Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Workplace Internet Use Monitoring and Employee Behavior Intention Change

Qinyu Liao
UT Brownsville

Xin Luo
Virginia State University

Anil Gurung
Kansas State University

Long Li
Virginia Commonwealth University

Workplace Internet Use Monitoring and Employee Behavior Intention Change

Qinyu Liao
The University of Texas at Brownsville and Texas South Most College, USA
Qinyu.liao@utb.edu

Xin Luo
Virginia State University, USA
xluo@vsu.edu

Anil Gurung
Kansas State University, USA
agurung@acm.org

Long Li
Virginia Commonwealth University, USA
lil3@vcu.edu

Abstract

The use of Internet in workplace has brought about concerns for companies. Previous researches focused on the effect of electronic control on employee productivity and job satisfaction. This paper uses the Theory of Planned Behavior and Deterrence Theory to understand the factors that could affect the workplace Internet use behavior intention. The results will provide insightful suggestions for improving workplace Internet use management with less costly and proactive approaches that can cultivate employee voluntary avoidance of Internet misuse.

Keyword*: workplace Internet use monitoring, Internet use, Internet use monitoring, behavior intention change*

Introduction

The explosive growth of Internet use has brought about an escalation of concerns for corporate Americans. The advantages of quick access to timely data and less restricted communications resulting from Internet connectivity in organizations have been accompanied by reduced productivity, increased legal liability, bandwidth waste, and information security concerns (Sandler 2002).

Employees using the Internet for non-work related activities can result in lost of both personal and system productivity, and ultimately profit. Internet addiction has been another concern affecting employee wellness on productivity. When an employee is Internet addictive, they tend to neglect their job responsibilities, decrease physical activity, be more irritable and diminish self worth and control, which can lead to workplace stress, employee absenteeism, reduced safety, reduced productivity, and ultimately lost profit (Davis 2003).

Legal liability can occur when employees improperly use web resources. Improper usages ranges from copyright infringement to sexual harassment issues associated with web pages containing pornographic content, and inappropriate emails that promote a hostile work environment (Boncella 2001).

Web users are more likely to access broadband entertainment sites than at home because of the high-speed connection at office. As broadband applications over the Internet continue to become increasingly popular, corporate networks are becoming bottlenecked with slower networks and increased network crashes. Network quality of service is the most important factor for some businesses and the bandwidth waste by employee Internet misuse hurt the company's ability to keep up with competition.

Security concern refers to both computer system and company information. Computer security can be compromised if an employee either intentionally or unintentionally downloads a virus or opens an email that contains a Trojan Horse program as an attachment. The proprietary corporate information is another primary concern when email and Internet connections can impose the risk for unauthorized access to them. Employers' greatest risk to their computer security comes not from outside hackers but from current and former employees who deliberately or inadvertently disclose confidential or sensitive information.

To deal with the far-reaching types of misconduct and risks faced, organizations have responded by creating the position of Chief Privacy Officer or using Internet usage monitoring technologies (Levin-Epstein 2002; Sandler 2002). Some of the major parameters for Internet monitoring are site visited, download time, time on the Internet, download size and email content (Davis 2003). Corporate can conduct Internet monitoring by supervising browser activity and email, using intrusion detection systems and remote control programs.

Managing the corporate Internet resource is becoming more difficult and increasing in importance. The concern for employee privacy, cost and the monitoring management has prompted many companies to weigh the tradeoffs in workplace Internet monitoring. Employee privacy is the most controversial issue (Ward 1997). The cost of workplace Internet monitoring includes the expenses for software, equipment, IT personnel as well as the opportunity cost of production time spent in monitoring.

Companies might have increased liability if they say that they monitor the workplace Internet use but actually don't (Martin 1997). Companies can suddenly have a duty to investigate everything (Zimmerman 2002) associated with Internet use that can procrastinate the cost for monitoring software and personnel. The normal practices are spot-check targeting areas of high risk or random check for cause basis instead of ongoing 24 hours basis to save cost of monitoring (Aikin 2000; Greco 2001). An intangible cost of Internet use monitoring is the effect on employee. Studies showed that monitoring has a detrimental effect on employee moral and an increase in employee stress (Zimmerman 2002).

