

Chapter V

Information Technology and Privacy: A Boundary Management Perspective

Jeffrey M. Stanton
Syracuse University, USA

ABSTRACT

With the rising popularity of the Internet and some widely publicized occurrences of privacy loss due to information technology, many individuals have recently become more concerned with the privacy and security of sensitive information. These concerns have special relevance within work organizations because of the substantial amounts of data that organizations typically collect about the work and non-work activities of their employees. This chapter presents a new theoretical perspective called Information Boundary Theory, that describes whether, when, and why employees care about the privacy and security of sensitive information at work. Analysis of interview data from N=25 non-managerial U.S. workers provided preliminary support for four of the new theory's research propositions. The chapter describes implications of the theory and the research findings for the design and deployment of information technology systems within organizations and maps a research agenda for future uses of the theory.

INTRODUCTION

The deployment of information technology into organizations has continued to accelerate over recent years. Information technology systems that leverage networks, databases, and telecommunications channels carry, distribute, display, and store an increasing amount of data that has personal relevance to individual

workers. Thus, designers, administrators, and users of such systems may have a strong interest in facilitating and assuring proper regulation of personal information flows. From a technical standpoint such matters are handled through a variety of mechanisms such as encryption and access control, but from a social standpoint it is important to understand what information must be protected, when, and why. In this paper I synthesize a framework for understanding the regulation of personal information flows based on three component theories relevant to the privacy of personal and performance information in organizational settings. This framework, called information boundary theory, uses a guiding metaphor from psychologically grounded research on communications boundary management. In support of the viability of the framework I discuss qualitative data from an interview study that provided a preliminary assessment of the framework. Finally, I discuss applications of the framework to future research and to the practice of information systems design.

INFORMATION TECHNOLOGY AND PRIVACY: A BOUNDARY MANAGEMENT PERSPECTIVE

Commercial, non-profit, and governmental organizations use information technology in a variety of ways to obtain and communicate data about their employees, clients, customers, and other relevant individuals. While this observation has been true for many years, key issues such as privacy have become particularly salient with the widespread availability of new data collection, transmission, and storage strategies facilitated by the Internet, intranets, databases, and related information technologies (see, for example, Agre, 1997; Kahin & Nesson, 1997, p. x; U.S. Congress, 2000). In parallel to these developments, increased use of telecommunications media to support the quotidian communications needs of organizations has resulted in a consequent increase in the transmission of sensitive personal information through such channels as email, voicemail, and instant messaging. Investigations of these issues have clearly shown that organizations and their members must take special care in regulating the flow of personal information through the wide variety of information technology systems available now and in the future (Eddy, Stone & Stone-Romero, 1999; Pincus and Trotter, 1995; Sipior, Ward, & Rainone, 1998; Stanton & Weiss, 2000).

From a purely technical standpoint, specific remedies to ensure the security of data (e.g., authentication, access control, encryption, etc.) have long been available, and researchers continue to expand and enhance the repertoire of available techniques. From a socio-technical point of view, however, these techniques comprise a toolbox; the difficult work lies in knowing when a particular tool is

needed and why. Thus, in designing or administering an information system that handles personal information, it is important to understand the perspectives and needs of those individuals whose privacy is at stake—workers, managers, clients, customers and others whose personal information is collected, transmitted, and stored by information technology.

To this end, this chapter describes a theoretical framework for information privacy that I have synthesized from three relevant component theories. The new framework provides predictions about how information collection, storage, and dissemination strategies affect people's attitudes, beliefs, and behaviors toward the institutions that seek to obtain the data. The framework may have particular relevance for information system design that has as its goal the development, implementation, and administration of digital government systems, e-commerce, customer relations management systems, human resource information systems, collaboration software, cooperative work systems, and other information technologies that handle sensitive personal information.

The information boundary theory that I describe below developed out of research investigating uses of monitoring and surveillance technologies within organizations. Analysis of two waves of interview and survey data (Stanton, 2000; Stanton & Weiss, 2000) suggested the viability of synthesizing communications boundary management theory (Petronio, 1991), justice theory (Alder, 1998; Alder & Tompkins, 1997), and a general expectancy-valence framework for privacy protection (Stone and Stone, 1990). In general terms, the framework predicts that individuals' reactions to uses of information technology to collect information about them should follow rules for "boundary opening" and "boundary closure." Boundary opening and closure are dynamic, psychological processes of regulation by which people attempt to control the flow of "intimate" information. In the remainder of this chapter, I introduce the component theories, develop the framework, outline the results from a recent interview study that was designed to provide a preliminary assessment of the framework, and discuss the implications of the framework for future research and practice.

SYNTHESIS OF INFORMATION BOUNDARY THEORY

Researchers have investigated workplace privacy from a variety of perspectives. For example, studies have focused on privacy invasions of physical space (e.g., Cangelosi & Lemoine, 1988; Duvallearly & Benedict, 1992) and of social space (e.g., LePoire, Burgoon, & Parrott, 1992). Organizational researchers have investigated privacy in personnel selection (Connerly, Mael, & Morath, 1999;

Fusilier & Hoyer, 1980; Jones & Joy, 1991; Kirchner, 1966 Stone & Stone, 1987), in the storage and use of human resources data (Eddy, Stone & Stone-Romero, 1999; Stone, Gueutal, Gardner, & McClure, 1983; Woodman, et al., 1982), and in the monitoring of employee communications and performance (Sipior, Ward, & Rainone, 1998; Stanton & Barnes-Farrell, 1996; Stanton & Weiss, 2000).

Although workplace privacy has provided fertile ground for research, no predominant theoretical perspective has emerged to account for the psychological mechanisms guiding employee attitudes and behaviors about workplace privacy. Stone and Stone (1990) provided a general expectancy-value framework that helped to classify and organize a variety of motivations for privacy protection behaviors. Later, Stone and Stone-Romero (1999) widened the focus of their model to account for balance and conflict among different constituencies concerning organizational privacy issues. In neither case, however, did their work explicate the psychological antecedents, processes, and outcomes that shape workers' reactions to privacy-related issues in the workplace. For additional insights into these mechanisms, it is necessary to incorporate theoretical developments from other areas of social science. Specifically, Petronio (1991), in the field of communications, proposed and tested a "communication boundary management" (CBM) model built on the work of Altman (1975; 1976) and others to explain privacy regulation in marital, family, and other interpersonal contexts. In complementary developments, Alder (1998; Alder & Tompkins, 1997) argued for the utility of organizational justice as an explanatory factor in understanding employees' reactions to workplace monitoring and surveillance. Together, these three theories provide a lens through which the privacy implications of organizational communications and data management practices can be examined.

