Journal of Computer Information Systems

ISSN: 0887-4417 (Print) 2380-2057 (Online) Journal homepage: http://www.tandfonline.com/loi/ucis20

Implications of Monitoring Mechanisms on Bring Your Own Device Adoption

James Lee Jr., Merrill Warkentin, Robert E. Crossler & Robert F. Otondo

JOURNAL OF COMPUTER INFORMATION SYSTEMS
http://dx.doi.org/10.1080/08874417.2016.1184032

Taylor & Francis
Taylor & Francis Group

Implications of Monitoring Mechanisms on Bring Your Own Device Adoption

James Lee Jr. [a], Merrill Warkentin [a], Robert E. Crossler [b], and Robert F. Otondo [a]

[a]Mississippi State University, Mississippi State, MS, USA; [b]Washington State University, Pullman, WA, USA

ABSTRACT

Bring Your Own Device (BYOD) programs permit employees to use personal devices to access organizational information. Users gain convenience, while employers benefit from increased productivity and reduced IT expense. Security boundaries must extend to personal devices to mitigate data exfiltration, thereby infringing on employees' privacy by monitoring their personal devices. These monitoring mechanisms play a critical role in employee participation in a BYOD program. Our results demonstrate that the BYOD monitoring mechanisms and privacy concerns suppress the benefits of increased job performance expectancy when evaluating whether to participate in a BYOD program. This research identifies that tasks measured, frequency of monitoring, and organizational control are significant impediments to behavioral intention for BYOD participation.

KEYWORDS
Security; monitoring; BYOD; factorial survey method; policy

Introduction

Smartphones now outship netbooks, notebooks, and desktop computers combined [13], with adoption of smartphones increasing each year [57]. The greatest increase in ownership is from 18- to 24-year-olds, with over 67% owning a smartphone. The next youngest demographic, 25- to 34-year-olds, had the highest level of adoption with a 71% penetration level. The younger workforce is adopting mobile technologies at a high rate, and the demand to incorporate technologies available at home into the workplace environment has spurred the Bring Your Own Device (BYOD) movement across all industries. The workforce's desire to use the latest technology, coupled with organizations' desire to reduce expenses, promotes this movement. Worldwide, 89% of Information Technology departments enable varying degrees of BYOD, and 83% of US companies predict a growth in BYOD within the next 2 years [10].

BYOD enables employees to utilize personal devices to access corporate data, shifting 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. Employees' personal devices that access corporate data become additional attack points. Stolen or misplaced laptops that contained sensitive information plague organizations (e.g. [31, 72]), and mobile technologies increase the number of remote devices that could be lost. Information stored on mobile devices could be compromised. Devices with remote access to corporate servers expand potential impacts beyond locally stored information. Employees are now accountable for corporate data on their personal devices, and employers must protect their data [36]. 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, location, phone state, and device status. The system can control hardware by disabling features such as cameras, Bluetooth, and GPS. Software is controlled by approving and requiring apps for devices, and restricting users from installing blacklisted apps [22]. MDM systems can protect organizational data by remotely erasing data on devices that are no longer under the organization's control (e.g., lost device and employee termination) [36].

Extant BYOD research focuses on the organizational risks and benefits, or the individual's benefits. Practitioners have addressed best practices for organizations to deploy BYOD [12, 46] and limited research has been done on the favorable factors of BYOD [74, 75]. Researchers have investigated the organizational dangers of BYOD, and have developed practices to mitigate the risk of BYOD to the organization [24, 66]. However, it does not account for the user's perceptions and assumes the user wants to adopt BYOD and does not address the BYOD's unfavorable factors. Lee et al. [37] suggested that employees must initially evaluate the BYOD policy to determine if the benefits of participating are worth the loss of privacy and control, but did not empirically test these propositions.

Accessing device information and restricting device usage provides organizations with the ability to electronically monitor employees. Employee monitoring has been used to measure job performance for a limited number of occupations [24]. Today, computers and the Internet are integral parts of business, and monitoring has moved beyond a task-performance focus to include all electronic use. Monitoring enhances the organization's ability to hold employees accountable for their electronic usage, improve employee efficiency and effectiveness, and reduce Internet abuse [38]. Accountability obligates actors to justify their actions [9]. Technological advances enable recording

CONTACT Merrill Warkentin ✉ m.warkentin@msstate.edu 🖃 Mississippi State University, Department of Management and Information Systems, College of Business, P.O. Box 9581, Mississippi State, MS 39762, USA.

employee activities down to the keystroke, sometimes creating consternation over privacy in the workplace [1, 35].

Privacy concerns are amplified in the BYOD environment because the device belongs to the user. Weeger et al. [74] identified perceived private threats as a hindrance to BYOD adoption because of the concern with providing organizations with potential access to 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 reports over half of users 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 [34]. 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 BYOD monitoring mechanisms affect 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) [2] 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 accounted by adapting Internet Users Information Privacy Concerns (IUIPC) [43] to the mobile context, and adoption benefits are examined through the Unified Theory of Acceptance and Use of Technology (UTAUT) [70]. We gather data and empirically test our theory using the factorial survey method and multilevel modeling.

Theoretical background

Research founded on the TPB [2] focuses on technology acceptance to explain and predict behavior based on intentions formed by the attitudes toward the behavior, subjective norms, and perceived behavioral control. These antecedents to behavioral intention can be described using additional beliefs or dispositions to provide additional granularity [2]. The theoretical strength of TPB makes it an ideal theory to use as a lens for analyzing IS behaviors.

We utilize TPB to frame our research by focusing on the attitudes toward 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 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 [2]. 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 (Figure 1).