Although increasing number of companies are using workplace Internet monitoring software, one-third of them still have no Internet Access Policy (Greco 2001). It has been suggested that a clearly defined Internet access policy should be established and disseminated through training programs to notify employees up front. This proactive approach can improve employee productivity in the long run with minimum monitoring.

It is important for managers to understand how Internet access policy and Internet use monitoring affect employee Internet use behavior so that technology and Internet access policy could be tailored to improve productivity, user satisfaction while ultimate the benefit of the technology. In this study, the Theory of Planned Behavior (TPB) and Deterrence Theory are used to investigate factors that can change employee workplace Internet use behavior intention and suggestions are provided for organizations to cultivate employee voluntary avoidance of Internet misuse.

Theoretical Development

Literature Review

Previous research in the area of employee Internet use management have generally being manifested in the form of industry-driven surveys, case study or controlled lab experiments. Few studies have primarily examined different types of monitoring and their effects. Chalykoff and Kochan's (1989) work studied the effects of electronic monitoring on job satisfaction and turnover intent. Straub and Nance (1990) examined how IS managers discovered and disciplined computer abuse in organizations. Among the two classes of countermeasures that have been found effective, deterrents are passive and preventives are more active. Based on his study, he suggests that there is a need for increased organizational detection activities that focus on hardware and service disruption abuses. George (1996) analyzed five cases to determine the effect of electronic monitoring on service employees' job performance. Urbaczewski and Jessup (2002) indicated that electronic monitoring can be used to provide feedback and implement control, and is a tradeoff between productivity and satisfaction. They also pointed out that positive forms of monitoring can be more instructive and acceptable to employees than negative forms of monitoring.

The Internet e-management framework introduced by Case and Young (2002) was the first to study the impact of employee Internet use management on productivity by investigating both employee and organization factors. The constructs identified are e-management, enforcement, job necessity, and e-behavior. However, Case and Young (2002) also found out that e-management measures are not implemented by most organizations for reasons like cost and privacy issues. Companies are relatively lenient in reacting to employee workplace Internet misuse and there is a general absence of a proactive Internet culture. Their research results suggested that education may be necessary to minimize the problems associated with employee Internet misuse. Young's Internet E-management framework didn't further investigate the causes of employee Internet use behavior.

Zweig and Websteb(2003) find that emotional stability and extraversion altered the relationships between the paths in a model of monitoring acceptance. That is, people who scored lower in extraversion and emotional stability were less likely to endorse positive attitudes toward monitoring, even with privacy and fairness safeguards in place. Harrington (1996) discovered that codes of ethics had little effect on computer abuse judgments and intentions relative to the psychological trail of responsibility denial. There are also studies on the impact of Internet monitoring on employee attitudes and behaviors, such as the perceptions of privacy (Alge 2001), fairness and justices (Alge 2001; Stanton 2000), and work stress. A critical task facing organizations and researchers is to identify the factors that improve employees' attitudinal and behavioral reactions to Internet monitoring.

Theory of Planned Behavior

The Theory of Planned Behavior (TPB) was designed to predict behavior across many settings. It provides more specific information as to what users consider when making a decision (Mathieson 1991). According to the theory, behavior intention is jointly determined by three factors: attitude toward the behavior, subjective norms, and perceived behavioral control. TPB has been successfully applied to the understanding of individual acceptance and usage of many different technologies (Harrison, Mykytyn & Riemenschneider 1997; Mathieson 1991; Taylor and Todd 1995). TPB is used here to investigate how Internet use management (Internet use policy, and training programs) affects employee Internet behavior. Based on TPB, we propose that an employee's workplace Internet use behavior is simultaneously determined by such factors as positive or negative evaluative affect about the monitoring, perception of others opinions on whether or not to use monitoring technology, and perception of the availability of the skills, resources and opportunities necessary for understanding how the monitoring system works. Therefore, it is proposed that a more positive attitude towards Internet monitoring, a high level of subjective norms towards committing Internet misuse, and a high level of perceived behavioral control will all lead to greater intention to avoid Internet misuse.