COMMUNICATION BOUNDARY MANAGEMENT APPLIED TO ORGANIZATIONS

In describing her theory of communications boundary management, Petronio (1991) argued that all human relationships contain an intrinsic tension between intimacy and autonomy. Intimacy, on the one hand, comprises revelatory processes through which one individual becomes known to another. Autonomy, conversely, is promulgated by communicative and other behaviors that protect and separate the self from others. Applications of these ideas to marital relationships, parent-child relationships and so forth are straightforward, but Petronio has argued (Petronio & Chayer, 1988) that the tension between intimacy and autonomy is intrinsic in workplace relationships as well. These concepts map onto workplace privacy

concerns with the assertion that employees view monitoring, surveillance, personal data collection, and technology-mediated organizational communications as potentially revelatory of themselves. Here are some illustrative examples: Having one's task performance or computer activities monitored provides a communication conduit through which a supervisor or manager can receive detailed information about one's productive (or unproductive) activities. Likewise, working in an environment with video surveillance cameras makes one's conscious and unconscious behaviors available for scrutiny while on company premises. Collection of personal data (e.g., lifestyle information for insurance purposes) also reveals intimate aspects of the self to others within the work environment. Finally, communication of opinions or ideas over email, voicemail, or other messaging technologies can publicize one's point of view about people and other important matters. I do not mean to imply that these forms of revelation are inappropriate or undesirable, but rather that they all constitute communicative activities in the workplace by which the self (e.g., an employee) becomes known to the other (e.g., coworkers, supervisors, managers, or human resources professionals). I do hypothesize, however, that stakeholders such as employees have a strong interest in or feel needs to "regulate" these forms of communication.

Regulating communication in order to influence whether and how others learn about the self provides the opposing force to revelation in Petronio's (1991) CBM theory. Thus, in tension with the conduits for revelation described above are individuals' well-documented needs for autonomy and control (cf. Deci & Ryan, 1991; Greenberger & Strasser, 1986; Spector, 1981). For example, after allowing for idiosyncratic individual differences, most employees appear to have at least some motivation to control their immediate work environment, their choice of tasks, their rate of working, and the impressions that other individuals have of them (particularly powerful others such as managers). With reference to this latter motivation, large bodies of literature on impression management (Giacalone & Rosenfeld, 1991; Morrison & Bies, 1991) and socially desirable responding (Moorman & Podsakoff, 1992) attest that individuals have consistent and sometimes strong motivations to control how others see them.

CBM theory (Petronio, 1991) asserts that people balance the tension between intimacy and autonomy by negotiating psychological boundaries between themselves and others. A boundary in this context is thus defined as a (usually tacit) "psychological contract" between oneself and another concerning the amount, nature, and circumstances of requesting, sending, and receiving personal information. Boundaries become open for sending and receiving information and closed for restricting the flow of information to and from the self. Open boundaries encourage requests for more information and closed boundaries discourage them. The details of CBM theory explicate a set of rules by which psychological needs

within a dyadic relationship and the type and context of the personal information interact to determine boundary opening and closure (see Petronio, 1991). Of particular interest for applications to the workplace, “senders” open their boundaries when there is interdependence in the dyad, when the sender does not perceive an undesirable level of vulnerability to negative reactions by the “receiver,” and when potential exists for an expressive or instrumental benefit of transmitting information across the boundary. Not coincidentally, these are elements that conceptually overlap with social psychologists’ definitions of trust (Boon & Holmes, 1991; Lewicki, McAllister, & Bies, 1998). For example Boon and Holmes (1991) defined trust as, “a state involving confident positive expectations about another’s motives with respect to oneself in situations entailing risk” (p. 194). In brief then, I have translated CBM for workplace applications by suggesting that individuals open their communication boundaries—and are therefore amenable to revealing personal information through performance monitoring, mediated communication, and other organizational data collection methods—when they perceive trust in their relationship with the organizational “other.” The other is personified by the information receiver, for example, a manager, supervisor, or human resources professional. Individuals also may realize, however, that this receiver is usually not simply the other member in a dyadic relationship but may also play the role of an official organizational representative with the intention and means of using the revealed personal information to serve the organization’s purposes. The implication is that the receiver’s role as an organizational member or representative may be as important a consideration in negotiating boundaries as the employee’s personal relationship with the specific individual.

At this point it is possible to intermix additional implications pertaining to the use of information technology as a medium for the transmission of personal information in organizations. Petronio’s (1991) research focused primarily on how boundary regulation occurs in face-to-face interactions. To support her propositions she drew on a rich tradition of social psychological and anthropological research on verbal and non-verbal behavior. For example, in a face-to-face situation, an individual can open a communications boundary beyond the dyad by raising her voice so that others can hear the message. Closing a boundary in a face-to-face situation could entail physically withdrawing from a conversation or using “verbal judo” to divert an inquiry to another topic. Mapped into the domain of mediated communication and technology-facilitated personal data collection, individuals have a larger repertoire of techniques for regulating disclosure, but are also subject to a broader range of situations where a catastrophic loss of control over personal data is possible. Taking email as just one of many possible examples, boundary opening to transmit a message beyond the dyad can be accomplished actively through “carbon copy” and “blind carbon copy” mechanisms, while,

analogously to the face-to-face situation, boundary closure can be accomplished simply by withdrawing from the dialog (i.e., refusing to reply). On the other hand, an email message, once transmitted, is more vulnerable to loss of regulatory control even than gossip (the face-to-face equivalent of forwarding an email), because the message is seen by in a form directly authored by the self, and because the amplifying power of the technology makes possible wider (and quicker) rebroadcast as well as semi-permanent storage of the message.

These insights form a central concern of the final section of this paper: Information technology amplifies both opportunities for boundary regulation and possibilities of loss of boundary control. Information systems designs that attempt to successfully incorporate the regulation of personal information can do so by providing tools for boundary regulation and barriers or firewalls to prevent catastrophic loss of control. Before examining these tools and firewalls, however, it is important to understand the circumstances under which individuals desire to open and close their information boundaries. The organizational justice and expectancy-valence theories described below can help to pinpoint these circumstances.

