

## Association for Information Systems AIS Electronic Library (AISeL)

---

AMCIS 2007 Proceedings

Americas Conference on Information Systems  
(AMCIS)

---

December 2007

# Electronic Monitoring in Workplace: Synthesis and Theorizing

Rui Chen

*State University of New York at Buffalo*

G. Lawrence Sanders

Follow this and additional works at: <http://aisel.aisnet.org/amcis2007>

---

### Recommended Citation

Chen, Rui and Sanders, G. Lawrence, "Electronic Monitoring in Workplace: Synthesis and Theorizing" (2007). *AMCIS 2007 Proceedings*. 279.

<http://aisel.aisnet.org/amcis2007/279>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# **ELECTRONIC MONITORING IN WORKPLACE: SYNTHESIS AND THEORIZING**

**Rui Chen and G. Lawrence Sanders**  
**Management Science & Systems**  
**State University of New York at Buffalo**  
ruichen@buffalo.edu mgtsand@acsu.buffalo.edu

## **Abstract**

*This paper explores the electronic monitoring in workplace and it discusses the monitoring consequences. The authors synthesize the prior research in electronic workplace monitoring and discuss a set of related research issues. The paper draws on organizational theories, privacy theories, and control theories to examine the strategies of organizational policy design as one solution to address the employee privacy issues. The multi-theoretic lens highlights the contingency between organizational policy and employee behaviors and it posits the long term impact of monitoring. This paper contributes to the theory development of electronic monitoring in the workplace and to the practice of organizational management as well.*

## **Introduction**

An increasing number of organizations are using information technologies (IT) to monitor the employee performance in the workplace. The American Management Association and ePolicy Institute conducted the 2005 Electronic Monitoring & Surveillances Survey with 526 U.S. companies (AMA 2005). The results reveal the workplace electronic monitoring status quo in terms of the variety and extent: 76% organizations monitor employee's website connection, 50% of them store and review employees' computer files, and 55% organizations retain and review email messages. The proliferation of workplace monitoring may also be inferred from the software market which produces the monitoring equipments. According to IDC, the market for secure content-management software, applications that monitor Web surfing, e-mail, instant messaging, and even keystrokes, is expected to grow to \$6.4 billion by 2007.

Inevitably, electronic workplace monitoring introduces conflict between business interests and employee privacy rights. Management utilizes monitoring to protect business intelligence, reduce mischief, and enhance IT security. Employees, however, consider monitoring as a direct threat to their privacy with an accompanying potential for misuse of personal information. Despite early exploratory work (Flanagan 1994; George 1996; Ariss 2002), the electronic workplace monitoring dispute has not been fully addressed as it lacks theoretical foundations related to the causes and impacts of monitoring practices.

The contributions of this paper are two-fold. First of all, we examine the multi-faceted nature of electronic workplace monitoring in order to understand and integrate the diverse viewpoints related to monitoring. Secondly, we incorporate prior studies into the development of a conceptual model which captures the dynamic of electronic workplace monitoring. The model is grounded in the literature and it assists in predicting the design impacts and how they influence

Chen and Sanders, *Electronic Monitoring in Workplace*

employee perceptions related to privacy invasion. The model further predicts how monitoring will effect employee commitment toward the organization.

The paper is organized as follows. In the next section, we provide a comprehensive review of the workplace electronic monitoring debate. Then we present the theoretical background and the development of research model. The last section of the paper discusses the research implications of our research model.

## **Literature Review of Electronic Monitoring in Workplace**

The central debate concerning workplace monitoring is captured by the following quote:

“Employers want to be sure their employees are doing a good job, but employees don't want their every sneeze or trip to the water cooler logged. That's the essential conflict of workplace monitoring. <http://www.privacyrights.org/fs/fs7-work.htm>”

In this section, we will summarize prior research findings on electronic workplace monitoring with the objective of attempting to reconcile and address the ongoing dispute between management and employees.

