2005

The Impact of Privacy Concerns on the Use of Information Technologies: A Preliminary Conceptual Model

Sharen Bakke
Kent State University, sbakke@bsa3.kent.edu

Robert Faley
Kent State University, rfaley@bsa3.kent.edu

Alan Brandyberry
Kent State University, abrandyb@kent.edu

Marvin Troutt
Kent State University, mtroutt@bsa3.kent.edu

The Impact of Privacy Concerns on the Use of Information Technologies: A Preliminary Conceptual Model

Sharen Bakke
Kent State University
sbakke@bsa3.kent.edu

Robert Faley
Kent State University
rfaley@bsa3.kent.edu

Alan Brandyberry
Kent State University
abrandyb@kent.edu

Marvin Troutt
Kent State University
mtroutt@bsa3.kent.edu

ABSTRACT

Privacy-related concerns are likely to be important to the successful adoption and implementation of new information technologies. While personal concerns about privacy (especially information privacy) are well documented in the literature, research on the specific source of these concerns is limited. In particular, there is a dearth of information system's research that focuses on the characteristics of information technologies that positively or negatively influence individual privacy perceptions. The objective of this paper is to present a preliminary conceptual model that identifies the privacy-related dimensions of information technologies that influence individual privacy perceptions. This knowledge should help organizations better determine the extent to which these new technologies are likely to be adopted by end users who perceive these technologies as threats to their privacy.

Keywords

Preliminary conceptual model, privacy, perceptions, technology characteristics, technology adoption

INTRODUCTION

The IT adoption process consists of a series of actions and choices during which an individual evaluates a new technology and decides whether to incorporate the technology into ongoing practice. Individual perceptions of the relevant characteristics of the technology are important determinants that affect whether the technology is successfully adopted. Those individuals who form unfavorable impressions, especially in the evaluation and trial phase of the adoption process, are less likely to adopt and use the technology (Rogers, 1962).

Failure to successfully adopt information technologies can have far-reaching consequences. For example, employees who resist using information technologies can form pockets of resistance that may cause co-workers to also resist. When a potentially valuable information technology is resisted or not adopted, the direct and indirect costs to the organization can be considerable (Agarwal & Prasad, 1998; Burgelman, Maidique and Wheelwright, 2001; Davis, Bagozzi and Warshaw, 1989; Taylor & Todd, 1995).

Advances in technology cultivate new sensibilities and vulnerabilities toward invasions of privacy. Individuals are becoming "privacy assertive": they ask to be removed from marketing databases, decline to register at e-commerce sites, and avoid web sites with dubious privacy practices (EPIC, 2004). This assertive behavior is detrimental to IT adoption.

The objective of this paper is to present a conceptual model that identifies the privacy-related dimensions of information technologies that influence individual privacy perceptions. This will be accomplished in two parts. The first part of the paper reviews the general and IT-related privacy literatures. The second part describes a conceptual model that includes the important dimensions that influence IT-related privacy concerns.

LITERATURE REVIEW

Although no universally accepted definition of privacy exists (Schoeman, 1984), the consensus among researchers is that privacy is the process of controlling personal transactions through the control over boundaries between self and "other" (where "other" could be another individual, group, or society) (Altman, 1975; Kelvin, 1973). Thus, the notion of control is inherent in all definitions of privacy (Fusilier & Hoyer, 1980; Stone, Gueutal, Gardner and McClure, 1983; Tolchinsky, McCuddy, Adams, Ganster, Woodman and Fromkin, 1981)

Privacy is most often described as the combination of three control-related perspectives (Stone & Stone, 1990): 1) individual control over disclosure of personal information (Johnson, 1974; Shils, 1966; Westin, 1967); 2) individual control over regulation of interactions with others (Altman, 1975; Derlega & Chaikin, 1977) and 3) freedom from control by others (Kelvin, 1973).

According to the first perspective, privacy is achieved when individuals are able to manage or control information about themselves and the subsequent impressions that others form about them based on that information (Stone & Stone, 1990). Shils (1966) described this as "information management" or the control over the possession and flow of information. As noted by Marshall (1972), individual privacy is threatened when others have access to personal information that the individual does not want disclosed.