ORGANIZATIONAL JUSTICE APPLIED TO BOUNDARY NEGOTIATION

Alder (1998; Alder & Tompkins, 1997) provided a literature review of monitoring and surveillance methods in the workplace highlighting both negative and positive effects of monitoring documented by various researchers. Alder then argued that an organizational justice perspective could provide insights into how employees would react to organizational performance monitoring procedures. Stanton (2000) provided empirical evidence from several diverse samples confirming that organizational justice served as a useful explanatory model for understanding how the characteristics of electronic and traditional performance monitoring affected employees reactions to monitoring. Although the theory and the findings were framed specifically to explain reactions to performance monitoring, these ideas arguably extend to a more general consideration of personal information flows in organizations as they relate to monitoring, surveillance, communication, and other forms of personal data flow that are managed by organizations and their information technology.

One successful theoretical perspective attributes individuals' preference for fair procedures and treatment to their need for affirmation of identity with a valued group. Termed the "group-value" model of organizational justice (Lind & Tyler, 1988), the theory proposes that people value their membership and status in certain

groups, and that fair treatment by group members and in group practices affirms their membership and status. For example, when a person is the target of gossip from another group member, this treatment is seen as unfair because it reflects badly upon the target's status as a group member. Thibaut and Walker (1975), Leventhal (1980), Bies (1987; Bies & Moag, 1986), Greenberg (1993), and others have discussed the conditions and factors that may lead to evaluations of fairness and unfairness, but Alder (1998; Alder & Tompkins, 1997), using the group-value model as a guide, distilled these down to four basic propositions. First, Alder asserted that personal data collection practices have sufficient impact on the work lives of employees to be seen by them as playing an important role in organizational justice. Second, Alder indicated that the personal data content collected and transmitted by information systems must have the highest possible "mission relevance" in order to be seen as fair (e.g., a performance evaluation system could capture work history but not race). Third, Alder commented that personal data collection policies and practices that encourage or at least allow a value expressive function (i.e., "voice" in Thibaut and Walker's terms) will be seen as most fair. Examples of such value expression would be the opportunity for employees to give feedback on the design and implementation of an information system that will process their personal data, or mechanisms built into the procedures of data processing that allow employees to address or appeal problems recorded in these systems. Finally, drawing on previous justice research, Alder described a zone of acceptance in which employees would not scrutinize the fairness of organizational monitoring practices. Routine requests for performance information fall within this zone, and such requests, too ordinary to arouse employee concerns about their status in the group, would not trigger an evaluation of the criteria for fairness described above.

SYNTHESIS OF CBM AND JUSTICE WITH STONE AND STONE'S EXPECTANCY-VALUE THEORY

Stone and Stone (1990) provided a general framework for predicting privacy protection behaviors based on an expectancy-value (EV) framework. EV frameworks have been applied to choice behavior and other motivated behavior in many work situations (Pinder, 1998). Vroom's (1964) valence-instrumentality-expectancy theory and Porter and Lawler's (1968) rework of this are widely known organizational applications, but these and other EV frameworks all harken back to seminal work by Lewin (1938) and Tolman (1959). Recent work on EV (e.g., Feather, 1995) is reflected in this simple formulation, "...a person's values, once engaged, induce valences (or positive and negative subjective values) on

actions and their possible outcomes and future consequences. Actions are assumed to occur in relation to these induced valences and the person's expectations about the likelihood of achieving the outcomes and future consequences." (Feather, 1988, p. 105). Stone and Stone's (1990) application of EV to privacy protection reflects the same underlying assumptions: "In the process of engaging in certain behaviors, including those designed to protect OP [organizational privacy], individuals are assumed to behave in ways that they believe will result in the most favorable net level of outcomes. . . . Consistent with expectancy models of motivation, cognitions about outcome levels are assumed to be a function of expectancies, valences, and instrumentalities." (Stone & Stone, 1990, p. 363).

In short, Stone and Stone (1990) considered motivation to protect privacy as a rational process of maximizing instrumental outcomes (e.g., by hiding information that might adversely affect a personnel action such as promotion). Instrumental outcomes, in this context, refer primarily to material or financial gains and losses and are thus distinct from the expressive outcomes intrinsic in theories of justice. By first adding the perspectives associated with CBM theory (Petronio, 1991), we can expand the repertoire of behaviors subject to explanation: Stone and Stone's privacy protection behaviors are akin to the closing of boundaries to achieve positive or avoid negative outcomes, whereas CBM additionally accounts for the opening of boundaries, strategies for negotiating the conditions of opening and closing, contextual factors governing the conditions under which senders transmit particular types of personally significant information to receivers, and the information requesting behavior of receivers. For example, CBM would explicate a conversation (i.e., the boundary negotiation) between a job applicant and an HR professional, in which the applicant hears a justification of the intended use of some information (i.e., the contextual factor) and decides to provide the information (i.e., boundary opening).

Next, by incorporating the organizational justice perspective, we can enhance understanding of the instrumental goals that boundary opening and closing can serve: Employees' concerns about the job-relatedness of monitoring and surveillance suggest a desire to shape how others view their on-the-job behavior (including non-prescribed activities such as organizational citizenship behaviors). Additionally, however, both CBM and the organizational justice perspective indicate that individuals wish to regulate the flow of personal information on bases other than purely instrumental ones. In particular, the organizational justice perspective suggests that revelation of personal information may serve expressive goals that test and affirm an individual's status as a group member.

Together, then, these theories suggest a set of related general research propositions. First, if monitoring, surveillance, communication, and other organizational forms of personal data flow are parallel to dyadic communication as

described by CBM, then individuals should frame their conceptions of these practices in terms of the flow of personal information within human relationships (e.g., “telling about me,” “knowing what I’m doing,” “becoming known,” or perhaps “becoming visible to others”). Individuals should be capable of articulating the calculus of boundary negotiation, i.e., the conditions under which permitting information flow about them is acceptable or unacceptable. The negotiation of boundaries should be highly dependent on the status of the relationship between the employee/sender and the organization/receiver. I have offered a shorthand term for the relationship status most conducive to the opening of boundaries: trust. If trust exists between the sender and the receiver, boundaries should open to the flow of more and more “intimate” types of information content. Incorporating the justice perspective, intimate, in this context, refers to information that is personally relevant but not “mission relevant.” To the extent that trust does not exist or has faltered in the relationship, senders may attempt to close boundaries to all but the most directly mission relevant types of information. Senders will evaluate receiver requests for information in light of the trust in the dyad and organizational justice concerns about the information. Senders will most likely open boundaries to information that serves their instrumental or expressive ends. Finally, a zone of acceptance may exist in which the sender transmits routine forms of information across the boundary without explicit consideration of instrumental or value expressive goals.

