IMPLICATIONS OF MONITORING MECHANISMS ON BRING YOUR OWN DEVICE (BYOD) ADOPTION

Research-in-Progress

James Lee, Jr.
Mississippi State University
M&IS Department
P.O. Box 9581
Mississippi State, MS 39762-9581
Jl1396@msstate.edu

Robert E. Crossler
Mississippi State University
M&IS Department
P.O. Box 9581
Mississippi State, MS 39762-9581
rob.crossler@msstate.edu

Merrill Warkentin
Mississippi State University
M&IS Department
P.O. Box 9581
Mississippi State, MS 39762-9581
m.warkentin@msstate.edu

Abstract

*Bring Your Own Device (BYOD) policies permit employees to use personal devices to access organizational information. Users gain convenience from the ability to work in geographically diverse locations, while organizations gain the benefit of increased productivity and reduced information technology expense. However, these symbiotic benefits come at a cost. Organizations' security boundaries are now extended to include personal devices, which must be controlled to mitigate data exfiltration. This control comes in the form of monitoring employees' personal d*evices, which infringe on their *privacy. The monitoring mechanisms employed by organizations play a critical role in employee participation in a BYOD program. This study investigates the impact of monitoring mechanisms, privacy concerns, and job performance when evaluating whether to participate in a BYOD program. A factorial survey design was developed to test the hypotheses. Initial testing was performed and was used to modify the instrument for the main study currently in progress.*

Keywords: Bring-Your-Own-Device, BYOD, Privacy, Monitoring

Introduction

In 2011, smartphones outshipped netbooks, notebooks, and desktops combined (Canalys 2012). In a poll conducted by the Pew Research Center, adoption of smartphones increased 11% from 2011 to 2012. The demand to incorporate technologies available at home into the workplace environment has spurred the Bring Your Own Device (BYOD) movement in public and private organizations that span the gamut of industries. The workforce's desire to use the latest smartphones, tablets, ultrabooks, and laptops, coupled with organizations' desire to reduce expenses, has facilitated this movement. Worldwide, 89% of Information Technology departments enable varying degrees of BYOD, and 83% of United States companies predict a growth in BYOD with in the next two years (Bradley et al. 2012).

BYOD enables employees to utilize personal devices to access corporate data. It shifts the responsibility for hardware to the end user, potentially saving organizations capital and operating expenses. However, there are many challenges to adopting the BYOD model. From the organizational perspective, permitting employees to utilize personal devices to access corporate data introduces an additional attack point to exfiltrate information. Moving to the mobile environment increases the number of remote devices that could be lost or stolen.

Employees are now accountable for the corporate data on their personal devices, and employers must utilize mechanisms to ensure this data are protected. Organizations can use Mobile Device Management (MDM) systems to monitor and control nearly all functions of employee devices. Monitoring capabilities include text, voice, and data usage, Global Positioning System (GPS) location, phone state, and device status. The system can control hardware by disabling features such as cameras, Bluetooth, and GPS software. Software is controlled by approving and requiring apps for devices, and restricting users from installing blacklisted apps (Fiberlink 2012). When a device is no longer under the organization's control due to the device being lost or the employee exiting the company, MDM systems can remotely erase the data on the device to protect organizational data (Krill 2012).

BYOD management techniques have been described in previous research from the organizational perspective. Practitioners have addressed best practices for organizations to deploy BYOD (e.g. Caldwell, Zeltmann, & Griffin, 2012; Lucier, 2012; Messmer, 2012; Raths, 2012; Ullman, 2011), however there is scant research on user adoption of BYOD. Researchers have investigated the organizational dangers of BYOD, and have developed practices to mitigate the risk of BYOD to the organization. However, current research does not account for the user's perceptions and assumes the user wants to adopt BYOD. We suggest that, prior to participating in a BYOD program, users must evaluate the BYOD policy to determine if the benefits of participating are worth the loss of privacy and control.

Privacy concerns are amplified in the BYOD environment because the device belongs to the user with both personal and organizational data stored on the device. Therefore, there is a concern for providing organizations with potential access to the personal data. Unlike previous employee monitoring programs, participating in BYOD is volitional, meaning the employee can opt out of being monitored by not participating in the program. The Information Systems Audit and Control Association (ISACA) reports over half of employees polled would be less inclined to use a personal device for work purposes if the organization could remove all their data from the device, could restrict online activities, or track online activities (58%, 55%, and 57% respectively) (Ketchum Global Research & Analytics 2012). The hesitation to participate in a BYOD program may be a product of the monitoring mechanisms used by the organization, which raises the question:

> **RQ:** How do monitoring mechanisms in an organizational BYOD policy affect individual BYOD adoption?