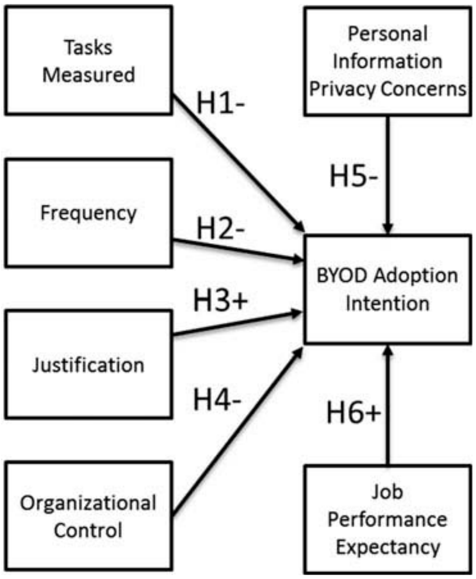

Figure 1. Research model

Design artifacts to increase accountability

Employers strive to ensure worker productivity, but monitoring may have negative effects when invasiveness is too high [44]. The impact of monitoring on employee perceptions of supervision depends on the job type, data monitored, management attitudes, organizational culture, and if monitoring is used in a punitive manner [24]. Previous research has examined monitoring's impact on trust [63], performance outcomes [26], absenteeism [76], ethical considerations [29], job satisfaction [4, 24], and privacy concerns [21] in mandatory settings. 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 overlapping concepts and does not address volitional conditions. For example, accountability can be increased through manipulating design artifacts that foster identifiability, evaluation awareness, social presence awareness, and monitoring awareness [68]. In turn, identifiability serves as a deterrent to social loafing because the efforts of identified individuals often increase as they contribute to a common goal [76]. Marx and Sherizen's [44] framework of privacy monitoring incorporates intrusiveness, frequency, relevance to job performance, visibility, focus, targeting, the nature of the data collected, and data accuracy. Grant and Higgins [26] tested the effects of tasks measured, frequency of measurement, object of monitoring, and recipient of the monitored data on personal importance of production and service and found that monitoring may not increase production. Tasks measured and monitoring frequency were also identified by George [24] to influence attitudes toward monitoring and jobs in multiple case studies. Alder, Noel, and Ambrose [4] found that advanced notice and perceived organizational support affected employees' trust of the organization postimplementation, however justification did not. Van Toorn and Shu [66] found that monitoring policy awareness was positively correlated with satisfaction in low-monitored environments but negatively correlated in high-monitored environments. The differences in satisfaction levels across organizations support the concept that organizational climate influences employee monitoring reactions [24].

The degree of intrusiveness is a function of the nature of the data collected [44] and the frequency of collection [44, 66]. The nature of the data collected depends on the tasks monitored [24, 26]. Monitoring awareness [68] is provided by notifications that increase visibility [44] either prior to monitoring or after monitoring has been implemented [3]. Justification [4] is based on the relevance of the data collected [44], which helps to establish procedural fairness [59]. Identifiability [68] depends on the target object of monitoring [44], whether it be an individual or a group [26]. Not all of the monitoring mechanisms in the literature apply to a new employee assessing the BYOD monitoring policy; however, the applicable consistent themes that emerge are identifiability, awareness, tasks measured, frequency, and justification.

When the employee's device is monitored in the BYOD environment, 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.

Monitoring can be performed on a task-specific basis for performance assessment [20, 24, 26] or in a general manner to prevent unwanted behaviors such as cyber loafing [4] and policy noncompliance [8]. The tasks measured for performance assessment depend on the completeness of a monitoring program to cover the full range of tasks involved in doing a job [26]. The number and types of tasks monitored have been shown to negatively impact employees' attitudes toward monitoring [24]. Monitoring as a prevention tool is not task specific; however, it does include monitored activities such as e-mail, 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. Supervisors who monitor employees more often will have a greater awareness of the employees' activities, which can improve performance [24]. When monitored tasks directly reflect performance, then increasing monitoring frequency has been shown to have a positive effect on acceptance [26]. However, in general, monitoring situations with increased frequency creates a sense of micromanagement [27]. In a non-task-specific monitoring situation such as BYOD, the monitored tasks are not directly tied to performance; therefore:

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 [59]. 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 postimplementation trust [3]. When the nature of the data collected is directly relevant to job performance, then justification is tautological [44]. 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 [4]. Organizations have full control over these assets and can allow or restrict activities by blocking websites, filtering e-mails [66], controlling hardware and software configuration, or restricting information access [18]. Unlike other monitoring programs, MDM systems in the BYOD environment can provide the organization with control over employees' personal device. The amount of control can range from *laissez-faire*, where employees have no restrictions, to a complete lockdown of devices [54]. The amount of control an organization has over a personal device is an intrusion on employees, and can affect employees' attitudes toward participating in a BYOD program:

H4: Monitoring design artifacts that increase the Organizational Control will decrease BYOD Adoption Intention.

Personal information privacy concerns

Employee monitoring can improve workplace behaviors, but can also make employees feel degraded, stressed, and dehumanized [5]. Monitoring is often viewed as a company rights versus employee rights issue [41]. Organizational access to personal devices raises privacy concerns from the user's perspective. E-mails 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 a 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 [6, 49, 58]) 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 [19] and participating in social media [1, 69]. Similarly, BYOD requires relinquishing privacy and control of the personal device to the organization to participate in a BYOD program.