Fairweather studied the “teleworking” workers and found electronic monitoring makes employees feel isolated and causes them to perceive strong sense of privacy invasion (Fairweather 1999). In a review article, George summarized the prior findings on the negative impacts of monitoring and found that workplace monitoring lead to anxiety, depression, fear, stress, and illness. Others found that monitoring may result in overly paced work, lack of involvement, reduced social support from peers and supervisors, and fears of job loss (Ariss 2002; Meyers 2003).

Despite the these concerns by employees, electronic monitoring has received wide support and its growth is expected to continue (George 1996; Shopis 2003). First of all, the workplace monitoring is considered as an important control measure for business necessity for the following reasons: (1) workplace monitoring may prevent the misuse of the organizational resources and the related expenses incurred, (2) it may enhance the company security in terms of business secrets, intellectual assets, and corporate knowledge, (3) monitoring may lead to the avoidance of legal liabilities resulted from employee misbehaviors, and (4) monitoring may increase the employee performance (Ariss 2002).

Workplace electronic monitoring is supported by the existing laws and regulations despite the perception held by employees that they have the right of privacy in the workplace. Flanagan found that most of the existing laws and market forces have not yet produced appropriate frameworks to control the proliferation of electronic monitoring (Flanagan 1994). Many of the existing laws and regulations (such as the Electronic Communications Privacy Act of 1986) are applicable only to non-computer based workplace monitoring while the others (such as state tort laws) grant permission to the electronic monitoring practices as long as the organizations have business reasons to do so (Galkin 1995). The increased concern for homeland security further promotes the legal systems to advocate the workplace electronic monitoring by passing laws such as The Patriot Act.

Most importantly, the implicit contractual relationships in the workplace warrant the acceptance of electronic monitoring by employees. Klepper and Jones suggest that the contract is the ultimate organizational management tool (Klepper and Jones 1998). The classical arms-length contractual relationship functions as a rent-generating administrative practice to enforce workforce control (Oosterhout, Heugens et al. 2006). The contractual relationship, as defined in written and psychological forms, prescribes appropriate behaviors, assists in establishing rule structures, and facilitates the development of a normative environment for the employee. Once formalized and made explicit, electronic monitoring is deemed as a mutual-agreed organizational practice by employees who choose to accept the contractual relationship (Kobayashi and Ribstein 2002). This subsequently reduces employees' angst towards electronic monitoring since existing employees are effectively granting permissions to monitoring.

## Chen and Sanders, Electronic Monitoring in Workplace

The above discussion suggests that employees should not assume that they have so-called rights to individual privacy in the workplace. Employees effectively surrender their privacy when they choose to accept a contractual relationship to be monitored in the workplace. In essence the contract establishes the appropriate expectations for privacy and gives employees the capabilities to make informed choices about their behaviors (Fisher 2002). Many people do not understand that they have surrendered their right to privacy when they go to work. The misunderstanding among the employees of the current regulations and legal practices intensifies this situation. Because workplace electronic monitoring practice has been widely adopted and expected to grow, a major challenge is how to effectively design monitoring practices so as to minimize the negative effects while achieving the monitoring goals.

