WORKPLACE MANAGEMENT AND EMPLOYEE MISUSE: DOES PUNISHMENT MATTER?

QINYU LIAO
Univ. of Texas at Brownsville/Texas Southmost College
Brownsville, TX 78520

XIN LUO
University of New Mexico
Albuquerque, NM 87131

ANIL GURUNG
Neumann University
Aston, PA 19014

LONG LI
Grambling State University
Grambling, LA 71245

ABSTRACT

With the ubiquitous deployment of Internet, workplace Internet misuse has raised increasing concern for organizations. Research has demonstrated employee reactions to monitoring systems and how they are implemented. However, little is known about the impact of punishment-related policies on employee intention to misuse Internet. To extend this line of research beyond prior studies, this paper proposes an integrated research model applying Theory of Planned Behavior, Deterrence Theory, and Theory of Ethics to examine the impact of punishment-related policy on employees' Internet misuse intentions. The results indicate that perceived importance, perceived behavioral control and subjective norms have significant influence on employee intention to avoid Internet misuse. Contrary to expectations, there is no support for the influence of punishment severity and punishment certainty.

KEYWORD: Workplace Internet use monitoring, Internet misuse, monitoring, behavioral intentions.

1. INTRODUCTION

During the past decade, ubiquitous deployment of the Internet has reshaped the workplace into an interconnected zone strengthening and catalyzing the organization's productivity. Telecommunication tools such as email, instant messaging and Internet access have revolutionized the way organizations manage and control their daily operations. However, the benefit of quick access to timely data and less restricted communications has been accompanied by reduced productivity, Internet addiction, increased legal liability, bandwidth waste, and security concerns [61, 45, 50, 54, 23]. A recent study shows that on average more than 81 minutes of work time per employee per day is wasted doing non-work-related computer activities [48]. In parallel, the Computer Crime and Security Survey of the Computer Security Institute (CSI) reports that 49% of respondents faced IT security incidents due to irresponsible acts of legitimate users [49].

It has been suggested that a clearly defined Internet access policy is a proactive approach to improve employee productivity in the long run with minimum monitoring [17, 50]. Yet results from studies are mixed. Kim [47] found that when an employee Internet management system was introduced in a Korean company, online search time decreased by 41% while others indicated that monitoring policies and systems are not effective in altering individuals' Internet behavior [31, 51]. One of the two reasons suggested is lack of punishment. Companies that do employ e-management measures are lenient in enforcement [14], whereas many employees are not aware of any disciplinary actions taken [54].

It is important for managers to understand how Internet use monitoring affects employee's Internet use behavior so that technology and Internet access policy can be tailored accordingly. Yet it has been a rather unexplored area in IS research. Thus, to bridge the research gap, this study employs Theory of Planned Behavior, the Deterrence Theory, and Theory of Ethics to investigate factors influencing employees' workplace Internet misuse intention. Our approach attempts to examine an individual's moral intensity grounded in teleological theories, in parallel with ethical decision-making process, that investigate the consequences of an action in organizations facing internal and external threats. Drawing on research in social ethics and information systems, we posit that the degree of importance of an issue is expected to influence employees' attitudes as to what constitute moral or immoral behavior under the circumstances (i.e., punishment). In addition to extending previous research on ethical decision-making and user behavior in various information security situations, this work furthers our understanding of individual and situational characteristics in security threats, organizational security mechanisms, and moral involvement. An integrative model is proposed and is empirically examined using data collected from various industrial segments. Moreover, managerial suggestions are offered for organizations to cultivate employee voluntary avoidance of Internet misuse.

The remainder of this article is structured as follows: the following section thoroughly revisits literature of Internet misuse and discusses the related theoretical underpinnings; the next section explains the research methodology, followed by data analysis and results. Implications are then offered, followed by a discussion of the research limitations and future research directions.

2. THEORETICAL DEVELOPMENT

In this section, we review literature related to user behavior,

Received: December 12, 2008 Revised: June 18, 2009 Accepted: July 15, 2009

threats deterrence, and human ethics to develop the theoretical model and hypotheses.

2.1. Recent Studies

Internet misuse, according to Lim [54], is "*any voluntary acts of employees using their companies' Internet access during office hours to surf non-job-related websites for personal purposes and to check personal emails*". It ranges from browsing non-work-related websites or taking time to check personal emails, or more destructive acts such as moonlighting for additional income, downloading information, or transmitting confidential data [12]. It can sometimes escalate to e-crimes including intellectual property theft, distributing offensive materials, and online piracy of copyrighted materials [17], thereby compromising the integrity, confidentiality, and availability of information assets in an organization.

To deal with the far-reaching categories of misconduct and risks faced, organizations have responded by using Internet use monitoring technologies that enable detection and control of undesirable employee behavior [52, 61, 71] despite the concerns for employee privacy, quality of work-life, fairness judgments, monitoring costs and increased employee stress [79, 81, 71]. According to a 2005 survey by American Management Association, 76% of companies monitor connections to websites by employees, 65% of companies block inappropriate websites using URL blocking software and 55% retain and review email messages. Furthermore, approximately 26% of companies have fired workers for misusing the Internet, 25% have fired employees for misusing email [9]. Worldwide, about 27 million employees are under such monitoring [27, 23].