To answer this question, we assess the design artifacts of monitoring in a volitional BYOD program, while accounting for Performance Expectancy and privacy concerns of employees. We utilize the Theory of Planned Behavior's (TPB) (Ajzen 1991) value expectancy foundation as our overarching framework. We suggest that monitoring mechanisms and privacy concerns are acrimonious forces that oppose adoption benefits. Privacy concerns are measured by adapting the Internet Users Information Privacy Concerns (IUIPC) scale (Malhotra et al. 2004) to the mobile context, and adoption benefits are examined through the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003). We

empirically test our theory using the factorial survey method, which was developed using rigorous instrument refinement practices. This study contributes to the IS discipline by extending the monitoring literature to include circumstances under employees' discretion and strengthening the stalwart UTAUT and privacy theories. Furthermore, it advances the use of the factorial survey method in IS security research.

Theoretical background

There is a stream of academic research founded on the TPB (Ajzen 1991) that focuses on technology acceptance. TPB is an extension of the theory of reasoned action (TRA) (Fishbein and Ajzen 1975) that attempts to explain and predict behavior based on intentions that are formed by the attitude towards the behavior, subjective norms, and perceived behavioral control. These antecedences to intention or behavior can be described using additional beliefs or dispositions to provide additional granularity on attitudes, subjective norms, and behavioral control (Ajzen 1991). The theoretical strength of TPB makes it an ideal theory to use as a framework for IS behaviors.

We utilize TPB by focusing on the attitudes towards participating in a BYOD program, and control for subjective norms and perceived behavioral control in the vignettes of the factorial survey method. Attitudes are the favorable or unfavorable views of a behavior, and are shaped through behavioral beliefs, which can be modified through external stimuli. The foundation of TBP, TRA, was built on an expectancy-value model, which posits that attitudes are a summative belief index composed of the subjective evaluation of the behavior belief's attributes. These attributes are the costs and benefits of performing the behavior (Ajzen 1991). Our focus is on the contrary factors of a BYOD program, specifically the design artifacts that increase accountability and privacy concerns. To form a complete theory, we also address the expected increase in job performance as the benefit to participating in the program. Our research model is depicted in Figure 1.

Design Artifacts to Increase Accountability

Employers have an obligation to employees, shareholders, and customers to ensure that workers are satisfactorily productive. Employees do not want to endure additional duties because of others' laziness or incompetence, and consumers do not want sub-standard products (Miller and Weckert 2000). Monitoring can have positive and negative effects depending on the level of invasiveness set by management (Marx and Sherizen 1986). The impact of monitoring on employee perceptions of supervision depends on the type of job, data monitored, management attitudes, organizational culture, and if the monitoring is used in a punitive manner (George 1996). Previous research has looked at monitoring's impact on trust (Tabak and Smith 2005), performance outcomes (Grant and Higgins 1991), absenteeism (Workman 2009), ethical considerations (Grodzinsky et al. 2010), job satisfaction (Alder, Noel, et al. 2006; George 1996), and privacy concerns (Eivazi 2011) in settings where the employee cannot opt out of the monitoring program. Our study investigates monitoring in a situation where employees can choose to participate by utilizing their personal devices for work purposes. The volitional nature of a BYOD program makes it an ideal scenario to determine how monitoring policies affect behavioral intentions.

Monitoring is effective at modifying behavior because of mechanisms that provide authority figures an awareness of actions the employees may have to justify. While the literature provides a rich understanding of monitoring in mandatory settings, it is plagued with inconsistent terms for similar design artifacts and it does not address volitional conditions. The consistent artifacts applicable to voluntary monitoring that emerge are identifiability (Vance et al. 2013; Williams et al. 1981), awareness (Vance et al. 2013) , tasks measured (George 1996; Grant and Higgins 1991; Marx and Sherizen 1986), frequency (Alder, Noel, et al. 2006; Grant and Higgins 1991), and justification (Alder, Noel, et al. 2006).