The second privacy perspective, interaction management, refers to the control individuals perceive they have over the amount of contact they have with others. This emphasizes the notion of boundary control, of opening and closing of the self to others, of freedom of choice and options regarding self-accessibility to others (Altman, 1975). A network of behavioral mechanisms such as territoriality, personal space and various other verbal and nonverbal behaviors are employed by individuals to manage their level of social interaction (Altman, 1975; Stone & Stone, 1990). Westin (1967), for example, describes interaction management as the "voluntary and temporary withdrawal of a person from the general society, through physical or psychological means, either in a state of solitude or small group intimacy or when among other large groups, in a condition of anonymity or reserve" (p. 6).

The third major privacy perspective refers to the degree to which individuals perceive they are free from the influence or control of others. According to this perspective, when other individuals have information another individual wants kept private, they are able to control the individual. Thus, for example, individuals use impression management techniques to insolate themselves from unwanted invasions of their privacy by manipulating their self impressions (Stone & Stone, 1990). Unfortunately, there is no relevant counterpart in the IT literature for this perspective, and it is not be included in the proposed model described below.

Culnan (1993) first addressed information privacy concerns in the IT world in an empirical study dealing with consumer attitudes toward secondary information use. Control emerged as a clear theme. Individuals' concerns about organizational practices were the focus of Smith, Milberg and Burke's work (1996). They developed a multidimensional scale consisting of four information privacy concerns: collection, unauthorized secondary use, improper access and errors. A refinement of this model by Stewart and Segars (2002) resulted in a more parsimonious second order model. Malhorta, Kim and Agarwal (2004) extended this model in the development of the IUIPC scale that represents privacy concerns of online consumers.

CONCEPTUAL MODEL OF IT-RELATED PRIVACY

The conceptual model described below focuses on the impact of information technologies on individual privacy in general. It consists of three dimensions: information management, interaction management, and organizational technology management.

Information Management

The primary source of the characteristics of the information management dimension of the IT-related privacy model illustrated below is the "Code of Fair Information Practices" as described in the U.S. Department of Health, Education and Welfare study (HEW, 1973), the Privacy Protection Study Commission (PPSC, 1977), the Organization of Economic Cooperation and Development (OECD) guidelines for the protection of personal data (OECD, 1980) and the Federal Trade Commission 's Core Principles of the Fair Information Practices (FTC, 2000). The HEW's Code of Fair Information Practices requires that individuals are: 1) aware their personal data is being collected, 2) informed of what information is collected and how it will be used, 3) able to prevent information obtained for one purpose to be used for another reason, 4) able to correct or amend their personal information records, and 5) assured that organizations creating, maintaining, using or

disseminating personal data records attest the reliability of the data and take precautions to prevent misuses of the data. The OECD started with these five HEW practices and extended the guidelines to include data controllers' openness and accountability. The core principles of the FTC guidelines, governing commercial web sites include: 1) notice of personal information collected and its use, 2) choice regarding secondary uses of the information, 3) access enabling individuals to view the data about themselves the organization has collected and to contest the data's accuracy and completeness, and 4) security which requires the organization to take reasonable steps to ensure personal information is secure during transmission and storage. These guidelines emerged as a result of public awareness and consumer concerns about online privacy.

Thus, information management focuses primarily on the characteristics of information technologies that enable individuals to control the collection and handling of their personal information. Some of the characteristics of information management include: 1) who can receive/retrieve data, 2) what data can be collected, 3) the ability to verify and modify data, 4) under what circumstances data can be collected, and 5) how data can be collected.

When individuals can specify who can receive or retrieve their personal information, they feel a greater sense of control. This can be accomplished, for example, by information technologies that allow individuals to select a check box to indicate the parties who can receive their personal information. As such, this characteristic addresses the secondary use and choice concerns identified in the fair information practices guidelines (FTC, 2000; HEW, 1973; PPSC, 1977) where personal information collected for one purpose is subsequently used for a different purpose (Culnan, 1993; Smith et al., 1996). When individuals can choose the information they wish to disclose they have a greater feeling of control; only the information they wish to reveal is made available. As noted by Culnan & Armstrong (1999) and Smith et al. (1996), individuals who have the opportunity to verify and modify personal information perceive a lesser threat to their privacy. The importance of this characteristic is evident by the fact that it is included in the core principles of the fair information practices developed by HEW, OECD, and the FTC.

Specifying under what circumstances information can be collected allows individuals to control the timing and/or context of data collection. Consider the situation where location information emanating from a location-tracking device can be collected only during normal work hours. Moreover, permitting individuals to choose how their data can be collected provides them with an opportunity to remain anonymous. For example, when data is collected in aggregate there is no information that identifies specific individuals. Thus, information management focuses on individual control over those characteristics that affect access to personal information.

