
Technology Trust
Utility
Security

Figure 1: Research Model.

PRIVACY SENSITIVITY

Privacy sensitivity is the "attitudinal disposition describing an individual's willingness to share information of a personal and private nature" (Hamilton, 2005, 7). Those responsible for creating effective interactive web sites must be proactive with respect to privacy concerns. One way to do this is by creating policies and practices that are understood by managers, employees, and end users. Policies regarding data privacy must be tailored to meet the complex and often competing demands of a wide array of organizational stakeholders (Ryker, Khurrum & Bhutta, 2005).

Generally speaking, the development of an effective privacy policy includes attention to: (1) providing a clear definition of private records; (2) specifying the data to be included in an individual's record; (3) identifying employees who should have access; (4) defining what information can be disclosed to outsiders, including appropriate approval processes known in advance to employees; and, (5) clarifying user access to their own data (Bland-Acosta, 1988).

Technology advances have brought with them a major change in the traditional interaction between data collectors and end users. Anonymity can now vanish with just a few keystrokes. In even a modestly sophisticated organizational setting, a user's complete profile – jobs held, educational background, income, performance, buying habits, and credit history – is potentially available to almost anyone with, and too often without, proper authorization. This is a well-known and contested issue, but the risk of legal or ethical violations are significantly magnified when sensitive information is recognized as a class of data within the broader category of personal data. In other words, it is increasingly necessary to acknowledge the distinction between sensitive and non-sensitive personal information.

In an organizational setting, it becomes readily apparent that privacy concerns are highly influenced by the employee's assumption that sensitive information will not be shared in an inappropriate manner. Data about individuals would not be collected or mined if organizations did not have an interest in using the information to make decisions about the individuals or situations (Johnson, 2001). The concept of a psychological contract is a useful tool for understanding dynamic and contextual character of privacy concerns (Argyris, 1960).

First introduced in the 1960s, the term psychological contract was used to characterize mutual expectations between the employer and employee (Argyris, 1960; Schein, 1965). The construct has expanded to represent the employment relationship, premised on employees' and employers' beliefs regarding their relationship. Psychological contracts impact many employment outcomes, including employee contribution, retention, and turnover, based on the content of the contract and the degree to which the expectations by both parties are met (Robinson & Rousseau, 1994; Turnley & Feldman, 1999).

As a byproduct of employment, employees presume they are accepting a minimal risk when personal information is collected and retained by the firm. One mechanism for data collection is through the use of workplace surveillance (Introna, 2003; Johnson, 2001; Weckert & Adeney, 1997). In this type of data collection, the employee's behavior is monitored and categorized for use against the employee in situations where the employer believes this is appropriate. E-mail monitoring is oftentimes considered another form of privacy invasion comparable to reading an individual's postal mail or listening to a telephone conversation (Sipior & Ward, 1995; Weckert & Adeney, 1997). The availability of advanced computer technology enables employers to gather personal data on current and prospective employees including reference checks, credit histories, motor vehicle histories, and telephone usage patterns (Brown, 2000). Culnan (1993) found that the issue of control was important in an exploratory study on consumers' attitudes toward secondary information use. In particular, Culnan (1993) suggests that individuals who are less sensitive toward the secondary use of their personal information are more likely to shop by mail.

However, over time as employees become more secure in their status, they are likely to develop a greater awareness of potential compromises associated with the loss of privacy (Townsend & Bennet, 2003). As a consequence, they are forced to place increasing reliance on their own personally developed standards for sharing person specific information as opposed to sole reliance on the standards and systems developed by the firm.

These person specific standards for deciding what information to share on an individual level can collectively be labeled as privacy sensitivity. This concept of privacy sensitivity can be characterized as being roughly equivalent to individual variations in sensitivity to allergens or toxins. For example, new data suggests that the metal beryllium, an essential raw material in thousands of new electronic products, will trigger a massive attack by the immune system, in some people, at exposures as low as a few millionths of a gram. In other cases, however, workers appear to be able to tolerate dramatically higher levels of exposure (Carey, 2005). Based on this analogy, privacy sensitivity can be differentiated by degree, such that the higher the degree of apparent sensitivity, the greater the negative consequences for violation. Given that privacy of personal data is ubiquitous in today's business environment, the smallest violations are likely to cause behavioral reactions based on the individual's degree of privacy sensitivity.