I have intentionally framed these ideas as a complex of related, general research propositions because the merger of these component theories, while promising, is not at this time mature enough to offer hypotheses of sufficient specificity to warrant quantitative measurement and statistical inference testing. In recognition of the preliminary status of this framework, I have sought early evidence by conducting a series of semi-structured interviews. This research explored whether these hypothesized communication boundaries exist in workplace situations and, if so, how employees negotiate the opening and closing of these boundaries in reference to contextual factors such as the type of information requested by the organization. The research was reported in detail in Sarkar, Stanton, and Line (2001) and is summarized more briefly below.

METHOD

My research team conducted interviews with $n=25$ non-managerial employees (40% males) from a variety of industries in the continental U.S. Participants’ job responsibilities included emergency medical technician, construction worker, cashier, secretary, data processing analyst, child support investigator, customer service representative, welder, and a variety of other types of work. Half of the respondents had been on their present job at least 2 years. We used a semi-

structured interview protocol that was designed to elicit descriptions of the conditions under which respondents would or would not reveal various kinds of performance and non-performance information to their organizations. The interview contained seven questions about monitoring, surveillance, and the organizational collection of personal information based on earlier interview work conducted by Stanton and Weiss (2000). Each question described a hypothetical company policy concerning a certain type of personal information and asked the respondent to indicate whether he or she would share that information and the rationale behind that decision. We transcribed the interviews verbatim (including interviewer queries), coded the resulting transcriptions and conducted frequency analysis of code assignments to identify major thematic content (see Charmaz, 1995; MacQueen, McLellan, Kay, & Milstein, 1998; Strauss & Corbin, 1990). We used the procedures described in Carey, Morgan, and Oxtoby (1996) to improve inter-coder agreement. We iterated through these procedures until we obtained 80% agreement across all respondents and questions. We triangulated on the themes by examining combinations of codes. In particular, we examined coding patterns that emerged in conjunction with material indicating the acceptability or unacceptability of information requests. Within these patterns we related codes back to respondent verbatims to ensure that our findings accurately represented the ideas of the respondents.

RESULTS

Descriptive Information

A total of 953 code assignments was made across all questions and respondents for an average of about 38 codes per respondent. That is, interviewees on average stated about 38 distinctly recognizable ideas during the course of their interview. Table 1 lists the set of thematic code descriptions and their frequency of occurrence. The most frequently occurring code ($n=355$) captured the idea that the respondent felt that the monitoring, surveillance, or data collection technique under discussion was acceptable to them: They would not hesitate to share the information requested. Conversely, the next most frequently occurring code ($n=120$) captured the idea that the respondent felt that they would not feel comfortable sharing the information requested. The frequent occurrence of these two opposing ideas reflects the primary orientation of the interview, which was to seek the boundary between acceptable and unacceptable information in order to explore the respondent's detailed reasoning concerning the negotiation of this boundary. The remainder of this analysis comprises one section describing conditions for sharing of information — boundary opening — and another section for withholding or

protection of information—boundary closing. The analyses described below all reflect an examination of the co-occurrence of at least two thematic codes and thus do not always match the overall frequencies reported in Table 1.

Conditions for Opening Boundaries

Zone of Acceptance. Three themes emerged pertaining to the typicality of organizational information requests. A theme describing a policy as common practice in most organizations was assigned nine times in conjunction with the code for acceptable transmission. This theme captured the idea that some personal information was typically requested and therefore, by custom, not sensitive. Another theme indicating prior experience with the technique appeared 13 times in conjunction with the theme for acceptable transmission. Finally, a theme indicating generic availability of requested information appeared four times with the theme for acceptable transmission. These themes all appear to capture Alder's (1998; Alder & Tompkins, 1997) idea of a zone of acceptance. Senders may often respond to information requests perceived as routine and ordinary by transmitting the information without thoughtful scrutiny.

Job Relatedness/Justice. Five themes emerged pertaining to the job-relatedness of the requested information. One theme, capturing the idea of the "employer's right to know," was used 13 times. Verbatims for this theme supported the employers' right to certain information because of their ownership of the underlying resource. Two additional themes, which appeared a total of 10 times, further emphasized the importance of business-related use of the underlying resource. Another thematic code, assigned twice, pertained to transmitting information to individuals outside of human resources as long as the information was performance related. The final theme in this area coded the importance of observing employee behavior only in work-related spaces. These codes all appear to capture Alder's (1998; Alder & Tompkins, 1997) ideas about the perceived fairness of monitoring job-related behaviors. In these responses, senders were willing to provide the requested information about their whereabouts, who they called on the phone and what they said, and other aspects of their job behavior, just as long as the information collected had a business-related purpose. Another justice theme concerning the acceptability of data collection pertained to the importance of preset company policies governing the procedures (coded 5 times). As above, the notion of established rules that decision-makers must follow is a hallmark of some theories of procedural justice (e.g., Leventhal, 1980).

Instrumental Goals. Several themes emerged pertaining to instrumental goals that would be served if the employee/sender transmitted the requested information. The most frequently occurring theme, emerging in 16 verbatims, pertained to abuse of company resources. In these verbatims respondents believed that certain types