The importance of attitude, subjective norms, and perceived behavioral control are expected to vary across situations (Ajzen 1991). Therefore, it is necessary to examine the significance of each factor in predicting the Internet misuse behavior intention.

Attitude is a function of the products of behavioral beliefs and outcome evaluation. A behavioral belief is the subjective probability that the behavior will lead to a particular outcome. The outcomes are fairly specific, utilitarian outcomes, such as "Using the monitoring technology will reduce non-work related Internet use time compared to current methods." An outcome evaluation is a rating of the desirability of the outcome. Attitude has been proposed to influence behavioral intentions in

multiple theories, such as TPB (Ajzen 1991) and the TRA (Fishbein and Ajzen 1975). The theoretical predictions of these theories have received substantial empirical support in multiple contexts. Applied to this study, favorable attitude toward workplace Internet use monitoring is likely to encourage employees to avoid workplace Internet misuse, reduce Internet use time on non-work related tasks, and voluntarily follow organization Internet use policies. This leads to the following hypotheses:

H1: A more positive attitude toward Internet monitoring will lead to greater intention to avoid Internet misuse.

Subjective norms reflect the perceived opinions of referent others. A "referent other" is a person or group whose beliefs may be important to the individual. A normative belief is the individual's perception of a referent other's opinion about the individual's performance of the behavior. Motivation to comply is the extent to which the person wants to comply with the wishes of the referent other. According to previous researches, subjective norms have an impact on individual behavior through three mechanisms: compliance, internalization, and identification (Venkatesh & Davis 2003; Warshaw 1980). While the later two relate to altering an individual's belief structure and/or causing an individual to respond to potential social status gains, the compliance mechanism causes an individual to simply alter his or her intention to response to the social pressure. Prior research suggests that individuals are more likely to comply with others' expectations when those referent others have the ability to reward the desired behavior or punish nonbehavior (French & Raven 1959; Warshaw 1980). This view of compliance is consistent with results in the technology acceptance literature indicating that reliance on others' opinions is significant only in mandatory settings (Hartwick & Barki 1994), particularly in the early stages of experience while an individual's opinions are relatively ill-informed (Agarwal & Prasas 1997; Hartwick & Barki 1994; Karahanna et al. 1999; Taylor & Todd 1995; Thompson et al. 1994; Venkatesh & Davis, 2003). Chiasson and Lovato (2001) reported that subjective norm is a significant antecedent of IS adoption intention, and Morris and Venkatesh (2000) found that IS workers were strongly influenced by subjective norm.

Some researches suggested that not only perceived social pressures but also personal feelings of moral obligation or responsibility to perform, or refuse to perform, a certain behavior (Levin-Epstein 2002; Pomazal & Jaccard 1976; Schwarz & Tessler 1972) are influenced by subjective norm. Such moral obligations would be expected to influence intentions, in parallel with attitudes, subjective norms and perceptions of behavioral control. Beck and Ajzen (1990) investigated this issue in the context of three unethical behavior: cheating on a test or exam, shoplifting, and lying to get out of taking a test or turning in an assignment on time. Thus, it is expected that subjective norm will have an influence on the intention of employee workplace Internet behavior.

H2: A higher level of subjective norm supportive of Internet monitoring will lead to greater intention to avoid Internet misuse.

Perceived behavioral control refers to the individual's perception of whether an action is within their control (Ajzen 1991). Perceived behavioral control depends on control beliefs and perceived facilitation. A control belief is a perception of the availability of skills, resources, and opportunities. Perceived facilitation is the individual's assessment of the importance of those resources to the achievement of outcomes. Ajzen (1985) differentiates perceived behavioral controls as internal and external control factors. Internal factors are characteristics of the individual, including skills and will power. External factors that depend on the situation include time, opportunity and the cooperation of others.

Research literature shows support for the role of perceived behavioral control on behavioral intention. For example, Mathieson (1991) showed that behavioral control influences the intention to use an information system. A positive relationship between control and intentions is also found in Taylor and Todd (1995) who examine users in a computer resources center. In the context of this study, the more an employee understands the skills and mechanism of Internet monitoring, the less likely they are going to have Internet misuse behavior. Behavioral control should have a positive effect on employees' intention of avoiding Internet misuse behavior.