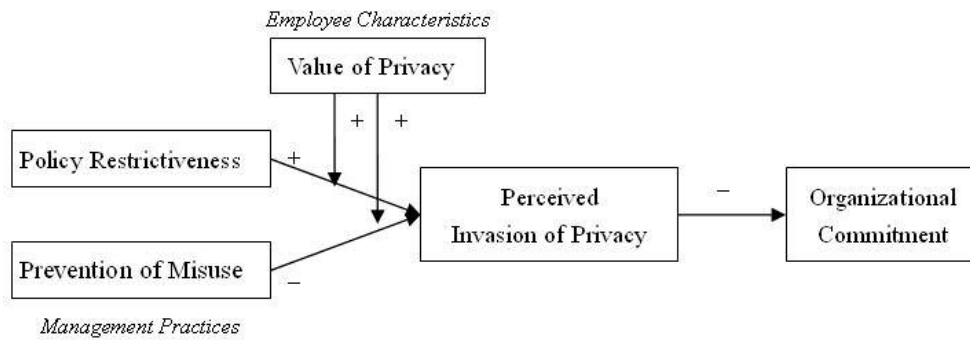
George suggested that workplace monitoring is a malleable practice: “Managers have a key role to play in designing systems that are effective yet are not viewed as too onerous or invasive” (George 1996). Through five large case studies, George found empirical evidence for the impacts of design on employee perceptions. He concluded that employees may tolerate workplace monitoring and even approve it if the managers designed the system appropriately. Ariss (2002) has noted the importance of using judgment in designing monitoring systems. He believed that such judgment should be contextual and based on the unique characteristics of the workplace and the employees and that the various issues surrounding ethical, legal, and employee relationship can be dealt with effectively.

Prior studies have discussed general guidance and strategies for workplace electronic monitoring. Ariss (2002) proposed a set of recommendations which included monitoring necessary activities, obtaining monitoring consent from employees, developing written organization policies on activities allowed, and a careful calculation of the social and monetary costs of excessive monitoring. Flanagan (1994) highlighted the rule of restrains to manage the information obtained. King (2003) advocated the control and restraint on the monitoring level as a mechanism to reduce the tension and ensure long-term gains. In general, an appropriate management strategy for electronic monitoring should (1) utilize the organizational management resources to reduce the employees’ negative attitude toward monitoring, and (2) enforce the privacy protection to avoid the incidents such as employee privacy information misuse.

Organizational policyfunction s as a major tool to convey the business rationale, the monitoring rules, and how information recorded will be used. Organizational policy has received limited attention in previous research on electronic monitoring and its importance in design strategies has remained largely unknown (Eddy 1997; Fisher 2002). In this study, we explore the design options of organization policies with their potential impacts on the employee privacy concerns. We also examine the causal path from policy design toward the organizational behaviors such as employee commitment. Finally, we study the individual traits (such as value of privacy) with its potential impact on the policy effectiveness. This assists in the development of a conceptual research model to help the practitioners better understand strategies in designing monitoring systems.

### **3. THEORETICAL DEVELOPMENT**

Figure 1 presents a research model of workplace privacy invasion. The restrictiveness of organizational policies, the prevention of privacy misuse, and the value of individual privacy are argued to influence the individual’s perceived invasion of privacy. The perceived invasion of privacy in turn affects employee commitment to the organization.



**Figure 1: Organizational Policy Design and Employee Privacy Concerns**

Organizational research has described the workplace employee privacy as a multi-faceted concept (Westin 1967; Marshall 1970; Woodman, Ganster et al. 1982). Fisher summarized workplace privacy as the “control over the disclosure of information, control over social interaction, personal space, territoriality, power, autonomy, individuality, intimacy, and solitude” (Fisher 2002). Stone and Stone defined the invasion of privacy as the perception of personal information release, constrained social interactions, and unnecessary external influences (Stone and Stone 1990).

Prior research suggests that the content of organizational policy has an influence on the employee privacy concerns with their social interactions and external influence controls. The policy content is an important part of organizational policy design in that it specifies the regulation details as well as the reinforcement to assure the expected employee behaviors. The existing literature has identified policy restrictiveness as an important attribute of policy content (Swanson 1993). Policy restrictiveness refers to the extent that (1) personal use of organizational resources, and, (2) non-business related activities are prohibited (Frairweather 1999). For policies that place restrictions in the workplace, the employees may perceive that they are being overly controlled and that their privacy has been breached (Stone and Stone 1990). In organizations where electronic monitoring is absent, Fisher found that the restrictiveness of an Email use policy influences the employees’ perception toward privacy invasion (Fisher 2002). This finding should be interpreted with caution. Unlike scenarios where monitoring is not enforced, the employee personal information leakage in a monitored workplace is known to exist. As a core dimension of the invasion of privacy construct, the perceived information leakage increases the level of privacy invasion. Fisher deemphasized the information leakage dimension in the study. The certainty in privacy loss, which is resulted by workplace monitoring, may cast dominant influence on the employees’ attitude forming on how they perceive the level of privacy invasion. This may render the organizational policy restrictiveness no longer a functional mechanism in addressing the workplace privacy issues.