In a similar manner, there are an almost unlimited number of opportunities for a privacy sensitivity response. For example, in 1996, President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA). This complex, expensive, and aggressively debated law gained wide voter support shortly after the general public became sensitized to privacy concerns regarding the use of personal medical information.

Given the growing number of reasons for privacy sensitivity, it is logical to conclude that there will be significant variations in user willingness to voluntarily share data. This willingness to share information is important on two levels. First, personal perceptions regarding the solicitor's right to know the requested information are involved. For example, in recent years, companies have invested a significant amount of money and effort to create knowledge management systems. At some level, these systems are designed to capture job knowledge from the employee in order to place the information under the control and at the disposal of the company as a whole. In practical terms, this practice is analogous to turn of the century efforts to capture the keyboarding skills of piano players to create the first player pianos and to contemporary modern synthesizers that sample and reproduce the work of accomplished musicians. Employees have a vested interest in withholding knowledge out of fear that their economic value and job security will be imperiled. As knowledge management technologies become more adept at capturing tacit knowledge of the firm's best employees, heightened levels of privacy sensitivity are likely to occur.

Second, as suggested, greater levels of privacy sensitivity can be expected to result in higher levels of withheld information. However, no less important is the related challenge of information accuracy that has long been a concern of the information systems community. The frequency, targeting, and importance of employee surveys offer an example and they have evolved due to the availability of Internet technologies. Information collected via these Internet-based surveyed may serve as input for important managerial decisions such as: (1) determining whether or not enter or leave a market; (2) valuing a firm to investors or potential suitors; or, (3) defending the firm in the event of a civil rights claim. In other words, their utility and value is dependent upon the accuracy of voluntary employee responses and the interpretation resulting from the data entry. Unfortunately, accuracy of employee, customer, or patient data will be compromised unless individual variations in privacy sensitivity are taken into account. These observations lead to two propositions:

P1: The higher the individual's level of privacy sensitivity, the greater the likelihood that the personal data submitted will be covertly or overtly inaccurate.

P2: The higher the individual's level of privacy sensitivity, the greater the likelihood that personal data will be withheld.

TECHNOLOGY TRUST

Technology trust is an individual's willingness to be vulnerable to a technology based on the individual's expectations that the technology is predictable, reliable and useful (Lippert, 2001; Lippert, in press). This form of trust is unique because the object of trust is an inanimate artifact rather than another individual and represents a different form of trust than interpersonal trust, trust between two human beings (Lippert, in press). Interpersonal trust represents a bidirectional assessment by each person toward the person in the trust situation. Technology trust represents a unidirectional assessment of trust by the individual toward the technology and cannot, in any situation, be a bi-directional assessment of trust. The object of trust in interpersonal trust is another individual; the object of trust in technology trust is a technology. These are key differences between the two forms of trust.

In technology trust, the trust assessment is formed by an individual toward the technology and results from the individual's attitude based on past experiences and expectations of how the system will function in the future (Lippert, in press; Lippert & Davis, 2006; Lippert & Forman, 2006). The individual makes the assumption that data entered into the system will be accurately maintained and available for later retrieval. This evaluation of the level of trust he has toward the technology is made by the individual every time personal information is incorporated into the organizational database. Understanding how individuals learn to trust in technology is becoming more important as individual and organizational dependence on information systems develops and matures (Jones, Wilikens, Morris, & Masera, 2000).

Sharing sensitive personal information requires a significant degree of trust and expresses a willingness to assume the risks associated with permitting personal information to become resident within a corporate database. This willingness to take a risk is a common characteristic of all trust situations (Costigan, Ilter, & Berman, 1998). In order for trust to exist, past experiences are needed to establish familiarity with the situation and lessen the level of perceived risk (Johnson-George & Swap, 1982). Lippert and Swiercz (2005) state that in order for trust to exist, past experiences are needed to establish familiarity. In other words, an individual's familiarity with a given technology coupled with a sense of trust that the organization will use the information appropriately, combines to shape the individual's attitude and subsequent behavior. Willingness to share personal information via the Internet assumes a level of risk (Lippert & Swiercz, 2005). An individual's willingness to share person information can be enhanced and nurtured through the establishment of a trusting relationship (Chen & Rea, 2004).