In the BYOD environment it is the employee's device that is being monitored, therefore there is a high degree of identifiability built into the program. Evaluation awareness requires that the actions monitored will have implied consequences. However, to determine the effects of the monitoring program on adoption the sanction effects must be controlled. Social presence is an indication that monitoring is currently active. It may be possible for an MDM system to provide an indicator that monitoring is

occurring. However, communicating the monitoring frequency in the policy provides a situation that can be immediately evaluated prior to opting into a BYOD program rather than a situation that should be experienced longitudinally. The level of awareness depends on the communication of the monitoring program's details in the BYOD policy.

Awareness of monitoring can be provided through advanced notice prior to a monitoring program. When employees are previously notified of task-specific performance monitoring, then their perceived procedural fairness is enhanced (Alder, Ambrose, et al. 2006). Providing the employees with the monitoring policy during the hiring process gives the employ advanced notice of monitoring. The policy should communicate the tasks measured, frequency of monitoring, justification, and in the BYOD context, organizational control over the personal device.

Monitoring can be performed on a task-specific basis for performance assessment (Douthitt and Aiello 2001; George 1996; Grant and Higgins 1991) or in a general manner to prevent unwanted behaviors such as cyber loafing (Alder, Noel, et al. 2006; Li et al. 2010), email abuse, and policy non-compliance (Boss et al. 2009). The tasks measured for performance assessment depends on the completeness of a monitoring program to cover the full range of tasks involved in doing a job (Grant and Higgins 1991). The number and types of Tasks Measured have been shown to negatively impact employees' attitudes towards monitoring (George 1996). Monitoring as a prevention tool is not task specific. However, it does include monitored activities such as email, application usage, and GPS location. We suggest that the information the organization monitors on the employees' devices exhibits similar characteristics to the task-specific monitoring measures, therefore:

H1: Monitoring design artifacts that increase the invasiveness of tasks measured will decrease BYOD adoption intention.

The frequency of the tasks monitored establishes how often data are collected from the monitored device. The uncertainty of employees' activities are reduced when frequent exchanges occur (Brice Jr et al. 2011). When monitored tasks directly reflect performance, then increasing monitoring frequency has been shown to have a positive effect on acceptance (Grant and Higgins 1991). However, in general monitoring situations increased frequency creates a sense of micromanagement (Grant and Higgins 1996). In a non-task specific monitoring situation such as BYOD, the monitored tasks are not directly tied to performance. We suggest that:

H2: Monitoring design artifacts that increase the frequency of monitoring will decrease BYOD adoption intention.

Justification for traditional and electronic monitoring increases perceived interactional fairness (Stanton 2000). In situations where the tasks monitored are directly tied to job performance (e.g. airline customer service employees' reservation accuracy), monitoring justification was not a significant antecedent to post-implementation trust (Alder, Ambrose, et al. 2006). We posit that when the nature of the data collected is directly relevant to job performance (Marx and Sherizen 1986), then justification is tautological. However, in the BYOD environment, the monitored activities do not measure job performance. Therefore, additional justification as to why an organization needs to collect data from the employees' personal device may be required to establish procedural fairness.

H3: Monitoring design artifacts that provide justification will increase BYOD adoption intention.

Previous research has focused on monitoring usage of company assets (e.g. Alder, Noel, et al., 2006). Organizations have full control over these assets and can allow or restrict activities by blocking websites, filtering emails (Van Toorn and Shu 2010), controlling hardware and software configuration, or restricting information access (Deshmukh Balaji 2006). Unlike other monitoring programs, MDM systems in the BYOD environment can provide the organization with control over employees' personal devices. The amount of control can range from Laissez-faire, where employees have no restrictions, to a complete lockdown of devices (Research in Motion 2013). The amount of control an organization has over a personal device is an intrusion on employees, and can affect employees' attitudes towards participating in a BYOD program. We proffer that:

H4: Monitoring design artifacts that increase the organizational control will decrease BYOD adoption intention.

Information Privacy

Employee monitoring can change workplace behaviors, but it also can make employees feel degraded, stressed, and dehumanized (Ariss 2002). Monitoring is often viewed as company rights versus employee rights, which are often at odds (Loch, Conger, & Oz, 1998). Organizational access to personal devices raises privacy concerns from the user's perspective. Emails sent and received on a company computer or Internet traffic that is routed through a company network may be regarded as company property, however in the BYOD environment the device that is transmitting and receiving company data is personally owned.