Table 1: Thematic code descriptions and occurrence frequencies

Frequency	Thematic Code Description
355	Monitoring/information request is acceptable
120	Monitoring/information request is unacceptable
49	Question not asked in this interview
41	This monitoring/information request invades privacy
36	Monitoring/information request is unacceptable but will comply
30	This monitoring/information request prevents abuse of company resources
28	I am concerned about security of the system
22	I like my job
22	The monitoring/information requested is not job related
20	Employer does not have the right to know this
20	This technology helps improve organizational efficiency
17	If this policy/practice discriminates among employees
15	I have experienced this technology before
14	The requested information may reach someone who is not authorized to have it
14	This policy/practice shows that the company does not trust employees
13	There must be guidelines about monitoring, storage, and how information is used
10	Computers are unreliable guardians of data
8	This is a common, acceptable practice in most organizations
8	Employer has the right to know this
8	This technology can provide protection when in danger
8	The monitoring/information requested is job related
7	I have not experienced this technology before
7	Access to this personal data should be restricted
7	Only if monitoring personal spaces
6	Only if tracking personal e-messages
6	It is difficult to cope with constant up-grades
6	If knowledge of this data collection is shared with me
5	Knowing the character of employees important to avoid making bad hiring decisions
5	Only if monitoring public places
5	One should obtain this employee data from supervisors not electronic databases
4	Only if tracking business related messages
4	Historical information about this is irrelevant to future decisions
4	If gathered information is used to make employment decisions
3	This monitoring can inhibit performance
3	This information can be learned by face-to-face contact with the person
3	Only if monitoring is non-secretive
2	This monitoring helps provide accurate feedback
2	This monitoring helps improve performance
2	This practice can cause physical ailments
2	This practice has made us dependent on technology
2	My job meets my needs
2	Only if monitoring is secretive
2	One cannot trust the guardians of the data
1	Do not wish to respond to this question
1	This monitoring leads to fair performance evaluations
1	This practice is equivalent to guilty without trial
1	More authorities should have access to personal data
1	I do not like my job
1	This information is irrelevant if I can physically do the job

of information collection were justified because they prevented “cheaters” — coworkers who might try to beat the system — from receiving more than their share of organizational resources. Two themes, each coded three times, reflected the importance that people place on having compatible coworkers and concerns about workplace security and their concomitant willingness to appear on video cameras. Two different themes, each coded twice, related to job performance.

Each of these themes provides a basis on which the respondent reasoned an advantage of providing the information requested. As such these themes fit Stone and Stone’s (1990) predictions about the importance of instrumental motivations. Importantly, however, the themes all suggest motivations for revelatory behavior — opening of boundaries — rather than privacy protection. Themes about disclosure of surveillance (coded 4 times) and sharing information from testing (coded 3 times) also emerged as relevant to the acceptance of these policies. Some respondents expressed a belief that if organizations kept surveillance secret it implied a lack of trust of the employees. Other verbatims pertaining to the results of genetic testing suggested that employees wanted to access their information so that they would be able to “appeal” any adverse results. The notion of an appeal process is central to many formulations of procedural justice. Thibaut and Walker (1975) have also indicated that appeals serve a value expressive function.

Conditions for Closing Boundaries

In an interesting contrast to Stanton and Weiss (2000), the most frequently mentioned general rationale (coded 38 times) for boundary closure was a concern for personal privacy. In general, respondents initially mentioned privacy and then, with follow-up questions from the interviewer, made their rationale known for considering a particular information inquiry a privacy issue. In ten of these cases respondents mentioned an intimacy theme (e.g., not wanting an organizational representative to know about bathroom habits). The next most frequently mentioned general rationale (coded 24 times) was an expression that the employer did not “have a right to” the information requested. Indicating that some types of information and requests were “none of the organization’s business” was the typical mode of expressing this idea. As with privacy, this theme provides little insight into the motivations or conditions for boundary closure, so one must look to the associated themes to understand these issues.

Job Relatedness/Justice. Five different themes emerged suggesting that individuals close their communication boundaries when requested information is not job related. First, in general terms, respondents indicated that the information requested was not relevant to performance on the job in 16 different statements. On a related note, seven respondents mentioned that certain types of information should remain within the employee-manager dyad rather than becoming available

to a wider audience of managers. Two additional reasons for boundary closure were coded separately but shared a common theme. First, six employees described as unacceptable any policies that might permit access to employees' personal communications. These verbatims also suggested a belief that organizations should provide employees with access to resources for private communications while at work. On four occasions, respondents extended this right to include the communications with customers, clients, or vendors. Note that although most of these verbatims pertained to telephone monitoring, one respondent mentioned the desire to control access to personal email communications and another respondent wished to control access to job-irrelevant medical information.

On four occasions, respondents described a "water under the bridge" theme: an indication that employers should not have the opportunity to use evidence of past problems against an employee in decisions such as hiring. Another justice theme that emerged (12 instances) was a concern for the release of information that might result in unfair discrimination against an incumbent employee or applicant. Although these verbatims reflected some well-known types of employment discrimination (e.g., racial bias), other verbatims indicated concern for discrimination based on personal habits (e.g., smoking or alcohol usage), family situation (e.g., being a single mother), health status, and financial status. In each case the respondent indicated an unwillingness to provide the requested type of information because of the possibility that the information would be used as the basis of an unfavorable (and unfair) employment decision.

Trust/Security/Access Control. Four themes emerged that related to trust. First, respondents frequently (coded 17 times) expressed mistrust of the underlying technology that was supposed to secure their personal or employment-related information. In clarification of this theme, 15 responses expressed concern that the underlying technology would permit information access to individuals who should not have that permission. On a related note, two responses indicated mistrust for the "guardians" or owners of the data. In a separate theme, 13 responses indicated that the specified information request was unacceptable because it indicated that the organization did not trust you.

Instrumental Motivations. Only one instrumental reason for boundary closure emerged. Two responses indicated a fear that performance monitoring practices might have adverse effects on job performance.

DISCUSSION

To summarize, the interview data appeared to support four of the predictions of the framework. First, as Alder (1998; Alder & Tompkins, 1997) suggested, a zone of acceptance appears to exist within which employees do not scrutinize

information requests for acceptability. Second, boundary opening and closure both appear to be partially governed by organizational justice considerations: mission-relatedness of the information, an appeals process, and preset guidelines to govern the use of the requested information. Third, boundary opening is also partially governed by instrumental motivations such as conservation of the organization's resources. In some cases, a concern for equity — also considered an organizational justice concept — may form the basis of such motivations. Interestingly, only one instrumental theme for boundary closure emerged; employees reported more strategies to pursue instrumental goals through revelation of information rather than withholding information. Finally, mistrust appeared to figure prominently into boundary closure considerations. In particular, mistrust of technology and the people who have access to it was a primary motivation for withholding information. In regard to boundary opening, some of the comments hinted at predicted themes of trust and value expression, but these references failed to emerge as strongly as other themes summarized above.