Technology trust is particularly applicable to situations involving sharing personal data via the Internet because the individual's interaction with the technology is a classic man-machine interaction. In a fairly typical Internet interaction scenario, the user is invited to access a database and interact with it directly, unmediated by human interaction. An individual's personally developed standards of technology trust will influence the character and flavor of the interaction. Thus, it is reasonable to argue that individuals will share person specific information with the organization consistent with a personally developed standard of technology trust. And further, individuals with more favorable perceptions of technology trust will share person specific information to the degree that they believe in the utility and security of the Internet technology.

P3: The higher the individual's trust in the utility of the technology, the less the likelihood that personal data will be shared.

P4: The higher the individual's trust in the security of the technology, the less the likelihood that personal data will be shared.

CONCLUSION

In this paper, we argued that a user's willingness to share sensitive information on a voluntary basis is an area of important concern. We suggest that that the voluntary dimension of data sharing is important as individuals make purposeful judgments regarding the sharing of their person specific information. Further, we propose that users will vary in terms of their privacy sensitivity and their level of technology trust. And a consequence, these factors are likely to influence an individual's willingness to share sensitive person specific data. As the Internet has matured, so have users; they are no longer passive actors in the data collection process. As such, developing a richer understanding of the interaction between user behavior, data collection practices, and information usage is essential to building sustainable internet mediated transactions.

The model presented in this paper is significant for both practicing mangers and academic researchers. Both communities will find the model valuable because it provides a roadmap for understanding the interaction between user volitional behavior and the success of a critical technology. The study of personal data sharing is important for information systems scholars because understand the sources of user resistance to new technologies can aid in their future development.

As pointed out in this paper, modern information system designs have now made it possible of convert what used to be an administrative byproduct – user data – into a tangible competitive resource. The model presented in this paper is an early, but nonetheless important, contribution to understanding the many process and quality factors that have an impact on system success. In particular, it calls attention to variables absent from most discussions of system success regarding the voluntary dimension of data sharing. To date, most web designers have collected data on the basis of two assumptions: (1) that the end user had little concern about the type and scope of information collected; and, (2) that the end users could be counted upon to provide the requested information in a timely and truthful manner. Both of these assumptions are being challenged by changes in the technological and competitive landscape. Coincident with the firm's discovery of the value of user data is a growing recognition by individuals that they have an interest in making purposeful judgments regarding the sharing of their person specific information.

As individuals continue to use information technologies for a range of internet friendly tasks, the challenge remains concerning the protection of sensitive private information from inappropriate use or abuse. An individual's privacy sensitivity threshold coupled with the degree of trust they place in the technology will have a direct effect upon the employee's willingness to share sensitive information on a voluntary basis. As such, we suggest that awareness and attentiveness to variations in privacy sensitivity and technology trust will be increasing important factors in the design and deployment of web-based systems.

REFERENCES

Adams, D., Todd, P., & Nelson, R. (1993). A Comparative Evaluation of the Impact of Electronic Mail and Voice Mail on Organizational Communication. *Information and Management 24,* 9-21.

Argyle, M., & Dean, J. (1965). Eye Contact, Distance and Affiliation. *Sociometry 28,* 289-304.

Argyris, C. (1960). *Understanding Organizational Behavior.* Homewood, IL: Dorsey Press.

Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct (1992). Retrieved December 3, 2005, from http://www.ccsr.cse.dmu.ac.uk/resources/professionalism/ codes/paper/acm.pdf.

Bland-Acosta, B.A. (1988). Developing an HRIS Privacy Policy. *HR Magazine 33*(7), 52-58.

Britz, J.J. (1999). Ethical Guidelines for Meeting the Challenges of the Information Age. In L.J. Pourciau (Ed.), *Ethics and Electronic Information in the 21st Century*, 9-28. West Lafayette, Indiana: Purdue University Press.