There is a vast body of literature on information privacy (for a detailed review see Belanger and Crossler 2011; Smith et al. 2011) that defines and applies privacy to a number of contexts. In the IS field, information privacy is often commoditized as a requirement to conduct online activities such as e-commerce (Dinev and Hart 2006; Pavlou et al. 2007) and participating in social media (Abril et al. 2012; Vegosen 2010). Similarly, BYOD requires relinquishing privacy and control of the personal device to the organization to participate in a BYOD program.

The concept of control is central to information privacy, as privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967 p. 7). Westin's (1967) definition of privacy included one's control over the when, how, and extent of information shared, which is defined by information policies for electronic monitoring. Using information outside of the usage agreement raises privacy concerns that question the fairness of the transaction (Malhotra et al. 2004). The cost and benefits of the disclosure are evaluated using a personal privacy calculus (Culnan and Armstrong 1999; Laufer and Wolfe 1977).

Mobile User's Information Privacy Concerns

Increased data portability has brought with it increased privacy concerns. Information that once was only available in physical repositories has become a target of concern due to the proliferation of digital information. As technology made it possible to conduct new activities by transmitting information through new communication tools, privacy concerns followed. Technology has enabled mobile computing that can perform activities once relegated to the office. Now privacy concerns are extended beyond physical repositories as well as centralized digital repositories to the mobile environment.

Mobile computing brings privacy concerns for information that are transmitted during typical personal computing activities such as ecommerce (Culnan and Bies 2003; Dinev and Hart 2006; Metzger 2004) and include new sources of concern such as location based information (Xu et al. 2012). The concern over the information in the mobile environment is similar to the fixed environment, but the new types of information and environmental context require defining information privacy concerns in the mobile space. Following previous studies (e.g. Dinev & Hart, 2006; Liu, Marchewka, Lu, & Yu, 2005; Miller & Weckert, 2000; Tang, Hu, & Smith, 2008), we proffer that mobile information privacy concerns will effect behavioral intention in the mobile space, and:

H5: Mobile users' information privacy concerns are negatively related to BYOD adoption intention.

Performance Expectancy

Performance Expectancy is the benefit of BYOD in the expectancy-value model. UTAUT postulates that Performance Expectancy is the theoretical result of comparing perceived usefulness (Davis 1989), extrinsic motivation (Davis et al. 1992), job-fit (Thompson et al. 1991), relative advantage (Moore and Benbasat 1991), and outcome expectations (Compeau and Higgins 1995). The common theme among these constructs is utilitarian value of technology and represents the primary benefit of adoption. Performance Expectancy is the belief that adopting a certain technology will help improve job performance (Venkatesh et al. 2003). While this definition is narrowly defined to the workplace environment, it fits the context of BYOD better than the revised UTAUT2 that encompasses general benefits to consumers (Venkatesh et al. 2012) because BYOD is an inherently work related phenomenon. Performance Expectancy has demonstrated a high degree of influence on technology acceptance intentions (Venkatesh et al. 2003), therefore:

H6: Performance expectancy will have a positive influence on BYOD adoption intention.

Mobile Computing Self-Efficacy

While the ability to participate in the program can be controlled for, the efficacy of using mobile technologies is an individual background factor that must be accounted for. The complexity of technology requires users to navigate through organized actions to obtain desired outcomes (Hsu and Chiu 2004). The nuances between technologies necessitates efficacy beyond general computing. Mobile computing self-efficacy is the belief in one's skill to use smartphone technology (Keith et al. 2011). It performs a similar function to computer self-efficacy by altering perceptions of technology usefulness (Marakas et al. 2007; Venkatesh et al. 2003), but in a more defined context. mobile computing self-efficacy influences the strength of performance expectations (Keith et al. 2011), and is appropriate for the BYOD context. Affecting the strength of the relationship between two variables suggests that mobile computing self-efficacy is a moderator, therefore:

H7: Mobile computing self-efficacy will positively moderate the relationship between job performance expectancy and BYOD adoption intention.