H3: A higher level of perceived behavioral control will lead to greater intention to avoid Internet misuse.

Deterrence Theory

General deterrence theory asserts that illegal behavior in the general population will vary inversely with more certain and severe punishment (Nagin 1978). Laws and legal sanctions or sanction threats may lead to total prevention of a particular deviance, may change the flagrancy of its manifestations or may reduce the frequency with which such acts are done. Deterrence theory identified punishment severity and punishment certainty as the two factors related to outcomes (Tittle 1980). That is, when punishment severity and punishment certainty increase, the level of unwanted behavior should decrease. Deterrence theory has been used to study the relationship between crime and the expected cost (Ehrlich, 1996). Straub (1990)

also applied deterrence theory in study of primary strategy for reducing computer abuse. Peace et al. (2003) used it to study software piracy. The deterrence theory highlights the importance of cost. The low probability of being caught was listed in a recent survey as the seventh most important reason in decision to illegally copy software (Cheng et al. 1997).

We proposed that both punishment severity and punishment certainty affects the attitude of the employees toward Internet monitoring. As the chances of being caught and the level of punishment increase, the employees' attitude toward Internet monitoring will become less positive. Therefore,

H4: Punishment severity will have a negative effect on attitude toward Internet monitoring.
H5: Punishment certainty will have a negative effect on attitude toward Internet monitoring.

The perceived behavior control factor in TPB is determined by control beliefs related to individual's perception of the resources and opportunities necessary to commit the act. In the case of Internet monitoring, the individual will perceive that the detection of Internet misuse will lead to the disciplinary action according to the company Internet use policy. Therefore, perception of the probability of detection (punishment certainty) is predicted to be a control belief affecting the individual's perceived behavioral control. The greater the chance of being caught leads to the lower the individual's level of perceived behavioral control. This leads to the hypothesis:

H6: Punishment certainty will have a negative effect on perceived behavioral control.

Perceived Importance

In the arena of social ethics, Jones (1991) birthed *moral intensity* which consists of magnitude of consequences, social consensus, probability of effect, temporal immediacy, proximity, and concentration of effect. He posited that moral intensity can influence ethical decision-making in business. Robin et al. (1996) further extended the research on moral intensity and empirically developed and validated a similar construct termed PIE (perceived importance). Defined as *the perceived personal relevance or importance of an ethical issue to an individual*, PIE parallels the concepts of user and social involvement. They argued that PIE differs from Jones' (1991) moral intensity in that he focused on exogenous characteristics of the issue rather than individual perceptions.

They thereby contended that *PIE is an individual state construct that is believed to be closer to the behavioral intention and behavior decisions than the moral intensity construct suggested by Jones (1991), and hence, is likely to be a better predictor of those decisions*. They found that PIE significantly influences behavioral intention. As such, in terms of behavioral intention, the greater the perceived importance of an ethical issue the grater the willingness to behave ethically while low levels of PIE correspond with a greater willingness to behave unethically.

Using different computing scenarios describing IT ethical problems and a survey, Cronan et al. (2005) validated and extended the perceived importance work of Robin et al. (1996) and assessed the relationship between PIE, attitude, and behavioral intention. They also found that perceived importance is a strong influence and suggested that future ethical models and research should include PIE as a probable influence on behavioral intention. This leads to the following hypotheses:

H7: Perceived importance of monitoring will have a positive effect on intention of Internet misuse avoidance.

H8: Perceived importance of monitoring will have a positive effect on attitude towards monitoring.