The mobile environment introduces constant connectivity and new data privacy challenges. In the context of BYOD, information privacy concern is a measure of the issues stemming from providing an organization access to the user's personal device. These issues can be described in the framework of the first-order constructs of IUIPC: control, awareness, and collection. BYOD is a volitional program; if employees do not have a device to bring, then they cannot participate in the program. Because of the high degree of voluntariness, control is decided by the user to opt-in or opt-out of the program. Awareness is established by BYOD policies and organizational practices. The intrusiveness of BYOD policies on personal privacy can range from nonexistent in the case of enabling corporate Internet Message Access Protocol (IMAP) e-mail to extremely high in the case of GPS tracking. The level of policy intrusiveness and organization's policy adherence will contribute to perceptions of fairness. The final dimension of IUIPC, collection, becomes contentious in BYOD programs because users grant the organization control over their personal data and meta-data. Such access changes the focus from information transmitted over the Internet to personal information residing on the user's device. Following IUIPC, we suggest that the term personal information privacy concerns (PIPC) is more appropriate for this study. Following previous studies on privacy's effect on behavioral intention (e.g., [19, 40, 47, 64], we proffer that:

H5: Personal 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 [17], extrinsic motivation [16], job-fit [65], relative advantage [48], and outcome expectations [15]. 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 [70]. 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 [71] because BYOD is an inherently work-related phenomenon. Performance expectancy has demonstrated a high degree of influence on technology acceptance intentions [70] specifically for BYOD [74], therefore:

H6: Performance Expectancy will have a positive influence on BYOD Adoption Intention.

Research method

A two-phased investigation [14, 42, 61] was used. Phase one specified the research context, identified salient constructs, developed experimental treatments and measurement scales, and pilot tested the instrument for validity and reliability. Phase two reevaluated the instrument's validity and reliability, and then tested for data biases and hypothesis support. This section will focus on the factorial survey method, instrument development, and participants.

Factorial survey approach

The factorial survey method provides respondents with scenarios that differ as independent variables are manipulated [33], and then measures dependent variables of interest [67]. During normal decision-making processes, individuals encounter situations with many influential factors that obscure decision drivers. The factorial survey method reduces this measurement error by manipulating relevant variables within clearly defined vignettes describing realistic situations [25]. The orthogonally manipulated variables are characteristics of the vignette actor or scenario ensures that the variables are fully crossed and reduces multicollinearity between factors that are closely related [56]. 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 [33]. These variables are under investigator control, thereby reducing endogeneity [33]. 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 [56].

The full factorial vignette population consisted of 36 unique combinations with no logically impossible vignettes. Each respondent was randomly presented three vignettes in a random order from the vignette population for full randomization. The vignettes were structured with an overarching scenario, followed by the manipulated variables in Table 1.

Table 1. Vignette scenario, levels, and treatments.

Overarching scenario	You have been hired at XYZ Inc., which has a policy that allows employees to use their personal device for work purposes if they want to. The policy provides the employee with all of the support needed to enter into the program, making it very easy to participate. You are handed the policy, in it are a few key areas highlighted:	
Vignette Dimension	Vignette Level	Treatment
Tasks Measured	Task1	The company will monitor your company e-mail
	Task2	The company will monitor your company e-mail, and installed applications and usage
	Task3	The company will monitor your company e-mail, installed applications and usage, and GPS data
Frequency	Freq_Ran	Monitoring will be done randomly
	Freq_Real	Monitoring will be done constantly in real time
Justification	Just_No	[NONE]
	Just_Yes	Monitoring is performed to ensure corporate information is safe on your device
Organizational Control	OrgCntrl0	[NONE]
	OrgCntrl1	The company will regulate installed applications
	OrgCntrl2	The company will regulate installed applications and delete all files if the device is lost

Instrumentation

All items were measured using previously validated items on a seven-point, fully anchored Likert scales. Two rounds of review panels consisting of experts from theoretical, scale development, methods, and subject matter domains assessed the face and content validity of the vignettes and measurement items. Terms that the target population would find ambiguous or unfamiliar were removed, and items were simplified to avoid unnecessary cognitive load. The vignettes were assessed for realism and readability, and were deemed appropriate for the target population. The instrument was examined for potential sources of common method variance (CMV), such as item ambiguity, social desirability, acquiesce bias, consistency motif, and illusory correlations [50]. The expert panels suggested that careful wording, item order, and randomization were appropriate to combat CMV.

CMV was controlled by directly addressing ambiguity, social desirability, and scale length in the expert review panels, and item context biases and order effect were taken into consideration when developing the instrument flow to reduce mood induction or priming effects [50]. Biases from common scale properties were minimized by using different anchor labels and reporting interfaces (e.g., radio buttons and sliders). Harmon's single factor test and the marker variable techniques were used to detect CMV. Fashion consciousness was used as the nontheoretically associated marker variable because it measures intrinsic traits similar to the substantive variables, and can only be assessed through querying the respondent's perception [55]. It is the degree of importance to dress fashionably, and should have no bearing on the substantive variables in the study.

The data were scrutinized for completeness and other biases to ensure quality. Involvement checks and response bias tests were performed on the pilot and main study data prior to analysis. The involvement checks were included after each vignette. The probability of randomly answering the two and three involvement checks correctly is 14.8% and 3.7%, respectively. Pilot study respondents who answered two of the three checks correctly were retained, and main study respondents who answered all three checks correctly were retained. Response set was also examined by calculating the standard deviation for all Likert scale items and removing cases that had a standard deviation of less than 0.7. The standard deviation cut-off value to detect extreme response style depends on the scale intervals [28]. Both samples were screened to ensure familiarity with smartphone technology and their potential for using a personal device in the workplace.

Participants

Seniors, graduate students, and alumni of a large US university provided the pilot data. An e-mail was distributed using a university listserv that requested participation in the study. Eighty respondents started the survey, of which 38 completed the survey and met the previously described criteria. Amazon's Mechanical Turk provided the main study data. There were 390 survey participants, of which 275 were deemed usable. The respondents were all from the United States as recommended based on previous studies [60].