Brown, W.S. (2000). Ontological Security, Existential Anxiety and Workplace Privacy. *Journal of Business Ethics 23*(1), 61-65.

Buchanan, T., Paine, C., Joinson, A.N., & Reips, U.D. (2007). Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology 58*(2), 157-165.

Carey, J. (May 2, 2005). Beryllium exposure: The "unrecognized epidemic". Retrieved May 2, 2005, from http://www.businessweek.com/cgi-bin/register/archiveSearch.cgi?h=05_18/b3931048_mz 011.htm.

Carlson, J. (1995). Channel Expansion Theory: A Dynamic View of Media and Information Richness Perceptions. *Unpublished Doctoral Dissertation*, Florida State University, Tallahassee.

Carlson, J., & Zmud, R.W. (1994). Channel Expansion Theory: A Dynamic View of Media and Information Richness Perceptions. *The Academy of Management Best Papers Proceedings* (D.P. Moore, ed.), 280-284.

Carlson, J., & Zmud, R.W. (1999). Channel expansion Theory and the Experiential Nature of Media Richness Perceptions. *The Academy of Management Journal 42*(2), 153-170.

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing 19*(1), 7-20.

Chen, K., & Rea, A.I., Jr. (2004). Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *The Journal of Computer Information Systems 44*(4), 85-92.

Coase, R.H. (1937). The Nature of the Firm. *Economica 4*, 386-405.

Costigan, R.D., Ilter, S.S., & Berman, J.J. (1998). A Multi-Dimensional Study of Trust in Organizations. *Journal of Managerial Issues 10*(3), 303-317.

Culnan, M.J. (1993). How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly 17*(3), 341-363.

Daft, R.L., & Lengel, R.H. (1986). Organizational Information Requirements, Media Richness and Structural Design. *Management Science 32*(5), 554-571.

Deutsch, M. (1960). The Effect of Motivational Orientation upon Trust and Suspicion. *Human Relations 13,* 122-139.

Donovan, D.C. (1995). Computer-Mediated Communication and the Basic Speech Course [Electronic version]. *Interpersonal Computing and Technology: An Electronic Journal for the 21st Century 3*(3), 32-53.

Earp, J.B., Anton, A.I., Aiman-Smith, L., & Stufflebeam, W.H. (2005). Examining Internet Privacy Policies within the Context of User Privacy Values. *IEEE Transactions on Engineering Management 52*(2), 227-237.

Ebersole, S. (1999). A Matrix of Theories for Interactive Computer-Mediated Communication. Retrieved July 14, 1999, from http://www.uscolo.edu/ebersole/333/matrix.html.

Eder, P. (1994). Privacy on Parade: Your Secrets on Sale. *Futurist 28*, 38-42.

Elgesiem, D. (1996). Privacy, Respect for Persons, and Risk. In C. Ess (Ed.), *Philosophical Perspectives on Computer-Mediated Communication*, 45-66, Albany, New York: State University of New York Press.

Email Costs Business over £1 Billion Per Year. (19 May 2005). Retrieved May 23, 2005, from http://www.theinquirer.net/?article=23332.

Federal Trade Commission. (2005). ID theft home. Welcome to the Federal Trade Commission: Your National Resource For Identity Theft. Retrieved May 23, 2005, from http://www.comsumer.gov/ idtheft/.

Federal Trade Commission. (1998). Privacy Online: A Report to Congress. *Internet Research.* Retrieved February 20, 2007, from http://www.ftc.gov.

Fulk, J. (1993). Social Construction of Communication Technology. *The Academy of Management Journal 36*(5), 921-950.

Fulk, J., Steinfield, C.W., Schmitz, J.A., & Power, J.G. (1987). A Social Information Processing Model of Media Use in Organizations. *Communication Research 14*(5), 529-552.

Gavison, R. (1995). Privacy and Limits of Law. In D.G. Johnson & H. Nissenbaum (Eds.), *Computers, Ethics & Social Values*, 322-351, Upper Saddle River, New Jersey: Prentice Hall.