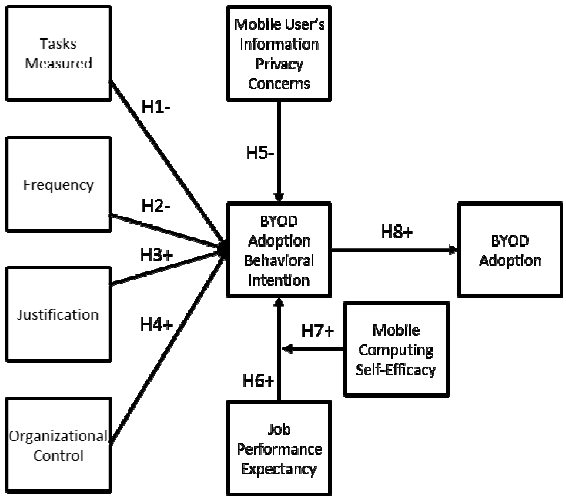

Figure 1: Research Model

BYOD Adoption

Previous research suggests that technology adoption is preceded by behavioral intentions (Venkatesh et al. 2003). Behavioral Intention indicates the level in which one is willing to perform a specified behavior. When the control conditions for a particular behavior are met, then the behavioral intention provides a good predictor of behavior (Ajzen 1991). The conditions to participate in a BYOD program simply require ownership of a compatible device. With the proliferation of personal computing devices, this condition is easily met. Because of the low barriers to participate in BYOD and the influence of adoption on behavior, we posit that:

H8: BYOD Adoption Intention are positively related to BYOD adoption.

Research Methodology

The factorial survey method will be utilized to test our hypotheses. It provides respondents with scenarios that differ as independent variables are manipulated (Jasso 2006) then measures dependent variables of

interest (Trevino 1992). We followed an initial development process to ensure the validity and reliability of the vignettes and measurement instrument.

Factorial Survey Approach

During the decision making process, individuals are placed into situations that have a number of influential factors, making it difficult to measure behavioral drivers. The factorial survey method reduces this measurement error by placing the respondent in the situation using vignettes. Vignettes describe a realistic situation that manipulates the variables relevant to the study against the outcome of interest and controls for non-substantive variables (Gould 1996). The embedded variables are characteristics of the vignette actor or scenario, which are manipulated orthogonally to ensure the variables are fully crossed. Manipulating variables orthogonally reduces multi-collinearity between factors that are closely related (Rossi and Anderson 1982). The respondent is randomly presented vignettes from the vignette universe, and each is modified to measure their positive-beliefs about and normative-judgments on the dependent variable (Jasso 2006). The variables presented to the respondent are under the control of the investigator, thereby reducing endogeneity problems in the estimation (Jasso 2006). By controlling the characteristics of the vignette, the researcher is able to capture the complexity of real-world behavior while delineating the influencing factors that affect those behaviors (Rossi and Anderson 1982).

The first step in the factorial survey method is to generate the input factors and vignette characteristics through the literature review (Jasso 2006). We identified the monitoring mechanisms Tasks Measured, Frequency, Justification, and Organizational Control as the factors to be manipulated, while Identifiability, Object of Monitoring, Recipient of Data were to be controlled. The UTAUT variables Voluntariness of Use, Facilitating Conditions, Social Influence, and Effort Expectancy to participate in the program were also controlled to reduce confounding effects. Next we developed our measurement of input factors by identifying the domain and range of each variable. Tasks Measured was an ordinal manipulation that increased the number and invasiveness of the information the organization monitored. The three levels were: 1. company email, 2) company email and installed applications and usage, and 3) company email, installed applications and usage, and GPS data. Frequency was manipulated as: 1) random, and 2) constantly in real-time. Justification was a binary manipulation with either: 1) no justification given, or 2) Monitoring is performed to ensure corporate information is safe on your device. Organizational Control was an additive ordinal manipulation with three levels: 1) no control, 2) the company will regulate installed applications, or 3) the company will regulate installed applications and delete all files if the device is lost. The full factorial vignette population is the Cartesian product of all possible combinations (Jasso 2006), therefore our population consisted of 36 unique combinations with no logically impossible vignettes. Vignettes were presented to respondents using a full vignette randomization strategy. Each respondent was randomly presented three vignettes from the vignette population.

To pre-test the reliability and validity of the instrument, initial data was collected from seniors, graduate students, and alumni of a large university in the southeastern US. After modifications based on this pre-test, a pilot test and main study using working adults will be conducted.

Discussion

Potential Implications for Research

This study can provide three important contributions for academic research. First, by extending theories to new contexts, we strengthen the generalizability of previous research. The TPB (Ajzen 1991) has demonstrated that the value expectancy model shapes attitudes and subsequently behaviors. Identifying the salient costs and benefits of the value expectancy calculation through manipulating monitoring mechanisms, and measuring IUIPC and UTAUT constructs extends the IS literature by enhancing the knowledge of technology adoption from a privacy versus performance perspective. Placing these theories in the BYOD context provides a unique perspective on workplace monitoring because employees must opt-into monitoring by electing to participate in a BYOD program.