The study's target demographic was working professionals who may use a smartphone for work purposes. The demographics of the main study data suggested that the participants were appropriate. The age of the respondents ranged from 18 to 61 years with an average age of 31 years. Fifty-six percent of the respondents were male. Ninety-seven percent indicated they owned a smartphone, and averaged 3.7 years of ownership. Sixty-four percent of the respondents have used a smartphone for business purposes.

Data analysis and results

Instrument validity

Convergent and discriminant validity of the reflective variables were tested through exploratory (EFA) and confirmatory factor analysis (CFA). The EFA during the pilot study provided support for convergent and discriminant validity. The reflective constructs Behavioral Intention, Fashion Concerns, and Job Performance Expectancy items all loaded on separate dimensions without cross loading at the suggested levels. A CFA was performed to examine the three dimensions of PIPC. This test indicated that three items cross-loaded above 0.4, which suggests that the measurement items of the scale may conceptually overlap. Furthermore, one failed to load on any dimension. The items were adjusted and clarified prior to administering them as part of the main study. For the main study, each construct loaded on a single factor greater than 0.7 and did not cross load above 0.4. A CFA of the PIPC items was performed similar to the one done in the pilot study. One Collection item, one Control item, and one awareness item cross loaded and were removed and the CFA was run again. There was sufficient convergent and discriminant validity for the remaining items for analysis. The reliability of the reflective items was established by calculating the Cronbach's alpha. In the pilot and main studies, all of the scales met the 0.7 acceptance threshold [23, 30].

Common method variance

We assessed the existence of CMV using Harmon's Single Factor test and a marker variable test. The Harmon's single factor test included all of the reflective items in an exploratory factor analysis with no rotation [50]. The result of the analysis was four factors, with no single factor accounting for a majority of the variance. Second, we conducted a marker variable analysis to determine if the bivariate correlations between the substantive variables and a theoretically unrelated variable were significant [39]. The correlation matrix indicated that there was no correlation over 0.4, which is evidence that CMV does not exist between the items.

Analysis

The factorial survey method captures perceptions from a single rater on multiple vignettes, therefore the between-subject and within-subject variation must be accounted for [73]. These structural dependencies can be analyzed through multilevel modeling [32]. BYOD Adoption Intention is the dependent variable in this study. The monitoring mechanism manipulations (Tasks Measured, Frequency, Justification, and Organizational Control) in the vignettes are modeled as level-1 variables. PIPC and Job Performance Expectancy are individual-level (i.e., level-2) variables that will affect the level-1 judgments.

Hypothesis testing was completed using the HLM for Windows version 7.01 ® software [52]. A random coefficients model was constructed using full maximum-likelihood estimation.

A multilevel model was constructed based on the research model portrayed in Figure 1. The monitoring mechanisms were dummy coded (0,1) and were used as the level-1 variables in the multilevel model. The dummy variables were named Task1, Task2, Task3, Freq_Real, Freq_Rand, Just_Yes, Just_No, OrgCntl0, OrgCntrl1, and OrgCntl2. Following recommendations in Hox et al. [32] (p507), these level-1 dummy (0,1) variables are left uncentered to enhance interpretation.

The first model in the HLM analysis (i.e., Model 1, Table 2) is fully unconditional; as such, it provides a baseline to assess improvement in subsequent models [53]. The second model included the level-1 predictors Task2, Task3, Freq_Real, Just_Yes, OrgCntrl1, and OrgCntl2. The level-1 predictors Task1, Freq_Rand, Just_No, and OrgCntl0 were omitted in order to mitigate multicollinearity problems and thus served as reference levels for their respective dimensions. We found that HLM could not successfully run this version of the second model because every level-1 predictor matrix was near singular. Following recommendations in the HLM Model 2 output, we examined the level-1 variables to determine which should be treated as random and which should be treated as fixed. Four different subsets of Model 2 were run, each restricted to only one dimension (e.g., the first test was based only on Task; the second only on Frequency). Each subset was run with the levels set as fixed, and then run again with all levels set as random. The χ^2 tests for change in deviance in these tests indicate that only the Task dimension produced significant improvement when modeled for random effects across individuals. Accordingly, Model 2 was rerun with the Task dimension evaluated for random effects and the Frequency, Justification, and Organizational Control dimensions treated as fixed.

Table 2. HLM analysis of factorial survey.[a]

Variables (Coefficients)	Model 1	Model 2	Model 3	Model 4
Level-1 Intercept and Independent Variables				
Task2 (π_{10})		−1.012***	−1.008***	−1.008***
		(0.067)***	(0.066)***	(0.066)***
Task3 (π_{20})		−1.301***	−1.300***	−1.298***
		(0.066)***	(0.064)***	(0.065)***
Freq_Real (π_{30})[b]		−0.185***#	−0.174***#	−0.175***#
		(0.039)***	(0.038)***	(0.038)***
Just_Yes (π_{40})[b]		0.026#	0.019#	
		(0.043)***	(0.043)***	
OrgCtrl1 (π_{50})[b]		−0.093#[c]	−0.110*#	−0.110*#
		(0.049)***	(0.049)***	(0.049)***
OrgCtrl2 (π_{60})[b]		−0.157**#	−0.170**#	−0.170**#
		(0.052)***	(0.052)***	(0.052)***
Direct and Moderating Effects on Level-1 Coefficients β_{01}[d]				
Intercept (β_{00})	−0.015	0.764***	0.833***	0.787***
	(0.047)	(0.075)***	(0.134)***	(0.065)***
Education (β_{01})			−0.084*	−0.084*
			(0.040)***	(0.040)***
PIPC (β_{02})			−0.136***	−0.142***
			(0.040)***	(0.039)***
PE (β_{03})			0.268***	0.272***
			(0.036)***	(0.035)***
Goodness-of-fit				
Deviance	2,136.4	1,616.1	1,566.4	−1,569.4
Number of parameters	3	14	20	16
Δ Deviance from previous model[e]		−520.3***	−49.7***	N/A

[a] $N = 786$ at vignette level; $N = 262$ at individual level. Unstandardized coefficient estimates and robust standard errors (in parentheses) reported. Estimation is Full Maximum Likelihood.