Golden, P., Beauclair, R., & Sussman, L. (1992). Factors Affecting Electronic Mail Use. *Computers in Human Behavior 8,* 297-311.

Greenspan, R. (June 11, 2004). eBay Tops For Trust Among Consumers. Retrieved May 23, 2005, from http://www.clickz.com/stats/sectors/retailing/article.php/3367181.

Hallerman, D. (2005). Email: Turning up the Volume, eMarketer. Retrieved May 19, 2005 from http://www.imediaconnection.com/content/5630.asp.

Hallowell, E.M. (1999). The Human Moment at Work. *Harvard Business Review 77*(1), 58-66.

Hamilton, A.A. (2005). Development and Validation of a Methodology to Assess Privacy Sensitivity. *Doctoral Dissertation*. The George Washington University, Washington, D.C.

Harrison, T. (2003). Why Trust Is Important In Customer Relationships And How To Achieve It. *Journal of Financial Services Marketing 7*(3), 206-209.

Internet Usage Statistics – The Big Picture. World Internet Users and Population Stats. (n.d.). Retrieved May 23, 2005 from http://www.internetworldstats.com/stats.htm.

Introna, L. (2003). Workplace Surveillance 'Is' Unethical and Unfair. *Surveillance & Society 1*(2), 210-216.

Johnson, D.G. (2001). *Computer Ethics*, 3rd ed. Upper Saddle River, New Jersey: Prentice Hall.

Johnson-George, C., & Swap, W.C. (1982). Measurement of Specific Interpersonal Trust-Construction and Validation of a Scale to Access Trust in a Specific Other. *Journal of Personality and Social Psychology 43*(12), 1306-1317.

Jones, S., Wilikens, M., Morris, P., & Masera, M. (2000). Trust Requirements in e-Business. *Communications of the ACM 43*(12), 80-87.

Kiesler, S. (1986). The Hidden Messages in Computer Networks. *Harvard Business Review 64*(1), 46-58.

Kiesler, S., Zubrow, D., Moses, A., & Geller, V. (1985). Affect in Computer-Mediated Communication: An Experiment on Synchronous Terminal-To-Terminal Discussion. *Human-Computer Interaction 1*, 77-104.

Lippert, S.K. (In press). Investigating Post-Adoption Utilization: An Examination Into The Role of Inter-Organizational and Technology Trust. *IEEE Transactions on Engineering Management*.

Lippert, S.K. (2001). An Exploratory Study into the Relevance of Trust in the Context of Information Systems Technology. *Doctoral Dissertation*. The George Washington University, Washington, D.C.

Lippert, S.K. & Davis, M. (2006). A Conceptual Model Integrating Trust into Planned Change Activities to Enhance Technology Adoption Behavior. *Journal of Information Science 32*(5), 434-448.

Lippert, S.K. & Forman, H. (2006). A Supply Chain Study of Technology Trust and Antecedents to Technology Internalization Consequences. *International Journal of Physical Distribution & Logistics Management 36*(4), 271-288.

Lippert, S.K. & Swiercz, P.M. (2005). Human Resource Information Systems (HRIS) and Technology Trust. *Journal of Information Science 31*(5), 340-353.

Marchewka, J.T., Liu, C., & Petersen, C.G. (2003). Perceptions of Unsolicited Electronic Mail or Spam. *Journal of International Technology and Information Management 12*(1), 77-92.

Markus, M.L. (1987). Toward a Critical Mass Theory of Interactive Media: Universal Access, Interdependence, and Diffusion. *Communication Research 14*(5), 491-511.

McAllister, D.J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal 38*(1), 24-59.

McCarthy, R.V., Aronson, J.E., & Petrausch, R. (2004). Building Relationships That Last: Integrating Public Relations Into Web Design. *Journal of International Technology and Information Management 13*(1), 1-12.

Mollick, J.S. & Pearson, J.M. (2006). Do Information Privacy Concerns Affect Students' Feelings of Alienation? *Journal of International Technology and Information Management 15*(1), 24-32.