Interaction Management

The definition and characteristics of interaction management were derived from an examination and analysis of the general privacy literature (Altman, 1975; Petronio, 2002; Stone & Stone, 1990) and focus on issues related to control over an individual's personal space. This is the least studied privacy dimension in IS research. This omission arises from the failure to recognize privacy as the control that individuals desire over the interactions that take place in that area (i.e. that "space" individuals consider their own).

According to the general privacy literature, individuals seek varying optimal levels of social interaction; they need to maintain some optimum balance between seclusion and interaction (Altman, 1975; Petronio, 2002). When more social contact occurs than is desired an invasion of individual privacy occurs. Examples include advertising messages that pop up on computer screens, audible beeps from cellular telephones, telephone calls from telemarketers, and unwanted email solicitations (e.g. spam).

Six characteristics describe interaction management: 1) proactive – who can access, 2) proactive – when can access, 3) proactive - how can access, 4) reactive – who can access, 5) reactive - when can access and 6) reactive – how can access. The first three characteristics are considered proactive because they are specified before an interaction occurs. To control social interactions, individuals can specify those individuals who have access (i.e. family members, bosses), when they have access and how they can access. For example, a university professor has office hours Tuesdays and Thursdays from 2:00 – 4:00 pm. Every Tuesday and Thursday between 2:00 and 4:00 students may access the professor, in person. Reactive characteristics refer to those that focus on controlling entry into personal space at the actual time of engagement. For example, an individual in an online chat room receives a request to join the online banter, but has the option to refuse the request on a person-by-person basis. Choosing when and how interactions are arranged (reactively) work similarly.

Organizational Technology Management

Organizational technology management is a new privacy dimension that consists of those privacy-related IT characteristics that are not directly controllable by individuals but can be influenced by the indirect pressures placed on organizations by

end-users. For example, passwords enable individuals to verify who they claim they are before they access information technology. However, individuals cannot control this characteristic; the information technology is either equipped with a security system or it is not. Individuals, though, may exert pressure on those organizations to install authentication procedures by not using technologies that lack this feature.

These characteristics were obtained, in part, from recommendations for IT security products appearing in IT security practitioner journals and from interviews with local IT security professionals (Grance, Stevens and Myers, 2003). Several characteristics honor obligations identified in the Code of Fair Information Practices and the OECD guidelines. For example, the security safeguard principle of the OECD guidelines is addressed by the unauthorized and authorized access notifications, data deletion, storage and integrity, and user verification characteristics.

Eleven IT characteristics describe organizational technology management: 1) data integrity, 2) data circulation, 3) privacy policy adherence, 4) unauthorized access notification, 5) data deletion, 6) user verification, 7) security assurance, 8) authorized access notification, 9) delivery confirmation, 10) automatic shutdown and 11) data storage. Data integrity refers to the fact that the information entered is the same as the information received. Data circulation refers to the process through which any information is circulated to recipients. Privacy policy adherence refers to the extent to which policies mandated by government agencies or developed and implemented by organizations to control how personal information can be collected and managed are followed. Unauthorized access notification involves a compilation of those individuals who attempt to use the technology but are not allowed. Data deletion refers to the assurance that deleted information is actually non-recoverable. User verification is the process of ensuring the individual attempting to use the information technology has authorization and is allowed access. The security assurance characteristic assures the user that the IT provider has adequate security procedures in place. Authorized access notification compiles a list of others who have accessed an individual's personal information and when they accessed it. The delivery confirmation characteristic ensures the information send by an individual was received by the intended party. The automatic shutdown characteristic ensures no unauthorized users can access the information technology when the authorized user has left the application. Finally, data storage refers to the length of time personal data is stored.

These dimensions and characteristics are illustrated in Figure 1. The construct under study, IT-related privacy-invasiveness perceptions, is an aggregate of the three dimensions described above: information management, interaction management, and organizational technology management. Information Management focuses on individual control over personal information, Interaction Management focuses on individual control over personal space, and Organizational Technology Management individual control over technology issues implemented by the organization.

Summary

The general privacy literature suggests that individuals desire to have some level of control over when, how and to what extent their personal information is communicated to others (Westin, 1967). It is not surprising that the IS privacy literature has focused on these concerns as information technologies have become the primary vehicles for managing all kinds of information, much of it personal. As a result, individuals are very likely to perceive that their control over personal information has diminished. This is especially the case as information technologies become even more sophisticated.