[b] This level-1 variable is treated as fixed.

[c] Estimated *p*-value is 0.058. "#" indicates the value should be treated as a rough approximation.

[d] Individual-level control variables BYOD Use, Age, and Gender, were included in Model 3, but their results—which were all nonsignificant—were not reported for brevity of display. These control variables were not included in Model 4.

[e] *p*-values for $\Delta\chi^2$ calculated using Soper [1].

*** $p < .001$ ** $p < .01$ *$p < .05$ # Should be treated as a rough approximation.

The results of this updated Model 2 (Table 2) indicate the Task, Frequency, and Organizational Control dimensions (as operationalized in our vignettes) are significantly associated with BYOD Adoption Intention, but Justification is not. As expected, the Task, Frequency, and Organizational Control dummy variables are negatively associated with BYOD Adoption Intention. These results support Hypotheses 1, 2, and 4, but not Hypothesis 3. The individual (level-2) variable PIPC was negatively and significantly associated with BYOD Adoption Intention, while Job Performance Expectancy was positively and significantly associated with the dependent variable. These results support Hypotheses 5 and 6, respectively. A chi-square test for change in deviance indicates the addition of these level-2 predictors in Model 3 gives significant improvement over Model 2 ($p < 0.001$), providing further support for Hypotheses 5 and 6. The effects of four individual-level control variables were also examined in Model 3 (i.e., BYOD Use, Age, Gender, and Education). Only Education was found to be significant ($p < 0.05$).

A final model (i.e., Model 4) was also run to examine if the elimination of nonsignificant variables substantially changed the results in Model 3. These results were substantially the same as those in Model 3, thus providing additional support for Hypotheses 1, 2, 4, 5, and 6 but no support for Hypothesis 3. A summary of the supported hypotheses is provided in Table 3.

Table 3. Results of HLM analysis.

Hypothesis		Finding
H1:	Monitoring design artifacts that increase the invasiveness of Tasks Measured will decrease BYOD Adoption Intention	Supported
H2:	Monitoring design artifacts that increase the Frequency of monitoring will decrease BYOD Adoption Intention	Supported
H3:	Monitoring design artifacts that provide Justification will increase BYOD Adoption Intention.	Not supported ($p > 0.05$)
H4:	Monitoring design artifacts that increase the Organizational Control will decrease BYOD Adoption Intention.	Supported
H5:	Personal Information Privacy Concerns are negatively related to BYOD Adoption Intention.	Supported
H6:	Performance Expectancy will have a positive influence on BYOD Adoption Intention.	Supported

Discussion

Attitude changes provide an insight into the relative importance of salient characteristics during the technology acceptance process. The benefit of technology acceptance can be viewed as a noncontrary factor that drives behavioral beliefs, which is balanced against contrary factors that represent the costs of adoption. Dinev and Hart [19] 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 suggests that even users with high privacy concerns will relinquish personal information to obtain benefits [58]. The threshold depends on the strength of the benefit versus the cost of the loss in privacy. Determining at what point users will relinquish privacy to achieve their goals is an important contribution. The findings partially explain the effect of monitoring mechanisms on behavioral intention to participate in a BYOD program. The significance of the Tasks Monitored is consistent with the previous monitoring literature [4, 24], and can help guide practitioners in developing BYOD policies. The present study illustrates that even though Job Performance Expectancy may exist when using a personal device for work purposes, the loss of privacy is too great based on the Tasks Monitored.

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 [11]. In the workplace, the employees are the resource the organization wishes to maximize. Because BYOD is a volitional program, the power symmetry is shifted toward the employee. The importance of the Tasks Monitored in a BYOD program suggests that practitioners should utilize the principle of least privilege when developing policy and only access the minimum data points required to sufficiently accomplish the objective. Organizations need to limit their access to employee data and only monitor the information and control the aspects of the device that are required to satisfy security requirements. Furthermore, this policy is supported by privacy ethics that encourage a minimal amount of personal information be collected (per AMC code of ethics).

We provide two important contributions to research. First, extending theories to new contexts strengthens the generalizability of previous research. The TPB [2] has demonstrated that the value expectancy model shapes attitudes and subsequently shapes 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 utilize the factorial survey method and multilevel modeling to empirically test our hypotheses. The factorial survey design is a method that has started to gain favor in the IS discipline [68]. 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 [56]. Our use of the factorial survey method brings additional insights on how it can be used to assess normative judgments in the IS context. The multilevel structure of the factorial survey method requires statistical techniques that can account for within- and between-subject variance and indicate which level-1 relationships vary across individuals (e.g., the relationship between Task and BYOD Adoption Intention varies, but those involving Frequency, Justification, and Organizational Control do not). Using HLM to test our hypotheses broadens the toolsets used in IS research, and this research provides support for future researchers when examining multilevel models.