A re-examination of the above research question is of critical importance to the researchers and practitioners in determining whether organization policy restrictiveness can be used as a valid management tool to reduce the unfavorable consequences in a monitored workplace. Stone and Stone’s privacy framework along with the psychology literatures suggest that when organizations grant employees flexibility and freedom, employees might be likely to reduce privacy concerns related to the monitoring systems. It is reasonable to argue that, in the context of monitored workplace, a low level of restrictiveness of the organizational policy may help reduce the perceived invasion of privacy. For example, employees in a monitored but less restrictive workplace may feel that their privacy has been invaded to a lesser degree compared with those in a monitored but much more restrictive environment. Organizations might consider relaxing monitoring policy to offset negative employee attitudes toward workplace monitoring. Thus:

*Proposition 1: Restrictiveness of organization policy in a monitored workplace will be positively related to the level of employee’s perceived invasion of privacy*

## Chen and Sanders, Electronic Monitoring in Workplace

The policy design strategies related to restrictiveness are concerned with policy content feature. It does not, however, address the procedural dimension of organization policies (Fisher 2002). The procedural characteristics of organization policies prescribe the way an organization administers the policies. In the context of electronic workplace monitoring, the key policy procedure is related to the management of the collected employee privacy information in terms of access, usage, and release. Shopis (2003) found that the employees are particularly concerned about the organizational use of their private information because of the high volume of usage violations reported. Captured information from employees may be used for purpose other than business management, such as humiliation, marketing, and crimes (Meyers 2003). This notion introduces the concept of perceived privacy risks to employees.

A number of researcher have studied the employee privacy risk issues in the IS literature. Among the early studies, Woodman et al (1982) surveyed two thousand corporate employees with regard to their concerns about the company's handing of personal information. They found that the employees perceived privacy risks when the organization disclosed their personal information to outsiders. Similarly, Eddy tested the organizational policies with regard to the privacy rules and found that the employee were concerned about their ability to authorize the information disclosure (Eddy 1997). Smith et al. found that employees rated the unauthorized secondary use and improper access to employee information as major privacy risk concerns (Smith, Milberg et al. 1996). The preventive mechanisms against misuse (unauthorized access, unauthorized release, and inappropriate use) of employee privacy information, therefore, may protect the employee personal information from flowing into illegitimate and vicious recipients. Control theories suggest that the centrality of control beliefs is essential to human attitudes and that the establishment of prevention mechanisms helps restore the employee's feelings of the control over the release of his or heir privacy information (Potter 1966; Phares 1976; Klein 1989). The prevention schemes may consequently reduce the perception of invasion of privacy (Stone and Stone 1990).

*Proposition 2: Prevention of the misuse of monitored information in organization policy will be negatively related to the perceived invasion of privacy*

Privacy researcher have found that individuals differ in their values of privacy (Stone and Stone 1990; Dinev and Hart 2006). The value of privacy refers to the importance an individual places on personal privacy (Fisher 2002) and it may be cultivated by personalities, cultures, and previous privacy invasion experience (Milberg, Burke et al. 1995; Awad and Krishnan 2006). Within the context of the monitored workplace, the value of privacy may conflict with the monitoring practices. As employees differ in their values of privacy, this may explain the individual differences in their attitudes towards electronic monitoring (George 1996). Further, it may predict the effectiveness of organization policy designs, in terms of restrictiveness and misuse prevention, on the individual employees. That is, employees with high values of privacy may be less influenced by the changes in organization policy restrictiveness and misuse prevention, when compared with individuals with low privacy values. Such moderating effects have not been fully examined by prior studies and earlier findings are problematic. For example, Fisher tested the moderating effects of privacy values, in the context without electronic monitoring, but did not find evidence of that (Fisher 2002). Workplace electronic monitoring represents a highly intrusive environment; therefore, the value of privacy may be a salient and strong factor and may have a moderating effect on policy designs. We therefore propose the following propositions.