Taken together, the interview evidence supported the idea that monitoring, surveillance, communication, and other organizational forms of personal data flow are analogous to dyadic communication as described by CBM. Interview respondents were apparently capable of articulating the calculus of boundary negotiation. The negotiation of boundaries appeared to be at least somewhat dependent on the status of the relationship between the employee/sender and the organization/receiver: When trust exists between the sender and the receiver, boundaries may open to the flow of more and more “intimate” types of information content. Senders also seem to open boundaries to information that serves their instrumental or expressive ends. Finally, a zone of acceptance seems to exist in which the sender transmits routine forms of information (particularly those that are “mission relevant”) across the boundary without invoking the calculus of instrumental or value expressive goals.

Unifying Monitoring, Surveillance, Data Collection, and Communication

By synthesizing communications boundary management and organizational justice with a general expectancy-valence framework, I asserted that seemingly different organizational policies and practices could be examined in a unified way. Specifically, I suggested that performance monitoring (e.g., by computers, video cameras, etc.), surveillance of non-performance behavior (e.g., email and web tracking), collection of personal data (e.g., in applying for insurance), and mediated communications (e.g., by email), could all be viewed as personal information flows governed by organizational policies and the capabilities of the related information technology. The interview data appeared to support this view in that a concise and well-defined set of conditions and motivations appears to govern boundary opening

and closing for all four types of personal data collection. In each case, a zone of acceptance exists in which information requests are fulfilled without careful scrutiny. Outside the zone of acceptance, boundary opening or closure depends upon organizational justice considerations (e.g., mission-relatedness), trust, and/or instrumental considerations (e.g., conservation of organizational resources). Some notable asymmetries appeared (e.g., instrumental concerns seemed less relevant for boundary closure), although it is difficult to ascertain whether these occurred as a result of the limitations of our sample and research methods.

On Compliance

In the above discussion of boundary closure, respondents said that they would not comply with the information request in most cases. In 17 different instances, however, respondents mentioned that they found the information request unacceptable but would comply nonetheless. In the breach, such a response seems more probable than outright refusal or other kinds of resistance strategies. When an information request has been honored only under duress, this represents a suspension of the normal dyadic negotiation of communication boundaries. In extreme cases, when an individual has been forced to reveal information that would preferentially be protected, one might say that a privacy violation has taken place. Petronio (1994) discussed such violations in her study of parents and college age children returning home during break. Specifically, when boundary negotiation between parent and child broke down, or when the parent ignored previously negotiated boundaries, the child often made a behavioral response. Responses to such privacy violations comprise a varied set of privacy restoring behaviors, some of which are relatively benign within the family context (e.g., leaving a warning note) and some which are more severe (e.g., running away from home). It is feasible to hypothesize a parallel set of processes that occur within organizations when employees perceive that their privacy has been violated. Depending upon the severity of the violation, employees could be expected to attempt to restore privacy through a variety of methods. In extreme cases (presumed to be relatively rare), resistance, retaliation, or withdrawal might occur.

On the Dyadic Boundary

We made no predictions concerning different types or levels of boundaries, but Derlega, Metts, Petronio, and Margulis (1993) described a distinction between an interpersonal boundary within the dyad, and the boundary between the dyad and the “outside world.” This distinction captures the idea that, for example, a sender may make some revelations to a spouse that the sender expects will not be divulged outside of the marital dyad. The interview data appeared to suggest that an employee might construct such a boundary around the dyad formed with their

immediate supervisor or manager. Our data indicated that when employees expected that certain sensitive data (such as formal performance evaluations) might be transmitted outside the dyad this expectation could lead to boundary closure. This highlights an important complication: The manager, in the role of a receiver, may simultaneously represent him or herself (on a purely personal level) and the department or organization as an official representative. In future development of the theoretical synthesis provided in this article, the framework should incorporate the distinction between interpersonal boundaries and the dyadic boundary. Relatedly, it is likely that there are distinct psychological boundaries around an individual's work group and that dyadic and interpersonal boundaries with group members are nested within these larger "community" boundaries.

Limitations of This Evidence

Because of the small sample size used in this study, these results are not representative of the population of U.S. workers or any sub-population thereof. Thus it is possible or even likely that the full range of issues influencing boundary opening and closure has not appeared in this study. In particular, future research that focuses on unique and distinct segments of the workforce (e.g., older workers, temporary workers, or cultural minority members) may find a substantially different mix of motivations and priorities concerning privacy regulation. Although results from this study can safely be interpreted as suggestive of several important and enduring themes that would likely be endorsed by many workers, ascertaining the applicability of any one theme to a representative sample of employees should serve as the focus of future research. For example, exploring the presumptive relationship between mission-relatedness and boundary opening and closure in a large sample of homogeneous individuals (e.g., employees) would have value in substantiating the universality of this theme.

Design and Practice Implications

Even though these recommendations must be tempered by an understanding of the limitations of the preliminary status of this framework, I believe that framework supports several recommendations for positive design and practice. First, every indication from our results indicates that employees do care about privacy in organizational settings. Beyond a "zone of acceptance" for routine information requests, the framework indicates that is imperative for organizations to gauge the impact of any policies and practices that involve collection of personal or performance information about individuals. When such data collection is warranted, favorable relations with employees, customers, and other stakeholders can be maintained by ensuring that information collection practices are perceived as fair and mission-related. Policies should be communicated and practices

conducted with the awareness that trust between individuals and the organization can quickly and easily be undermined by requesting or obtaining information that individuals perceive as unfair, potentially discriminatory, or unrelated to the organization's mission.

Understanding the Zone of Acceptance. Certain kinds of information requests and flows can occur without special attention to individuals' boundary regulation. The best method of understanding this zone of acceptance probably lies in conducting a stakeholder survey to ascertain specifically what kinds of personal data are considered unremarkable and under what circumstances, but a few heuristic rules probably suffice for many cases. Information requests that can be fulfilled anonymously probably fall within most people's zone of acceptance. For example, individuals often complete anonymous attitude surveys with little concern about the privacy of their responses. Non-controversial, publicly available data also typically fall within the zone of acceptance. For instance, an individual's gender can typically be determined by a casual observer (even over the telephone), so few individuals resist having this personal data coded into employee or customer databases.