The conceptual model of IT-related privacy described above expands the existing IT literature by including a new privacy dimension, interaction management. The model also explicitly acknowledges the direct influence organizations have over the privacy-related concerns of end-users through the dimension of organizational technology management. The measurement instrument developed based on this model (called the Privacy Invasiveness Perception Scale - PIPS) is in the process of being validated.

There are some very practical uses to which the measurement instrument developed based on the conceptual can be put. For example, we believe that it can be adapted to help organizations better determine the privacy-related impediments to the adoption of information technologies by end users before organizations select a technology. It could also be used to determine the characteristics of information technologies already in use that are impediments to more widespread adoption.

Organizations have choices over which information technologies they can incorporate into their infrastructures. Information provided by the PIPS will enable organizations to choose information technologies that have a greatest likelihood of being adopted because they minimize resistance based on individual privacy concerns.

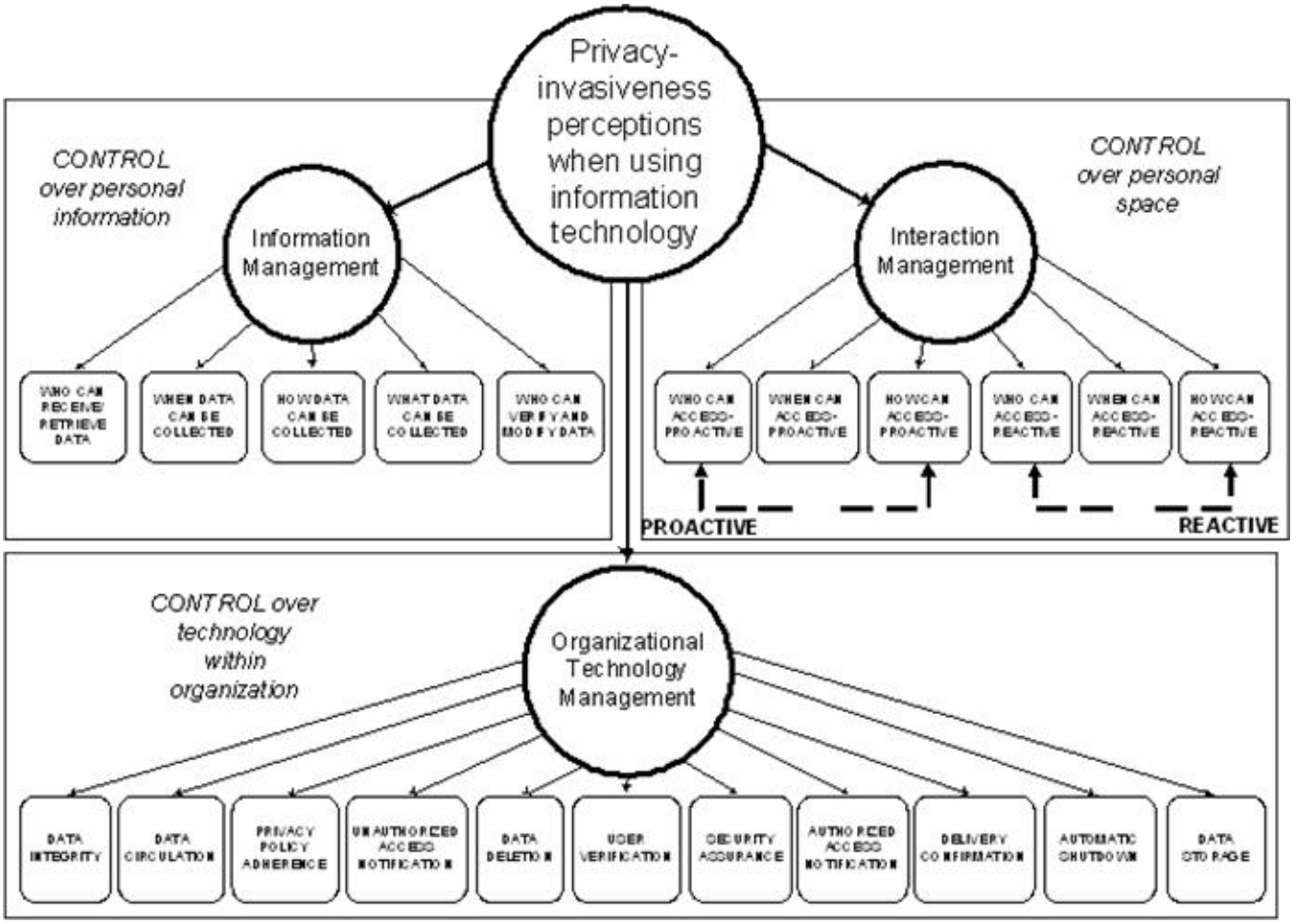

Figure 1: Conceptual model for the privacy-invasiveness perceptions when using information technology construct