*Proposition 3a: The value of privacy will positively moderate the relationship between policy restrictiveness and the perceived invasion of privacy*

*Proposition 3b: The value of privacy will positively moderate the relationship between prevention of misuse and the perceived invasion of privacy*

Early research work in workplace privacy suggests that the perceptions of employee privacy invasion result in anxiety, depression, fear, illness, low autonomy, low self-esteem, and workplace stress (Sundstorm 1986; Stone and Stone 1990; George 1996; Meyers 2003). The research, however, is at best scanty in predicting the long-term impacts of privacy invasion. Organizational commitment has long been recognized as a key topic in the organizational behavior

Chen and Sanders, *Electronic Monitoring in Workplace*

research because it gauges employee attitudes toward the firms as well as the health of workplace relationships (Cooper-Hamik and Viswesvaran 2005). Mowday et al (1958) found that low level of organizational commitment may directly impact on the job performance, absenteeism, and even the employee turn over (Strickland 1958; Mowday, Porter et al. 1982). As suggested by the resource-based theories of the firm, high potential loss in human resources may jeopardize the firm's long-term growth and sustained competitive advantages (Wade and Hulland 2004). Organizational commitment issues, therefore, have to be carefully examined in the strategic management decisions of any firm.

Meyer and Allen found that organizational commitment has three general themes: affective attachment, perceived costs and obligations (Meyer and Allen 1987). Affective attachment refers to the emotional connection with the organization and it may be reflected in the individual's identity in the organization and his or her enjoyment of membership. The perceived costs theme is also referred to as "continuous" commitment and it suggests that the employee's commitment to an organization is based on economic benefits. The obligation theme refers to the perceived responsibility in staying in the organization rather than leaving it. Meyer and Allen described the three commitment themes as "employees with strong affective commitment remain because they want to, those with strong continuous commitment because they need to, and those with strong normative commitment because they feel they ought to do so." In our study, we focus on the affective attachment as it is most related to the context and our research interest.

Mastrangelo and Popovich suggested that privacy-related attitudes are likely to impact employees' feeling toward the organization (Mastrangelo and Popovich 2000). As electronic monitoring introduces privacy invasion in the workplace, the affective attachment to the organization may therefore be greatly threatened. Hovorka-Mead et al suggested that the employees may perceive being less important and perceive a lack of respect when their privacy is invaded, which may lead to lowered level of organizational commitment (Hovorka-Meda, Ross et al. 2002). Tabak and Smith pointed out that the privacy invasion may also destroy the perceived organizational identity, which antecede organizational commitment (Tabak and Smith 2005). Belanger et al. also posited that the effects of privacy concerns resulted by workplace monitoring may negatively influence the employees' commitment to the organization. On the basis of the above discussion, we propose the following proposition.

*Proposition 4: Perceived invasion of privacy will be negatively correlated with the affective commitment to organization*

## **Discussion and Conclusion**

This paper investigates electronic workplace monitoring phenomena by attempting to synthesize the varying viewpoints of the monitoring practices. It is posited that the proper design of employee monitoring strategies may assist in alleviating the workplace privacy concerns. This paper explores the area of organization policy design with its potential impacts on the monitoring outcomes. The paper also investigates into the relationship between policy design and individual perceived privacy invasion. Through the lens of privacy theories and control theories, the paper suggests that the policy restrictiveness may increase the perceived privacy invasion while the misuse prevention may dampen the perception of privacy invasion. Unlike earlier research, this paper further studies the long-term impact, i.e. organization commitment, of electronic monitoring upon the employees. As a key index of management effectiveness, organization commitment may be influenced by the perception of privacy invasion.