Second, we propose utilizing the factorial survey method to empirically test our hypotheses. The factorial survey design is a method that has started to gain favor in the IS discipline (Vance et al. 2013). This method expands the internal reliability of the scenario method because of the increased number of manipulations that can be tested at the vignette level to determine statistical differences (Rossi and Anderson 1982). Our use of the factorial survey method brings additional insights on how it can be used to assess normative judgments in the IS context.

Finally, the adapted items for Behavioral Intention, Mobile Computing Self-Efficacy, Job Performance Expectations, and Mobile User's Information Privacy Concerns will be tested for content validity, construct validity, and internal reliability. This will provide evidence of the psychometric properties and stability of the scales, and can help inform future researchers during instrument development.

Potential Implications for Practice

The degree to which attitudes are changed provides insight into the relative importance of salient characteristics during the technology acceptance process. The benefit of technology acceptance can be viewed as a non-contrary factor that drives behavioral beliefs which is balanced against contrary factors that represent the costs of adoption. Dinev and Hart (2006) suggested that privacy concerns are contrary beliefs in the evaluation to provide personal information for Internet transactions. Similarly, using a personal device for work purposes engages privacy concerns by permitting an organization to monitor information on the device. Recent research has suggested that there is a privacy paradox to the value-expectancy model, where users with high privacy concerns still relinquish personal information to obtain benefits (Smith et al. 2011). The threshold depends on the strength of the benefit versus the cost of the loss in privacy. For example, 58% would reveal email addresses for a 50% discount on a $100 item (Ketchum Global Research & Analytics 2012). Determining at what point users will relinquish privacy to achieve their goals is an important contribution.

The willingness to divulge personal information has been attributed to the power-dependency asymmetry, where the firm has control over resources that the consumer desires (Bulgurcu and Benbasat 2009). In the workplace, the employees are the resource the organization wishes to maximize. Because BYOD is a volitional program, the power symmetry is shifted towards the employee. This study's findings could inform practitioners on the effects of monitoring mechanisms when implementing a BYOD program. This is important from the organizational perspective because of the increase productivity and decreased operating expenses organizations can realize by permitting employees to utilize their personal devices for work purposes.

Conclusion

Technology proliferation has increased the demand to incorporate personal computing devices into the workplace. How organizations develop BYOD programs will have critical security posture implications on both the organization and the individual user. Securing corporate information, while limiting the infringement on employee privacy is a challenging task. Personal devices must be monitored and controlled to ensure organizational data is safe. However, it must be balanced with employee privacy concerns.

Opponents of monitoring argue that it is unfair and abusive, unnecessarily infringes on employee rights, and creates an atmosphere of mistrust (Alder, Noel, et al. 2006). BYOD is a volitional program that employees can opt-into, thereby shifting the locus of control from the organization to the individual. This empowers the workforce to voice their attitudes towards the monitoring mechanisms used in the BYOD program, which in turn can increase procedural justice perceptions (Douthitt and Aiello 2001). Employee surveillance erodes trust (Strickland 1958), therefore it behooves organizations to understand the implication of the monitoring mechanisms utilized when crafting a BYOD strategy. This study aims to establish the monitoring mechanisms as critical components in a BYOD program.

References

Abril, P. S., Levin, A., and Del Riego, A. 2012. *Blurred boundaries: social media privacy and the twenty-first-century employee*, *American Business Law Journal*, (Vol. 49) , pp. 63–124.

Ajzen, I. 1991. "The theory of planned behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Alder, G. S., Ambrose, M. L., and Noel, T. W. 2006. "The effect of formal advance notice and justification on Internet monitoring fairness: Much about nothing?," *Journal of Leadership & Organizational Studies* (13:1), pp. 93–107.

Alder, G. S., Noel, T. W., and Ambrose, M. L. 2006. "Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust," *Information & Management* (43:7), pp. 894–903.

Ariss, S. S. 2002. "Computer monitoring: benefits and pitfalls facing management," *Information & Management* (39), pp. 553–558.

Bélanger, F., and Crossler, R. E. 2011. "Privacy in the digital age: A review of information privacy research in information systems," *MIS Quarterly* (35:4), pp. 1017–1041.