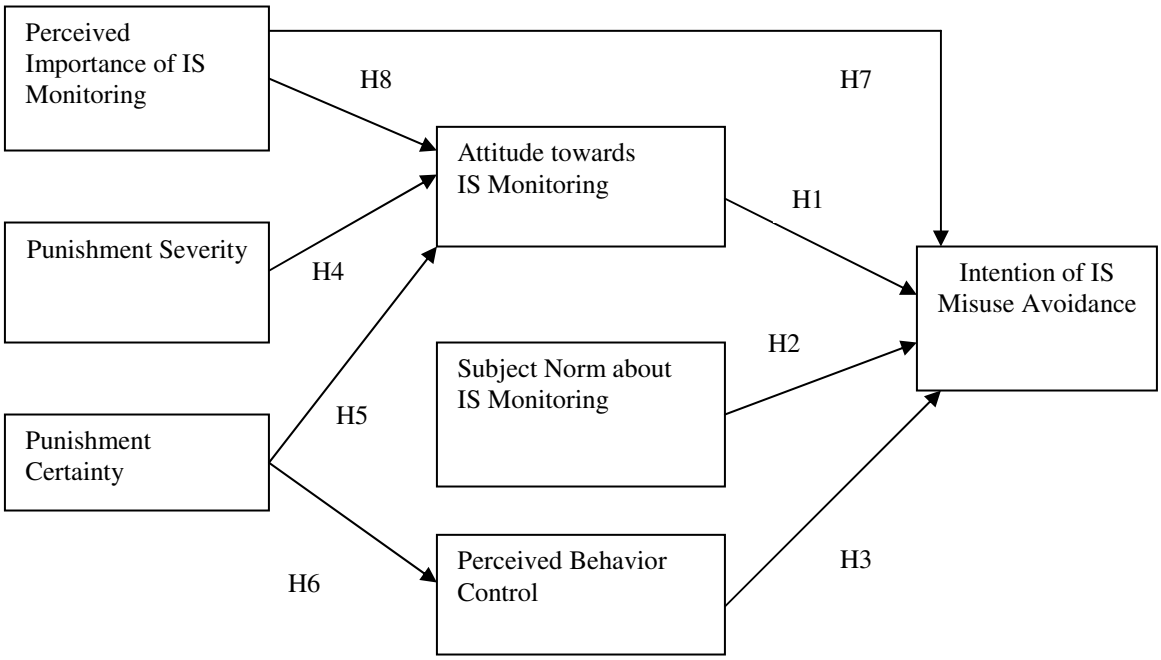

Figure 1. Research model

Research Method

This study will use a field survey method, in which participants will be asked to evaluate their responses regarding the company Internet use monitoring system. The instrument used will be formed out of the items used in prior researches (Robin 1996; Chau & Hu 2002; Mathieson 1991; Peace 2003) and pilot-tested before the actual launch. The respondents will be asked to answer the questions on a 5-point Likert scale, 1 being strongly disagree and 5 strongly agree. Partial Least Square (PLS), a Structural Equation Modeling (SEM) tool, will be employed to analyze the correlations between the factors identified and to examine the overall model fit**.** Other information concerning internet experience, company size, awareness and time of Internet monitoring system used, employee accessibility to computer and Internet, Internet access policy and monitoring training program will also be collected.

The survey instrument will be administered to employees in companies selected from four different industries (pharmaceutics, banking, financial service, and insurance). Anonymity of the survey will be ensured. The reasons for selecting those four industries are the comparatively higher information security requirement and high rate of active monitoring (Dzamba 2001).

Implications

The relationships of employee workplace Internet use behavior intention with other identified factors will be found out. Implications could be drawn from the result for directing companies in choosing the monitoring technology, training regime as well as stipulating Internet access policies. Organizational culture and behavior norm could be established by employee training programs to alleviate the load on actual monitoring. This can lead to increased employee productivity, less monitoring cost, reduced workplace stress with the minimum monitoring investment and voluntary employee Internet use behavior change.

Conclusion

This study will identify the factors that influence employees' workplace Internet use behavior intention towards monitoring. The relationships among the factors were investigated. The Theory of Planned Behavior and Deterrence Theory were used to understand how companies' monitoring measures affect employee behavior. The result of the study will provide companies

with some possible suggestions such as a good Internet access policy and monitoring training program that could bring about voluntary Internet use behavior change, a favorable corporate culture and reduced monitoring cost.

References

Agarwal, R. and Prasas, J."The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies," Decision Sciences (28:3), 1997, pp. 557-582.

Aikin, O. "Insider Information," People Management (23:11), 2000, pp. 18-19.