Designing to Facilitate Boundary Regulation. One clear imperative implied by the content of this chapter is that designs of organizational information systems should incorporate tools that help stakeholders regulate their information boundaries. Although the framework eloquently affirms the need for such tools, there is a considerable body of prior writing that has explored the form that such tools might take. For example, three possibilities appeared in the "Code of Fair Information Practices" that appeared several decades ago in a federal government report (U.S. Dept. of Health, Education, & Welfare, 1973). First, the report suggests, "There must be a way for a person to find out what information about the person is in a record and how it is used." More generally, every organizational information system that manages personal information flows should contain a retrieval mechanism through which individuals can locate and review prior correspondence and stored records that contain information that originated with them. Second, the report continues, "There must be a way for a person to correct or amend a record of identifiable information about the person." This point closes the loop with the first point: Given a method of reviewing one's own personal information, there must also be a method for correcting it if it is wrong or inappropriately incomplete. Finally, the report says, "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent." This is by far the most difficult of the three stipulations from a system design point of view, but it also exemplifies the heart of the boundary regulation concept. An information system user must have the tools to designate that a certain information flow belongs to a particular audience, for a particular purpose, and for a particular lifetime or timeframe.

Most importantly, the information system must then enforce those designations and limit overrides to the smallest possible community of system administrators. Few if any existing organizational information systems meet the ideals contained in these three stipulations.

Promoting Boundary Opening. Another design imperative implied by the content of this chapter is that an information system whose essential goal is communication or sharing of information should promote boundary opening rather than boundary closure. (Note that this need not be the goal of all information systems: A mental health database containing sensitive personal histories might best be designed to discourage information sharing.) According to the data described in this chapter, boundary opening occurs when organizational justice considerations are appropriately supported. Three specific (and ubiquitous) justice themes emerged. First, in regard to mission-relatedness of the information processed, an information system should include sufficient structure to encourage the request and exchange of only mission-relevant data. Think, for example, of the potential positive impact of designing an email system that prevented people from inadvertently sending highly personal messages to wide distribution lists. Such a system would not prevent people from communicating such information to a trusted confidante, but could provide a friendly warning to help individuals from sharing intimate information beyond the dyadic boundary. Second, information systems that contain or transmit personal data should contain a structure for an appeals process. Double opt-in methods in market research databases exemplify this issue: Such systems pose a final question – are you *sure* you want us to use your demographic data for this purpose – before committing the individual’s personal data to the database. Finally, information systems should communicate to their clients and carefully enforce specific guidelines governing the use of the information in the system. Privacy policies on e-commerce websites provide one example of such guidelines, although it is not always clear that the enforcement behind the policy is sufficient.

CONCLUSION

Future research on the topic of information boundaries could explore the possibilities and limitations of the theoretical framework presented here. As a first step, the idea of a psychological boundary, presented in this paper as an instance of a tacit psychological contract, should find expression as a set of behavioral, attitudinal, and affective constructs pertaining to boundary opening and boundary closure. This step would serve the dual purpose of sharpening the definition of boundaries and supporting a structured method of assessing boundary opening and closure in specific situations. Built on this progress, the general research propositions described in this chapter can then become sharper and more specific a priori

hypothesis statements. Together, these developments would support subsequent exploration of the information boundary framework.

This exploration can take two distinct and equally important forms. First, one set of research projects should focus on testing whether the basic propositions of the framework that received preliminary support in this chapter can survive a retest using different research methods and contexts. Second, a more applied set of projects could include development of specific artifacts, such as an experimental email interface, that embodied some of the ideas for promoting boundary opening suggested in this chapter. Research could then compare such artifacts to their more traditional predecessors to ascertain whether any benefit was derived from including features that enhance users' trust and perceptions of fairness. With basic and applied evidence concerning the utility of information boundary theory, it will be possible to reassess the promise suggested in the present chapter of understanding individuals' motivations to regulate the flow of personal information through the wide variety of information technology systems available now and in the future.

ACKNOWLEDGMENT

This research was supported in part by National Science Foundation award SBR9810137 and in part by award SES9984111. The National Science Foundation does not necessarily endorse the findings or conclusions of this study.

REFERENCES

- Agre, P. E. (1997). Introduction. In Agre, P. E. and Rotenberg, M. (Eds.), *Technology and Privacy, the New Landscape*, 1-28. Cambridge, MA: MIT Press.
- Alder, G. S. (1998). Ethical issues in electronic performance monitoring: A consideration of deontological and teleological perspectives. *Journal of Business Ethics*, 17, 729-743.
- Alder, G.S. and Tompkins, P. K. (1997). Electronic performance monitoring: An organizational justice and concertive control perspective. *Management Communication Quarterly*, 10, 259-288.
- Altman, I. (1975). *The Environment and Social Behavior*. Monterey, CA: Brooks/Cole.
- Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behavior*, 8, 7-29.
- Bies, R.J. (1987). The predicament of injustice: The management of moral outrage. In Cummings, L. L. and Staw, B. M. (Eds.), *Research in Organizational Behavior*, 9, 289-319. Greenwich, CT: JAI Press.

- Bies, R. J. and Moag, J. S. (1986). Interactional justice: Communication criteria of fairness. In Lewicki, R. J., Sheppard, B. H. and Baxerman, M. (Eds.), *Research on Negotiation in Organizations, 1*, 43-55. Greenwich, CT: JAI Press.
- Boon, S. D. and Holmes, J. G. (1991). The dynamics of interpersonal trust: Resolving uncertainty in the face of risk. In Hinde, R. A. and Groebel, J. (Eds.), *Cooperation and Prosocial Behavior*, 190-211. Cambridge, UK: Cambridge University Press.
- Cangelosi, V. E. and Lemoine, L. F. (1988). Effects of open versus closed physical environment on employee perception and attitude. *Social Behavior and Personality, 16*, 71-77.
- Connerly, M. L., Mael, F. A. and Morath, R. A. (1999). Don't ask-please tell: Selection privacy from two perspectives. *Journal of Occupational and Organizational Psychology, 72*, 405-422.
- Dallas v. England, 846 S.W.2d 957, 1993 Tex.App. LEXIS 643 (Tx.Ct.App 1992), rev'd, 849 S.W.2d 941, 1994 Tex. LEXIS 17 (Tex. 1994).
- Deci, E. L. and Ryan, R. M. (1991). Intrinsic motivation and self-determination in human behavior. In Steers, R. M. and Porter, L. W. (Eds.), *Work Motivation*. New York: McGraw-Hill.
- Derlega, V. J., Metts, S., Petronio, S. and Margulis, S. T. (1993). *Self-Disclosure*. Newbury Park, CA: Sage.
- Duvalleary K. and Benedict, J. O. (1992). The relationships between privacy and different components of job-satisfaction. *Environment And Behavior, 24*, 670-679.
- Eddy, E. R., Stone, D. L. and Stone-Romero, E. F. (1999). The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology, 52*, 335-358.
- Feather, N. T. (1988). From values to actions: Recent applications of the expectancy-value model. *Australian Journal of Psychology, 40*, 105-124.
- Feather, N. T. (1995). Values, valences, and choice: The influence of values on the perceived attractiveness and choice of alternatives. *Journal of Personality and Social Psychology, 68*, 1135-1151.
- Fusilier, M. R. and Hoyer, W. D. (1980). Variables affecting perceptions of invasions of privacy in a personnel selection situation. *Journal of Applied Psychology, 65*, 623-626.
- Giacalone, R. A. and Rosenfeld, P. (Eds.). (1991). *Applied Impression Management: How Image-Making Affects Managerial Decisions*. Thousand Oaks, CA: Sage.
- Greenberg, J. (1993). The social side of fairness: Interpersonal and informational classes of organizational justice. In Cropanzano, R. (Ed.), *Justice in the*