Boss, S. R., Kirsch, L. J., Angermeier, I., and Shingler, R. A. 2009. "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security," *European Journal of Information Systems* (18:2), pp. 151–164.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., and Buckalew, L. 2012. *BYOD: A global perspective harnessing employee-led innovation*, Cisco Systems, pp. 1–21.

Brice Jr, J., Nelson, M., and Gunby Jr, N. W. 2011. "The governance of telecommuters: an agency and transaction cost analysis," *Academy of Strategic Management Journal* (10:1), pp. 1–17.

Bulgurcu, B., and Benbasat, I. 2009. "Analysis Of Consumers' Privacy Breach Consent: A Resource Dependency Perspective," in *Workshop on Information Security & Privacy*, Phoenix, AZ, pp. 1–9.

Caldwell, C., Zeltmann, S., and Griffin, K. 2012. "BYOD (Bring Your Own Device).," *Competition Forum* (10:2), pp. 117–121.

Canalys. 2012. "Smartphones overtake client PCs in 2011," .

Compeau, D. R., and Higgins, C. A. 1995. "Application of Social Cognitive Theory to Training for Computer Skills," *Information Systems Research* (6:2), pp. 118–143.

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104–115.

Culnan, M. J., and Bies, R. J. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), pp. 323–342.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319–340.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. 1992. "Extrinsic and intrinsic motivation to use computers in the workplace.," *Journal of Applied Social Psychology* (22:14), pp. 1111–1132.

Deshmukh Balaji, A. 2006. "Performance analysis of filtering software using Signal Detection Theory," *Decision Support Systems* (42:2), pp. 1015–1028.

Dinev, T., and Hart, P. 2006. "An extended privacy calculus model for e-commerce transactions," *Information Systems Research* (17:1), pp. 61–80.

Douthitt, E. A., and Aiello, J. R. 2001. "The role of participation and control in the effects of computer monitoring on fairness perceptions, task satisfaction, and performance," *The Journal of applied psychology* (86:5), pp. 867–874.

Eivazi, K. 2011. "Computer use monitoring and privacy at work," *Computer Law and Security Review: The International Journal of Technology and Practice* (27:5)Elsevier B.V, pp. 516–523.

Fiberlink. 2012. "Mobile device management (MDM) policies: Best practices guide," Blue Bell, PA, pp. 1–14.

Fishbein, M., and Ajzen, I. 1975. *Belief, attitude, intention, and behavior: An introduction to theory and research*, Reading, MA: Wesley.

George, J. F. 1996. "Computer-based monitoring: Common perceptions and empirical results," *MIS Quarterly* (20:4), pp. 459–480.

Gould, D. 1996. "Using vignettes to collect data for nursing research studies: How valid are the findings?," *Journal of Clinical Nursing* (5:4), pp. 207–212.

Grant, R. A., and Higgins, C. 1991. "The impact of computerized performance monitoring on service work: Testing a causal model," *Information Systems Research* (2:2), pp. 116–142.

Grant, R. A., and Higgins, C. A. 1996. "Computerized Performance Monitors as Multidimensional Systems: Derivation and Application," *ACM Transactions on Information Systems* (14:2), pp. 212–235.

Grodzinsky, F., Gumbus, A., and Lilley, S. 2010. "Ethical implications of internet monitoring: A comparative study.," *Information Systems Frontiers* (12:4), pp. 433–441.

Hsu, M.-H., and Chiu, C.-M. 2004. "Internet self-efficacy and electronic service acceptance," *Decision Support Systems* (38), pp. 369–381.

Jasso, G. 2006. "Factorial Survey Methods for Studying Beliefs and Judgments," *Sociological Methods & Research* (34:3), pp. 334–423.

Keith, M. J., Babb Jr., J. S., Furner, C. P., and Abdullat, A. 2011. "The Role of Mobile Self-Efficacy in the Adoption of Location-Based Applications: An iPhone Experiment," in *Proceedings of the 44th Hawaii International Conference on System Sciences*, Kauai, HI, pp. 1–10.

Ketchum Global Research & Analytics. 2012. "2012 IT risk/reward barometer: US consumer edition," .

Krill, P. 2012. "BYOD: A world of pain awaits IT," *Infoworld*, .

Laufer, R. S., and Wolfe, M. 1977. "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues* (33:3), pp. 22–42.

Li, H., Zhang, J., and Sarathy, R. 2010. "Understanding compliance with internet use policy from the perspective of rational choice theory," *Decision Support Systems* (48:4), pp. 635–645.