Ajzen, I. From Intentions to Actions: a Theory of Planned Behavior. In J. Kuhl & J. Beckmann (eds.), Action-control: From Cognition to Behavior, 11-39. Heidelberg: Springer, 1985.

Ajzen, I. "The Theory of Planned Behavior," Organizational Behavior and Human Decision Process (50), 1991, pp. 179-211.

Ajzen, I. and Madden, T. J."Prediction of Goal-directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control," Journal of Experimental Social Psychology (22), 1986, pp. 453-474.

Alge, B. J. "Effects of Computer Surveillance on Perceptions of Privacy and Procedural Justice," Journal of Applied Psychology (86:4), 2001, pp. 797-804.

Chalykoff, J. and Kochan, T."Computer-aided Monitoring: Its Influence on Employee Job Satisfaction and Turnover," Personnel Psychology (42), 1989, pp. 807-834.

Dzamba, A."AMA Reveals Monitoring of Employees' Online Activity Rises Sharply," IOMA's Report on Managing HR Information Systems[Internet] (7: 4-5), 2001 Available from: < www.worldatwork.org/pub/E158673055X_smp.pdf >.

Beck, L. and Ajzen, I. "Predicting Dishonest Actions Using the Theory of Planned Behavior," Journal of Research in Personality (25:33), 1990, pp.285 -301.

Boncella, R. J. "Internet Privacy- at Home and at Work," Communications of the AIS[Internet] (7:14), 2001. Available from: <http://cais.isworld.org/articles/default.asp?vol=7&art=14>.

Case, C. J. and Young, K. S."Employee Internet Management: Current Business Practices and Outcomes, Cyber Psychology & Behavior (5:4), 2002, pp. 355-361.

Chau, P. Y. K. and Hu, P. J. "Investigating Healthcare Professionals' Decisions to Accept Telemedicine Technology: an Empirical Test of Competing Theories," Information & Management (39:4), 2002, pp. 297-311.

Cheng, H., Sims, R., and Teegen, H. "To Purchase or Pirate Software: An Empirical Study," Journal of Management Information Systems (13:4), 1997, pp. 49-60.

Chiasson, M. W. and Lovato, C.Y. "Factors Influencing the Formation of a User's Perception and Use of a DSS Software Innovation," Database for Advances in Information Systems (32:3), 2001, pp.16 35.

Cronan, T. P., Leonard, L. N. K. and Kreie, J. "An Empirical Validation of Perceived Importance and Behavior Intention in IT Ethics," Journal of Business Ethics (56:3), 2005, pp. 231-238.

Davis, R. A. "Internet Abuse in the Workplace [Internet]," Available from: < http://www.internetadditciton.ca/cyberslacking.htm>, [Accessed June 24, 2003].

Ehrlich, I. "Crime, Punishment, and the Market for Offenses." Journal of Economics Perspectives (10:1), 1996, pp. 43-67.

Fishbein, M.and Ajzen, I. Belief, Attitude, Intention and Behavior: an Introduction to Theory and Research, Reading, MA: Addison-Wesley, 1975.

French, J. R. P. and Raven, B. The Bases of Social Power, in Studies in Social Power, D. Cardwright (ed.), Institute for Social Research, Ann Arbor, MI, 1959, pp. 150-167.

George, J. F. (1996) "Computer-based Monitoring: Common Perceptions and Empirical Results," MIS Quarterly (20:4), 1996, pp. 459-480.

Greco, J. "Privacy Whose Right is It Anyhow?" Journal of Business Strategy (22:1), 2001, pp. 32-35.

Harrison, D. A., Mykytyn, P.P. and Riemenschneider, C. K. "Executive Decision About Adoption of Information Technology in Small Business: Theory and Empirical Test," Information Systems Research (8:2), 1997, pp. 171-195.

Harrignton, S.J. (1996) "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," MIS Quarterly (20:3), 1996, pp. 257-278.

Hartwick, J. and Barki, H. "Explaining the Role of User Participation in Information System Use," Management Science (40:4), 1994, pp. 40-465.

Jones, T. M."Ethical Decision Making By Individuals in Organizations: An Issue-Contingent Model," Academy of Management Review (16:2), 1991, pp. 366-395.