Limitations and future research

Our study provides initial insights into the effects of monitoring mechanisms and privacy concerns on BYOD program participations; however, there are some limitations that should be addressed. The use of Behavioral Intention versus actual behavior has long been debated in the IS literature [62]. Behavioral intention may be reversed when the promise of real-world convenience is presented [7]. In the present study, when a new employee is presented with the option to use his personal device at work, he may opt to do so for convenience sake despite his privacy concerns. However, intentions are an appropriate surrogate for our interest in the initial behavior of opting into a BYOD program because intentions are formed immediately after the BYOD policy is presented. This captures the reaction to the monitoring mechanisms and Job Performance Expectancy better than measuring actual participation and actual job performance because it limits the influence factors such as BYOD efficacy. Furthermore, to measure participation in an organization that is implementing BYOD was cost-prohibitive. Using the factorial survey method was an economical way to simulate an organization and manipulate monitoring mechanisms. Future research in this area could take an action-oriented approach and implement different BYOD policies in organizations by manipulating the monitoring mechanisms presented in this study.

The use of the factorial survey method involves trade-offs. While they maximize the generalizability of findings by efficiently reaching many respondents and provide high levels of precision by controlling variables in the vignettes, their artificiality decreases realism [45]. Gaining generalizability through increasing the number of vignette observations by presenting each respondent with multiple vignettes comes at a cost. The use of nonindependent observations may introduce error that overestimates regression coefficients. The method also artificially inflates the sample size by focusing on the vignette as the unit of analysis. However, the multilevel modeling accounts for the within-subject variance of nonindependent samples while simultaneously accounting for the between-subject variance caused by the experimental manipulation [53]. Future research that investigates monitoring mechanisms using different methods (e.g., action research) could cross-validate factorial survey findings.

Another limitation of the study's use of the factorial survey method was the order in which respondents were presented with latent measures and the vignettes. Subjects' Mobile Information Privacy Concerns were measured prior to being exposed to the overarching scenario or the manipulated vignettes. Job Performance Expectancy was measured after establishing the scenario and initial intentions were captured. A vignette was then administered and the respondents' behavioral intentions were measured. By querying respondents on Mobile Information Privacy Concerns and Job Performance Expectancy prior to the vignettes, a priming effect may have biased the data. Inquiring about Mobile Information Privacy Concerns and Job Performance Expectations prior to the treatment could have respectively deflated and inflated respondents' assessment of their Behavioral Intention. Future studies should increase the proximal separation [51] of these measures by changing the order the items are presented in relation to the vignettes. Alternatively, the original and reordered versions of the instrument could be administered with random assignment to test if priming is causing rater bias.

Only justifying the monitoring program and not each monitoring mechanism was a calculated drawback that resulted in an unsupported hypothesis. Providing reasoning for each monitoring mechanism could allow the user to rationalize why tasks are measured, how frequently they are measured, and how much the organization exerts control over the device. Justification would then have a moderating effect on each of the Monitoring Mechanisms and the adoption relationship. Including justification for each Monitoring Mechanisms exponentially increases the complexity of the research because each level of the mechanism manipulation would require a justification manipulation. This would result in a vignette universe of 144 vignettes. The Tasks Measured had the largest impact on adoption intentions. Future researchers interested in how justification affects adoption may want to scope the research to only that mechanism to make the vignette universe manageable.

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 are safe; however, it must be balanced against employee privacy concerns.

Opponents of monitoring argue that it is unfair and abusive, unnecessarily infringes on employee rights, and creates an atmosphere of mistrust [4]. 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 toward the monitoring mechanisms used in the BYOD program, which in turn can increase procedural justice perceptions [20]. Employee surveillance erodes trust [63], therefore it behooves organizations to understand the implication of the monitoring mechanisms utilized when crafting a BYOD strategy.

This study demonstrates that understanding the appropriate tasks to monitor is a critical component of establishing fair practices in a BYOD program. When the Tasks Monitored are too invasive, then employees will be hesitant to participate in the program. Despite the potential increase in job performance gained from using a personal device at work, the performance expectations are overshadowed by privacy concerns. Furthermore, this study illustrates that the operationalization of Internet Users' Information Privacy Concerns as a multidimensional construct has challenges with exhibiting convergent and discriminant validity on the first-order factors.

ORCID

James Lee Jr. http://orcid.org/0000-0003-3816-6228
Merrill Warkentin http://orcid.org/0000-0001-7435-7676
Robert E. Crossler http://orcid.org/0000-0002-8179-9138
Robert F. Otondo http://orcid.org/0000-0002-3502-8877

References

[1] Abril PS, Levin A, Del Riego A. 2012. Blurred boundaries: Social media privacy and the twenty-first-century employee. Am Bus Law J. 49(1):63–124.

[2] Ajzen I. 1991. The theory of planned behavior. Organ Behav Hum Decis Process. 50(2):179–211.

[3] Alder GS, Ambrose ML, Noel TW. 2006. The effect of formal advance notice and justification on Internet monitoring fairness: Much about nothing?. J Leadersh Organ Stud. 13(1):93–107.

[4] Alder GS, Noel TW, Ambrose ML. 2006. Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. Inf Manage. 43(7):894–903.

[5] Ariss SS. 2002. Computer monitoring: benefits and pitfalls facing management. Inf Manage. 39:553–558.

[6] Bélanger F, Crossler RE. 2011. Privacy in the digital age: A review of information privacy research in information systems. MIS Q. 35(4):1017–1041.

[7] Bélanger F, Hiller JS, Smith WJ. 2002. Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. J *Strategic* Inf Syst. 11(3/4):245.

[8] Boss SR, Kirsch LJ, Angermeier I, Shingler RA. 2009. If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. Eur J Inf Syst. 18(2):151–164.

[9] Bovens M. 2010. Two concepts of accountability: Accountability as a virtue and as a mechanism. West Eur Polit. 33(5): 946–967.