The paper contributes to organizational research in two areas. First, it reviews and reconciles the prevailing debates and suggest a new direction for workplace monitoring research. Secondly, it delves into the workplace monitoring designs and considers how they can alleviate the perception of privacy encroachment. This paper also has implications on practice. Grounded on the relevant literatures, it lays the foundations for the workplace electronic monitoring by shedding light on the management strategies (i.e., organization policy) that enable practitioners to leverage the expected benefits of electronic monitoring while restraining the unfavorable consequences.

## Chen and Sanders, Electronic Monitoring in Workplace

There are a number of avenues to further extend the current research. First, future study may explore the role of organizational trust and how it may effect the monitoring issues (Alder, Noel et al. 2006). Prior research suggest that trust is an important predictor of workplace behaviors and it functions as an effective and information control mechanism to bond the employee to the organization (Mayer, Davis et al. 1995; Lewicki, McAllister et al. 1998; Zaheer, McEvily et al. 1998; McEvily, Perrone et al. 2003). It is therefore important to study how the workplace monitoring may impact on the organizational trust and how the firms may protect and foster employees' trust toward the organization. Second, future research may examine management design concerns such as distributive fairness and procedural fairness (Eddy, Stone et al. 1999; Aycan and Kabasakal 2006). Third, future research also includes the empirical testing of the research model. To maximize the variances, data may be collected through surveying employees from separate firms which are enforcing monitoring policies with difference levels of restrictiveness and misuse prevention schemes.

## Reference

- Alder, G. S., T. W. Noel, et al. (2006). "Clarifying the Effects of Internet Monitoring on Job Attitudes: The Mediating Role of Employee Trust." Information & Management **43**(7): 894-903.
- AMA (2005). 2005 Electronic Monitoring & Surveillance Survey, American Management Association & ePolicy Institute.
- Ariss, S. S. (2002). "Computer Monitoring: Benefits and pitfalls facing management." Information & Management **39**: 553-558.
- Awad, N. F. and M. S. Krishnan (2006). "The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization." MIS Quarterly **30**(1): 13-28.
- Aycan, Z. and H. Kabasakal (2006). "Social Contract and Perceived Justice of Workplace Practices to Cope with Financial Crisis." Group Organization Management **31**: 469.
- Cooper-Hamik, A. and C. Viswesvaran (2005). "The Construct of Work Commitment: Testing an Integrative Framework." Psychological Bulletin **131**: 241-258.
- Dinev, T. and P. Hart (2006). "An Extended Privacy Calculus Model for E-Commerce Transactions." Information Systems Research **17**(1): 61-80.
- Eddy, E. R. (1997). *The Effects of Information Management Policies on Reactions to Human Resource Information Systems*, University at Albany.
- Eddy, E. R., D. L. Stone, et al. (1999). "The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives."
- Fisher, J. G. (2002). *Implications of Electronic Mail Policies of Fairness and Invasion of Privacy: A Field Experiment*, University at Albany.
- Flanagan (1994). "Restricting Electronic Monitoring in the Private Workplace." Duke Law Journal **43**(6): 1256-1281.
- Frairweather, N. B. (1999). "Surveillance in Employment: The Case of Teleworking." Journal of Business Ethics **22**(1): 39.
- Galkin, W. S. (1995). *Electronic Privacy Rights: The Workplace*. The Computer Law Report.
- George, J. F. (1996). "Computer-based Monitoring: Common Perceptions and Empirical Results." MIS Quarterly **20**(4): 459.
- Hovorka-Meda, A., W. H. Ross, et al. (2002). "Watching the Detectives: Seasonal Student Employee Reactions to Electronic Monitoring with and without Advance Notification." Personnel Psychology **55**(329-362).
- Klein, H. (1989). "An Integrated Control Theory Model of Work Motivation." Academy of Management Journal **14**(2): 150-172.
- Klepper, R. and W. O. Jones (1998). Outsourcing Information Technology, Systems and Services. Upper Saddle River; NJ, Prentice Hall.
- Kobayashi, B. and L. Ribstein (2002). "Privacy and Firms." Denv. U.L. Review **526**.