- Workplace: Approaching Fairness in Human Resource Management*. Hillsdale, NJ: Erlbaum.
- Greenberger, D. B. and Strasser, S. (1986). The development and application of a model of personal control in organizations. *Academy of Management Review*, 11, 164-177.
- Jones, J. W. and Joy, D. S. (1991). Empirical investigation of job applicants' reactions to taking a preemployment honesty test. In Jones, J. W. (Ed.), *Preemployment Honest Testing: Current Research and Future Directions*, 121-131. New York: Quorum.
- Kahin, B. and Nesson, C. R. (1997). *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*. Cambridge, MA: MIT Press.
- Kirchner, W. K. (1966). A note on the effect of privacy in taking typing tests. *Journal of Applied Psychology*, 50, 373-374.
- LePoire, B. A., Burgoon, J. K. and Parrott, R. (1992). Status and privacy restoring communication in the workplace. *Journal of Applied Communication Research*, 20, 419-436.
- Leventhal, G. S. (1980). What should be done with equity theory? New approaches to the study of fairness in social relationships. In Gergen, K., Greenberg, M. and Willis, R. (Eds.), *Social Exchange: Advances in Theory and Research*. New York: Plenum.
- Lewicki, R. J., McAllister, D. J. and Bies, R. J. (1998). Trust and distrust: New relationships and realities. *Academy of Management Review*, 23, 438-458.
- Moorman, R. H. and Podsakoff, P. M. (1992). A meta-analytic review and empirical test of the potential confounding effects of social desirability response sets in organizational behaviour research. *Journal of Occupational & Organizational Psychology*, 65, 131-149.
- Morrison, E. W. and Bies, R. J. (1991). Impression management in the feedback-seeking process: A literature review and research agenda. *Academy of Management Review*, 16, 522-541.
- Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between marital couples. *Communication Theory*, 1, 311-335.
- Petronio, S. (1994). Privacy binds in family interactions: The case of parental privacy invasion. In Cupach, W. R. and Spitzberg, B. H. (Eds.), *The Dark Side of Interpersonal Communication*, 241-257. Hillsdale, NJ: Lawrence Erlbaum.
- Petronio, S. and Chayer, J. (1988). Communicating privacy norms in a corporation: A case study. Paper presented at the *International Communication Association*, New Orleans, LA.

- Pincus, L. B. and Trotter, C. (1995). The disparity between public and private sector employee privacy protections: A call for legitimate privacy rights for private sector workers. *American Business Law Journal*, 33, 51-89.
- Sarkar-Barney, S., Stanton, J. M. and Line, K. (2001). Crossing the line: When do organizations ask for too much personal data about workers? In Alge, B. J. (Ed.), *Design Considerations in Electronic Workplace Surveillance Systems. Symposium presented at the 16th annual conference of the Society for Industrial and Organizational Psychology*, April, San Diego, CA.
- Shahar v. Bowers, 836 F. Supp. 859, 1993 U.S. Dist. LEXIS 14206 (N.D. Ga., 1993).
- Sipior, J. C., Ward, B. T. and Rainone, S. M. (1998). Ethical management of employee e-mail privacy. *Information Systems Management*, 15, 41-47.
- Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 1991 Cal. App. LEXIS 1241 (Cal. Ct. App. 1st Dist. 1991).
- Spector, P. E. (1982). Behavior in organizations as a function of employee's locus of control. *Psychological Bulletin*, 91, 482-497.
- Stanton, J. M. and Barnes-Farrell, J. L. (1996). Effects of computer monitoring on personal control, satisfaction and performance. *Journal of Applied Psychology*, 81, 738-745.
- Stanton, J. M. (2000). Traditional and electronic monitoring from an organizational justice perspective. *Journal of Business and Psychology*, 15, 129-147.
- Stanton, J. M. and Weiss, E. M. (2000). Electronic monitoring in their own words: An exploratory study of employees' experiences with new types of surveillance. *Computers in Human Behavior*, 16, 423-440.
- Stone, D. L. and Stone E. F. (1987). Effects of missing application blank information on personnel selection decisions: Do privacy protection strategies bias the outcome? *Journal of Applied Psychology*, 72, 452-456.
- Stone, D. L. and Stone-Romero, E. F. (1998). A multiple stakeholder model of privacy in organizations. In Schminke, M. (Ed.), *Managerial Ethics: Moral Management of People and Processes*, 35-59. Mahwah, NJ: Erlbaum.
- Stone, E. F. and Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings and protection mechanisms. *Research in Personnel and Human Resources Management*, 8, 349-411.
- Stone, E. F., Gueutal, H. G., Gardner, D. G. and McClure, S. (1983). A field experiment comparing information privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68, 459-468.
- Thorne v. El Segundo, 726 F.2d 456 (9th Cir. 1983), cert. denied, 469 U.S. 979 (1984).

- U. S. Congress, House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property. (2000). Electronic communication privacy policy disclosure: hearing before 106th Congress, 1st session, May 27, 1999. Washington, DC : U.S. G.P.O.
- U.S. Dep't. of Health, Education and Welfare. (1973). Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii., Author: Washington, DC: Government Printing Office.
- Woodman, R. W., Ganster, D. C., McCuddy, M. K., Tolchinsky, P. D. and Fromkin, H. (1982). A survey of the perceptions of information privacy in organizations. *Academy of Management Journal*, 25, 647-663.