[10] Bradley J, Loucks J, Macaulay J, Medcalf R, Buckalew L. 2012. BYOD: A Global Perspective Harnessing Employee-Led Innovation. Cisco Systems, San Jose, CA.

[11] Bulgurcu B, Benbasat I. 2009. Analysis of consumers' privacy breach consent: A resource dependency perspective. In: Workshop on Information Security & Privacy. Phoenix, AZ; 1–9.

[12] Caldwell C, Zeltmann S, Griffin K. 2012. BYOD (Bring Your Own Device). Compet. Forum 10(2):117–121.

[13] Canalys. 2012. Smartphones Overtake Client PCs in 2011. http://www.canalys.com/newsroom/smart-phones-overtake-client-pcs-2011

[14] Churchill GA. 1979. A paradigm for developing better measures of marketing constructs. J Mark Res. 16(1):64–73.

[15] Compeau DR, Higgins CA. 1995. Application of social cognitive theory to training for computer skills. Inf Syst Res. 6(2):118–143.

[16] Davis FD, Bagozzi RP, Warshaw PR. 1992. Extrinsic and intrinsic motivation to use computers in the workplace. J Appl Soc Psychol. 22(14):1111–1132.

[17] Davis FD. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. 13(3):319–340.

[18] Deshmukh Balaji A. 2006. Performance analysis of filtering software using Signal Detection Theory. Decis Support Syst. 42 (2):1015–1028.

[19] Dinev T, Hart P. 2006 An extended privacy calculus model for e-commerce transactions. Inf Syst Res. 17(1): 61–80.

[20] Douthitt EA, Aiello JR. 2001. The role of participation and control in the effects of computer monitoring on fairness perceptions, task satisfaction, and performance. J Appl Psychol. 86(5): 867–874.

[21] Eivazi K. 2011. Computer use monitoring and privacy at work. Comput Law Secur Rev Int J Technol Pract. 27(5): 516–523.

[22] Fiberlink. 2012. *Mobile Device Management (MDM) Policies: Best Practices Guide*. http://www.webtorials.com/main/resource/papers/fiberlink/paper2/MDM_Policies_Best_Practices_Guide.pdf

[23] Gefen D, Straub DW, Boudreau M. 2000. Structural equation modeling and regression: Guidelines for research and practice. Commun Assoc Inf Syst. 4(7): 1–76.

[24] George JF. 1996. Computer-based monitoring: Common perceptions and empirical results. MIS Q. 20(4): 459–480.

[25] Gould D. 1996. Using vignettes to collect data for nursing research studies: How valid are the findings?. J Clin Nurs. 5(4): 207–212.

[26] Grant RA, Higgins C. 1991. The impact of computerized performance monitoring on service work: Testing a causal model. Inf Syst Res. 2(2): 116–142.

[27] Grant RA, Higgins CA. 1996. Computerized performance monitors as multidimensional systems: Derivation and application. ACM Trans Inf Syst. 14(2): 212–235.

[28] Greenleaf EA. 1992. Measuring extreme response style. Public Opin Q. 56(3): 328–351.

[29] Grodzinsky F, Gumbus A, Lilley S. 2010. Ethical implications of internet monitoring: A comparative study. Inf Syst Front. 12(4): 433–441.

[30] Hair JF, Black WC, Babin BJ, Anderson RE. 2010. *Multivariate Data Analysis: A Global Perspective*, Vol 7th ed. Pearson Education, Upper Saddle River, NJ.

[31] Hoover N. 2010. Stolen VA laptop contains personal data. http://www.darkreading.com/risk-management/stolen-va-laptop-contains-personal-data/d/d-id/1089135

[32] Hox JJ, Kreft IGG, Hermkens PLJ. 1991. The analysis of factorial surveys. Sociol Methods Res. 19(4): 493–510.

[33] Jasso G. 2006. Factorial survey methods for studying beliefs and judgments. Sociol Methods Res. 34(3): 334–423.

[34] Ketchum Global Research & Analytics. 2012. 2012 IT Risk/reward Barometer: US Consumer Edition.

[35] Kim EKJ. 2006. The new electronic discovery rules: a place for employee privacy?. Yale Law J. 115(6):1481–1490.

[36] Krill P. 2012. BYOD: A world of pain awaits IT. http://www.infoworld.com/article/2619520/byod/byod–a-world-of-pain-awaits-it.html

[37] Lee J, Crossler R, Warkentin M. 2013. Implications of monitoring mechanisms on bring your own device (BYOD) adoption. In: Proceedings of the 34th International Conference on Information Systems. Vol Milan, Italy; 1–12.

[38] Liao Q, Gurung A, Luo X, Li L. (2009). Workplace management and employee misuse: Does punishment matter? J Comput Inf Syst. 50(2):49–59.

[39] Lindell MK, Whitney DJ. 2001. Accounting for common method variance in cross-selectional research designs. J Appl Psychol. 86(1): 114–121.

[40] Liu C, Marchewka JT, Lu J, Yu C-S. 2005. Beyond concern—a privacy-trust-behavioral intention model of electronic commerce. Inf Manag. 42: 289–304.

[41] Loch KD, Conger S, Oz E. 1998. Ownership, privacy and monitoring in the workplace: A debate on technology and ethics. J Bus Ethics 17(6):653–663.

[42] MacKenzie SB, Podsakoff PM, Podsakoff NP. 2011. Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Q. 35(2): 293–334.

[43] Malhotra NK, Kim SS, Agarwal J. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Inf Syst Res. 15(4): 336–355.

[44] Marx GT, Sherizen S. 1986. Social Aspects of Changes in Worker Monitoring and Computer/communications Privacy and Security Practices. Washington, D.C.: The Office.