REFERENCES

1. Agarwal, R. and J. Prasad (1998). "A conceptual and operational definition of personal innovativeness in the domain of information technology." Information Systems Research 9(2): 204 - 215.
2. Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, California, Brooks/Cole Publishing Company.
3. Burgelman, R. A., M. A. Maidique, et al. (2001). Strategic management of technology and innovation. Boston, McGraw-Hill.
4. Culnan, M. J. (1993). ""How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use." MIS Quarterly September: 341 - 363.
5. Culnan, M. J. and P. K. Armstrong (1999). "Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation." Organization Science 10(1): 104 - 115.
6. Davis, F. D., R. P. Bagozzi, et al. (1989). "User Acceptance of Computer-Technology - a Comparison of Two Theoretical-Models." Management Science 35(8): 982-1003.
7. Derlega, V. J. and A. L. Chaikin (1977). "Privacy and self-disclosure in social relationships." Journal of Social Issues 33(3): 102 - 115.
8. EPIC (2004). Public Opinion on Privacy - Electronic Privacy Information Center. Retrieved: October 18, 2004 from http://www.epic.org/privacy/survey/. 2004.
9. FTC (2000). "Fair information practices in the electronic marketplace."
10. Fusilier, M. R. and W. D. Hoyer (1980). "Variables affecting perceptions of invasion of privacy in a personnel selection situation." Journal of Applied Psychology 65(5): 623 - 626.

11. Grance, T., M. Stevens, et al. (2003). Guide to selecting information technology security products. Recommendations of the National Institute of Standards and Technology. Gaithersburg, MD, Technology Administration, U.S. Department of Commerce: 65.
12. HEW (1973). Records, computers, and the rights of citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, D. C., U.S. Department of Health, Education, and Welfare.
13. Johnson, C., Ed. (1974). Privacy as personal control. Man-environment interactions: Evaluations and applications. Washington, D.C., Environmental Design Research.
14. Kelvin, P. (1973). "A social-psychological examination of privacy." British Journal of Social Clinical psychology 12: 248 - 261.
15. Malhotra, N. K., S. S. Kim, et al. (2004). "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model." Information Systems Research 15(4): 336 - 355.
16. OECD (1980). OECD guidelines on the protection of privacy and transborder flows of personal data. Retrieved: April 24, 2005 from http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, Organisation for Economic Co-operation and Development.
17. Petronio, S. (2002). Boundaries of privacy: Dialectics of disclosure. Albany, NY, State University of New York Press.
18. PPSC (1977). Personal privacy in an information society: Report of the Privacy Protection Study Commission. Washington, D.C., U.S. Government Printing Office.
19. Rogers, E. M. (1962). Diffusion of Innovations. New York, The Free Press.
20. Schoeman, F. D., Ed. (1984). Philosophical dimensions of privacy: An anthology. Cambridge, Cambridge University Press.
21. Shils, E. (1966). "Privacy: Its constitution and vicissitudes." Law and Contemporary Problems 31(Spring): 281 - 306.
22. Smith, H. J., S. J. Milberg, et al. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." MIS Quarterly 20(2 (June)): 167-196.
23. Stewart, K. A. and A. H. Segars (2002). "An empirical examination of the concern for information privacy instrument." Information Systems Research 13(1): 36 - 49.
24. Stone, E. F., H. G. Gueutal, et al. (1983). "A field experiment comparing information-privacy values, beliefs and attitudes across several types of organizations." Journal of Applied Psychology 68(3): 459 - 468.
25. Stone, E. F. and D. L. Stone (1990). "Privacy in organizations: Theoretical issues, research findings, and protection mechanisms." Research in Personnel and Human Resources Management 8: 349 - 411.
26. Taylor, S. and P. A. Todd (1995). "Understanding Information Technology Usage - a Test of Competing Models." Information Systems Research 6(2): 144-176.
27. Tolchinsky, P. D., M. K. McCuddy, et al. (1981). "Employee perceptions of invasion of privacy: A field simulation experiment." Journal of Applied Psychology 66(3): 308 - 313.
28. Westin, A. F. (1967). Privacy and Freedom. New York, Atheneum.