Liu, C., Marchewka, J. T., Lu, J., and Yu, C.-S. 2005. "Beyond concern—a privacy-trust-behavioral intention model of electronic commerce," *Information & Management* (42), pp. 289–304.

Lucier, J. 2012. "Make BYOD Work: How Cloud Helps," *Federal Computer Week* (26:15), p. 15.

Malhotra, N. K., Kim, S. S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp. 336–355.

Marakas, G. M., Johnson, R. D., and Clay, P. F. 2007. "The Evolving Nature of the Computer Self-Efficacy Construct: An Empirical Investigation of Measurement Construction, Validity, Reliability and Stability Over Time.," *Journal of the Association for Information Systems* (8:1), pp. 15–46.

Marx, G. T., and Sherizen, S. 1986. "Social aspects of changes in worker monitoring and computer/communications privacy and security practices," Washington, D.C., pp. 1–191.

Messmer, E. 2012. "Government IT strains under BYOD challenge," *Network World* (29:7), p. 10.

Metzger, M. J. 2004. "Privacy, trust, and disclosure: Exploring barriers to electronic commerce," *Journal of Computer-Mediated Communication* (9:4).

Miller, S., and Weckert, J. 2000. "Privacy, the Workplace and the Internet," *Journal of Business Ethics* (28:3), pp. 255–265.

Moore, G. C., and Benbasat, I. 1991. "Development of an instrument to measure the perceptions of adopting an information technology innovation," *Information Systems Research* (2:3), pp. 192–223.

Pavlou, P. A., Liang, H., and Xue, Y. 2007. "Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective," *MIS Quarterly* (31:1), pp. 105–135.

Raths, D. 2012. "The BYOD revolution," *Healthcare informatics: the business magazine for information and communication systems* (29:3), pp. 28–30.

Research in Motion. 2013. "BlackBerry 10: Setting new standards in mobile security," , pp. 1–5.

Rossi, P. H., and Anderson, A. B. 1982. "The Factorial Survey Approach: An Introduction," in *Measuring Social Judgments: The Factorial Survey Approach*, SAGE Publications, Inc.

Smith, H. J., Dinev, T., and Xu, H. 2011. "Information privacy research: An interdisciplinary review," *MIS Quarterly* (35:4), pp. 989–1015.

Stanton, J. M. 2000. "Traditional and electronic monitoring from an organizational justice perspective," *Journal of Business and Psychology* (15:1), pp. 129–147.

Tabak, F., and Smith, W. 2005. "Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development," *Employee Responsibilities & Rights Journal* (17:3), pp. 173–189.

Tang, Z. L., Hu, Y., and Smith, M. D. 2008. "Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor.," *Journal of Management Information Systems* (24:4), pp. 153–173.

Thompson, R. L., Higgins, C. A., and Howell, J. M. 1991. "Personal computing: Toward a conceptual model of utilization," *MIS Quarterly* (15:1), pp. 125–142.

Van Toorn, C., and Shu, A. Y. 2010. "Assessing the impact of organizational Internet and email monitoring policy on Australian employees," in *AMCIS 2010 Proceedings*, Lima, Peru, pp. 1–12.

Trevino, L. K. 1992. "Experimental Approaches to Studying Ethical-Unethical Behavior in Organizations," *Business Ethics Quarterly* , pp. 121–136.

Ullman, E. 2011. "BYOD and security," *Technology & Learning* (31:8), pp. 32–36.

Vance, A., Lowry, P. B., and Eggett, D. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems," *Journal of Management Information Systems* (29:4), pp. 263–290.

Vegosen, J. 2010. "Employee Monitoring and Pre-Employment Screening.," *Risk Management* (57:8), p. 29.

Venkatesh, V., Morris, M. G., Hall, M., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425–478.

Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technolgoy," *MIS Quarterly* (36:1), pp. 157–178.

Westin, A. F. 1967. *Privacy and Freedom*, New York, NY: Atheneum.

Williams, K., Harkins, S., and Latané, B. 1981. "Identifiability as a Deterrent to Social Loafing: Two Cheering Experiments.," *Journal of Personality & Social Psychology* (40:2), pp. 303–311.

Workman, M. 2009. "A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions," *Information and Organization* (19:4), pp. 218–232.

Xu, H., Teo, H.-H., Tan, B. C. Y., Agarwal, R., and Heng, X. 2012. "Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services," *Information Systems Research* (23:4), pp. 1342–1363.