Karahanna, E., Straub, D. W. and Chervany, N. L."Information Technology Adoption Across Time: a Cross-sectional Comparison of Pre-adoption and Post-adoption Beliefs," MIS Quarterly (23:2), 1999, pp. 183-213.

Levin-Epstein, M. "HR Plays Growing Role in Monitoring Employee Internet Use," Staff Leader (16:4), 2002, pp. 3-4.

Martin, J.A. "You Are Being Watched? Are you at risk?" PC World (15:11), 1997, pp. 245-253.

Mathieson, K. "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," Information Systems Research (2:3), 1991, pp. 173-191.

Morris, M.G. and Venkatesh, V. "Age Difference in Technology Adoption Decisions: Implications for a Changing Work Force," Personnel Psychology (53:2), 2000, pp. 375-403.

Nagin, D. General Deterrence: A Review of the Empirical Evidence, in Deterrence and in capacitation: Estimating the Effects of Criminal Sanctions on Crime Rates, A. Blumstein, J. Cohen, and D. Nagin (eds.), National Academy of Sciences, Washington, D.C., 1978, pp. 95-139.

Peace, A. G., Galletta, D. F., and Thong, J. Y. L. "Software Piracy in the Workplace: A Model and Empirical Test," Journal of Management Information Systems (20:1), 2003, pp. 153-177.

Pomazal, R. J. and Jaccard, J. J. "An Informational Approach to Altruistic Behavior," Journal of Personality and Social Psychology (33), 1976, pp. 317-326.

Robin, D. P., Reidenbach, R. E. and Forrest, P. J. "The Perceived Importance of an Ethical Issue as an Influence on the Ethical Decision-making of Ad Managers," Journal of Business Research (35:1), 1996, pp. 17–28.

Sandler, S. F. (2002) "Balancing Security & Privacy in the Internet Age," HR focus (79:8), 2002, pp. 13-15.

Schifter, D.B. and Ajzen, I."Intention, Perceived Control and Weight Loss: an Application of the Theory of Planned Behavior," Journal of Personality and Social Psychology (49:3), 1985, pp. 843-851.

Schwarz, S. H. and Tessler, R. C. "A Test of a Model for Reducing Measured Attitude-behavior Inconsistencies," Journal of Personality and Social Psychology (24:2), 1972, pp. 225-236.

Stanton, J.M. "Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions," Human Performance (13:1), 2000, pp. 85-113.

Straub, D. "Effective IS Security: An Empirical Study," Information Systems Research (1:3), 1990, pp. 255-276.

Straub, D.W. and Nance, W.D. "Discovering and disciplining computer abuse in organizations: A field study," MIS Quarterly (14:1), 1990, pp. 45-60.

Taylor, S. and Todd, P.A. "Assessing IT Usage: the Role of Prior Experience," MIS Quarterly (19:4), 1995, pp. 561-570.

Thompson, R.L., Higgins, C. A. and Howell, J. M. "Influence of Experience on Personal Computer Utilization: Testing a Conceptual Model," Journal of Management Information Systems (11:1), 1994, pp. 167-178.

Tittle, C.R. Sanctions and Social Deviance: The Question of Deterrence. New York: Praeger, 1980.

Urbaczewski, A. and Jessup, L. M. "Does Electronic Monitoring of Employee Internet Usage Work?" Communications of the ACM (45:1), 2002, pp. 80-83.

Venkatesh, V. and Davis, F.D. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," Management Science (46:2), 2000, pp. 186-204.

Ward, D.B. "Surfing on Company Time? You Could Loose Your Privacy…and Maybe Your Job," PC World (15:11) , 1997, pp. 245-253.

Warshaw, P. R. "A New Model for Predicting Behavioral Intentions: an Alternative to Fishbein," Journal of Marketing Research (17:2), 1980, pp. 153-172.

Zimmerman, E. "HR Must Know When Employee Monitoring Crosses the Line," Workforce (2), 2002, pp. 38-45.

Zweig D, Websteb, J. "Personality as a moderator of monitoring acceptance," Computers In Human Behavior (19:4), 2003, pp. 479-493.