Chen and Sanders, *Electronic Monitoring in Workplace*

- Lewicki, R. J., D. J. McAllister, et al. (1998). "Trust and Distrust: New Relationships and Realities." *Academy of Management Review* **23**(3): 438-458.
- Marshall, N. J. (1970). *Orientations toward Privacy: Environmental and Personality Components*, University of California, Berkeley.
- Mastrangelo, P. M. and P. M. Popovich (2000). "Employees' Attitude Toward Drug Testing, Perceptions of Organizational Climate, and Withdrawal From the Employer." *Journal of Business and Psychology* **15**(1).
- Mayer, R. C., J. H. Davis, et al. (1995). "An Integrative Model of Organizational Trust " *Academy of Management Review* **20**(3): 709-734.
- McEvily, B., B. Perrone, et al. (2003). "Trust as an Organizing Principle." *Organization Science* **14**(1): 91-103.
- Meyer, J. P. and N. J. Allen (1987). *Organizational Commitment: Toward a Three-Component Model*. *Research Bulletin*, The University of Western Ontario. **660**.
- Meyers, N. (2003). *Employee Privacy in the Electronic Workplace: Current Issues for IT Professionals*. 14th Australasian Conference on Information Systems, Perth, Western Australia.
- Milberg, S. J., S. J. Burke, et al. (1995). "Values, Personal Information Privacy, and Regulatory Approaches " *Communications of the ACM* **38**(12): 65-74.
- Mowday, R. T., L. W. Porter, et al. (1982). *Organizational Linkage: The Psychology of Commitment, Absenteeism, and Turnover*. San Diego, CA, Academic Press.
- Oosterhout, j. V., P. Heugens, et al. (2006). "The Internal Morality of Contracting: Advancing the Contractualist Endeavor in Business Ethics." *Academy of Management Review* **31**(3): 521-539.
- Phares, E. J. (1976). *Locus of Control in Personality*. Morristown, NJ, General Learning Press.
- Potter, J. B. (1966). "Generalized Expectancies for Internal Versus External Control of Reinforcement." *Psychological Monographs* **80**(1).
- Shopis, M. (2003). "Employee Monitoring: Is Big Brother A Bad Idea."
- Smith, H. J., S. J. Milberg, et al. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *MIS Quarterly* **20**(2): 167-196.
- Stone, E. F. and D. L. Stone (1990). "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." *Research in Personal and Human Resource Management* **8**: 349-411.
- Strickland, L. H. (1958). "Surveillance and Trust." *Journal of Personality* **26**(200-215).
- Sundstorm, E. (1986). *Workplaces: The Psychology of Physical Environment in Offices and Factories*. Cambridge, Cambridge University Press.
- Swanson, D. J. (1993). *Toward a policy for managing the use of computer mediated communication in the workplace*. 4th Annual Sooner Communications Conference, Norman, OK.
- Tabak, F. and W. P. Smith (2005). "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development." *Employee Responsibilities and Rights Journal* **17**(3): 173.
- Wade, M. and J. Hulland (2004). "The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research." *MIS Quarterly* **28**(1): 107-142.
- Westin, A. F. (1967). *Privacy and Freedom*. New York, Atheneum.
- Woodman, R., D. Ganster, C, et al. (1982). "A Survey of Employee Perceptions of Information Privacy in Organizations." *Academy of Management Journal*.
- Zaheer, A., B. McEvily, et al. (1998). "Dose Trust matter? Exploring the Effects of Interorganizational and Interpersonal Trust on Performance." *Organization Science* **9**(2): 141-159.