Nissenbaum, H. (2001). Toward an Approach to Privacy in Public: Challenges of Information Technology. In R.A. Spinello & H.T. Tavani (Eds.), *Readings in Cyberethics*, 392-403, Sudbury, MA: Jones and Bartlett.

Online Travel Market Largely Avoids Economic Slowdown (April 23, 2001). Retrieved on May 23, 2005, from http://www.skymarkgroup.com/industry-news-travel.html#slowdown.

Online Travel Spending Surpasses $1 Billion In January (March 20, 2001). Retrieved on May 23, 2005, from http://www.skymarkgroup.com/industry-news-travel.html#surpass.

Phillips, S.R. (1989). Electronic Persuasion: The Uses of Electronic Mail for Interpersonal Influence In Organizations. *Unpublished Doctoral Dissertation*, University of Southern California.

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics 62*(3), 221-235.

Rice, R.E. (1992a). Task Analyzability, Use of New Media, and Effectiveness: A Multi-Site Exploration of Media Richness. *Organization Science 3*(4), 475-500.

Rice, R.E. (1992b). Issues and Concepts in Research on Computer-Mediated Communication Systems. In M. Lea (Ed.), *Contexts of Computer-Mediated Communication*, 436-476. New York: Harvester.

Rice, R.E., & Love, G. (1987). Electronic-Emotion: Social-Emotional Content in a Computer-Mediated Communication Network. *Communication Research 14*(1), 85-108.

Robinson, S.L., & Rousseau, D.M. (1994). Violating the Psychological Contract: Not the Exception but the Norm. *Journal of Organizational Behavior 15*(3), 245–259.

Ryker, R., Khurrum, M. & Bhutta, S. (2005). Online Privacy Policies: An Assessment of the Fortune Global 100. *Journal of International Technology and Information Management 14*(1), 24-32.

Schein, E. (1965). *Organizational* P*sychology.* Englewood Cliffs, NJ: Prentice Hall.

Severson, R.J. (1997). *The Principles of Information Ethics*. London: M.E. Sharpe.

Sheehan, K.B., & Hoy, M.G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond To Privacy Concerns. *Journal of Advertising 28*(3), 37-51.

Short, J., Williams, E., & Christie, B. (1976). *The Social Psychology of Telecommunications*. London: John Wiley.

Sipior, J.C. & Ward, B.T. (1995). The Ethical and Legal Quandary of Email Privacy. *Communications of the ACM 38*(12), 48-54.

Spinello, R.A. (2000). *Cyberethics: Morality and Law in Cyberspace*. London: Jones & Bartlett.

Stalder, F. (2002). Privacy is Not the Antidote to Surveillance. *Surveillance & Society 1*(1), 120-124.

Straub, D.W., & Collins, R.W. (1990). Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy. *MIS Quarterly 14*(2), 143-156.

The Effects of Identity Theft. (n.d.). Retrieved May 23, 2005, from http://www.identity-theft-help.us/the.effects.of.identity.theft.htm.

Townsend, A.M., & Bennett, J.T. (2003). Information Technology and Employment Law: Challenges in an Evolving Workplace. *Journal of Labor Research 24*(3), 425-435.

Trevino, L.K., Lengel, R.H., & Daft, R.L. (1987). Media Symbolism, Media Richness, and Media Choice in Organizations. *Communication Research 14*(5), 553-574.

Turnley, W.H., & Feldman, D.C. (1999). The Impact of Psychological Contract Violations on Exit, Voice, Loyalty, and Neglect. *Human Relations 52*(7), 895–922.

Velasquez, M. (1998). *Business Ethics: Concepts and Cases*, 4th ed. Upper Saddle River, New Jersey: Prentice Hall.

Walther, J.B. (1992). Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective. *Communication Research 19*(1), 52-90.

Warren, S.D., & Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review 4*(5), 193-220.

Weckert, J. & Adeney, D. (1997): *Computer and Information Ethics*. London: Greenwood Press.

Yates, J., & Orlikowski, W. (1992). Genres of Organizational Communication: A Structurational Approach to Studying Communication and Media. *The Academy of Management Review 17*(2), 299-326.