[45] McGrath JE. 1994. Methodology matters: Doing research in the behavioral and social sciences. In: Research Strategies. Vol Morgan Kaufmann Publishers, Inc.,San Francisco, CA; 152–169.

[46] Messmer E. 2012. Government IT strains under BYOD challenge. Netw World 29(7): 10.

[47] Miller S, Weckert J. 2000. Privacy, the workplace and the internet. J. Bus. Ethics 28(3): 255–265.

[48] Moore GC, Benbasat I. 1991. Development of an instrument to measure the perceptions of adopting an information technology innovation. Inf Syst Res. 2(3): 192–223.

[49] Pavlou PA. 2011. State of the information privacy literature: Where are we know and where should we go?. MIS Q. 35(4): 977–988.

[50] Podsakoff PM, MacKenzie SB, Lee J-Y, Podsakoff NP. 2003. Common method biases in behavioral research: A critical review of the literature and recommended remedies. J Appl Psychol. 88(5): 879–903.

[51] Podsakoff PM, MacKenzie SB, Podsakoff NP. 2012. Sources of method bias in social science research and recommendations on how to control it. Annu Rev Psychol. 63: 539–569.

[52] Raudenbush SW, Bryk AS, Congdon R. 2013. HLM for Windows, In: Version 7.01. Vol Scientific Software International,Lincolnwood, IL.

[53] Raudenbush SW, Bryk AS. 2002. Hierarchical Linear Models: Applications and Data Analysis Methods, Vol 1. Thousand Oaks, CA: Sage.

[54] Research in Motion. 2013. BlackBerry 10: Setting New Standards in Mobile Security. http://www.bizreport.com/whitepapers/blackberry_10_setting_new_standards.html

[55] Richardson HA, Simmering MJ, Sturman MC. 2009.A Tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. Organ Res Methods 12 (4): 762–800.

[56] Rossi PH, Anderson AB. 1982. The factorial survey approach: An introduction. In: Measuring Social Judgments: The Factorial Survey Approach. Vol SAGE Publications, Inc

[57] Smith A. 2012. 46% of American Adults Are Smartphone Owners. http://www.pewinternet.org/2012/03/01/nearly-half-of-american-adults-are-smartphone-owners/

[58] Smith HJ, Dinev T, Xu H. 2011. Information privacy research: An interdisciplinary review. MIS Q. 35(4): 989–1015.

[59] Stanton JM. 2000. Traditional and electronic monitoring from an organizational justice perspective. J Bus Psychol. 15(1): 129–147.

[60] Steelman ZR, Hammer BI, Limayem M. 2014. Data collection in the digital age: Innovative. alternatives to student samples. MIS Q. 38(2): 355–378.

[61] Straub DW, Boudreau M, Gefen D. 2004. Validation guidelines for IS positivist research. Commun Assoc Inf Syst. 13 (24):380–427.

[62] Straub DW, Limayem M, Karahanna-Evaristo E. 1995. Measuring system usage: Implications for IS theory testing. Manage Sci. 41 (8):85–92.

[63] Tabak F, Smith W. 2005. Privacy and electronic monitoring in the workplace: A model of managerial cognition and relational trust development. Empl Responsib Rights J. 17(3): 173–189.

[64] Tang ZL, Hu Y, Smith MD. 2008. Gaining trust through online privacy protection: Self-regulation, mandatory standards, or caveat emptor. J Manag Inf Syst. 24(4): 153–173.

[65] Thompson RL, Higgins CA, Howell JM. 1991. Personal computing: Toward a conceptual model of utilization. MIS Q. 15(1): 125–142.

[66] Van Toorn C, Shu AY. 2010. Assessing the impact of organizational Internet and email monitoring policy on Australian employees. In: AMCIS 2010 Proceedings. Vol Lima, Peru; 1–12.

[67] Trevino LK. 1992. Experimental approaches to studying ethical-unethical behavior in organizations. Bus. Ethics Q. 2(2): 121–136.

[68] Vance A, Lowry PB, Eggett D. 2013. Using accountability to reduce access policy violations in information systems. J Manage Inf Syst. 29(4): 263–290.

[69] Vegosen J. 2010. Employee monitoring and pre-employment screening. Risk Manage 57(8): 29.

[70] Venkatesh V, Morris MG, Hall M, Davis GB, Davis FD. 2003. User acceptance of information technology: Toward a unified view. MIS Q. 27(3): 425–478.

[71] Venkatesh V, Thong JYL, Xu X. 2012. Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technolgoy. MIS Q. 36(1): 157–178.

[72] Vijayan J. 2012. NASA breach update: Stolen laptop had data on 10,000 users. http://www.computerworld.com/article/2493084/security0/nasa-breach-update–stolen-laptop-had-data-on-10-000-users.html

[73] Wallander L. 2009. 25 years of factorial surveys in sociology: A review. Soc Sci Res. 38(3): 505–520.

[74] Weeger A, Wang X, Gewald H. 2015. IT consumerization: BYOD-Program acceptance and its impact on employer attractiveness. J Comput Inf Syst. 56(1): 1–9.

[75] Whitten D, Hightower R, Lutfus S. 2014. Mobile device adaptation efforts: The impact of hedonic and utilitarian value. J Comp Inf Syst. 55(1): 48–58.

[76] Williams K, Harkins S, Latané B. 1981. Identifiability as a deterrent to social loafing: Two cheering experiments. J Personal Soc Psychol. 40(2): 303–311.

[76] Workman M. 2009. A field study of corporate employee monitoring: Attitudes, absenteeism, and the moderating influences of procedural justice perceptions. Inf Organ. 19(4): 218–232