Prior to the pervasive use of the Internet, monitoring studies focused on "junk computing" and computer abuse [33, 35, 41, 67, 66, 68, 70]. The research stream gradually evolved to the design and examination of information security strategies against Internet abuse [69, 70]. Previous studies have primarily examined different types of workplace monitoring and their effects on employee job performance and satisfaction [32, 76]. Positive forms of monitoring are more instructive and acceptable to employees. Employees may accept some level of email and Internet monitoring if the employer can make a convincing social account of the need for a policy and the policy must be clearly communicated and properly implemented [21]. Employee and organizational factors have been combined to study the impact of employee Internet use management on productivity [14]. Formal characteristics of monitoring implementation are less important than the organizational climate in determining employee reactions to Internet monitoring [6].

Recent studies paid more attention to individual behavioral adjustment for legitimate Internet use in organizations. Zweig and Websteb [82] found that people who scored lower in extraversion and emotional stability are less likely to endorse positive attitudes toward monitoring, even with privacy and fairness safeguards in place. Harrington [35] discovered that codes of ethics have little effect on computer abuse judgments and intentions relative to the psychological trail of responsibility denial. There are also studies on the impact of Internet monitoring on employee attitudes and behaviors, such as the perceptions of privacy [8], fairness and justices [8, 65], and work stress [40]. Alder et al. [7] investigated the impact of individual differences on reactions to monitoring. Little has been done on how punishment-related Internet use policies can affect employee Internet misuse behavior.

2.2. Theory of Planned Behavior

The Theory of Planned Behavior (TPB) was designed to predict behavior across many settings. It provides more specific information as to what users consider when making a decision [55]. According to the theory, behavior intention is jointly determined by attitude toward the behavior, subjective norms, and perceived behavioral control. It has been successfully applied to the understanding of individual acceptance and usage of many different technologies [36, 55, 72]. TPB is used here to investigate how workplace management (ie. punishment for non-compliance) affects employee Internet misuse behavior. We propose that an employee's workplace Internet use behavior is simultaneously determined by such factors as positive/negative evaluative effects of Internet misuse avoidance, perceptions of opinions on avoidance of Internet misuse, and perceptions of the availability of the skills, resources and opportunities to avoid Internet misuse. Therefore, it is proposed that a more positive attitude towards Internet misuse avoidance, a high level of subjective norms towards Internet misuse avoidance, and a high level of perceived behavioral control will lead to greater intention to avoid Internet misuse.

The importance of attitude, subjective norms, and perceived behavioral control are expected to vary across situations [5]. Therefore, it is necessary to examine the significance of each factor in predicting Internet misuse intentions. Attitude is a function of the products of behavioral beliefs and outcome evaluation. A behavioral belief is the subjective probability that the behavior will lead to a particular outcome. An outcome evaluation is a rating of the desirability of the outcome. Attitude has been proposed to influence behavioral intentions in multiple theories, such as TPB [5] and TRA [28]. The theoretical predictions of these theories have received substantial empirical support in multiple contexts. Applied to this study, favorable attitude toward workplace Internet misuse avoidance is likely to encourage employees to avoid workplace Internet misuse, reduce Internet use time on non-work related tasks, and voluntarily follow organization Internet policies. This leads to the following hypothesis:

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

Behavior occurring in a social interaction may not be under a single person's direct control because there are external variables, including the referent other's action that may influence that control. Subjective norms reflect the perceived opinions of referent others. A referent other is a person or group whose beliefs may be important to an individual [2]. A normative belief is an individual's perception of a referent other's opinion about the individual's performance of a behavior [75]. Motivation to comply is the extent to which a person wants to comply with the wishes of the referent other. According to previous studies, subjective norm has an impact on individual behavior through three mechanisms: compliance, internalization, and identification [77, 80]. While the later two relate to altering an individual's belief structure and/or causing an individual to respond to potential social status gains, the compliance mechanism causes an individual to simply alter his or her intention to respond to the social pressure. Prior studies suggest that individuals are more likely to comply with expectations of others when those referent

others have the ability to reward the desired behavior or punish non-behavior [30, 80]. This view of compliance is consistent with the results in the technology acceptance literature indicating that reliance on others' opinions is significant only in mandatory settings [37], particularly in the early stages of experience while an individual's opinion are relatively ill-informed [1, 37, 46, 72, 73, 77]. Chiasson and Lovato [81] reported that subjective norm is a significant antecedent of IS adoption intention, and Morris and Venkatesh [56] found that IS workers were strongly influenced by subjective norms.

Some studies suggest that not only perceived social pressures but also personal feelings of moral obligation or responsibility to perform, or refuse to perform a certain behavior [52, 59, 63] are influenced by subjective norms. Alder [6] argued that organizational culture interacts with monitoring system characteristics to determine employees' perception of fairness and their acceptance of the system. He found that organizational members' perception of Internet monitoring system also depends on the workplace context [8]. We argue that an employee's subjective norm towards avoidance of Internet misuse that reflects the opinion of his or her supervisors and peers will have an influence on the intention to avoid Internet misuse behavior. Therefore,

H2: Subject norms towards Internet misuse avoidance will have a significant influence on intention to avoid Internet misuse.

Perceived behavioral control refers to the individual's perception of whether an action is within their control [5]. Perceived behavioral control depends on control beliefs and perceived facilitation. A control belief is a perception of the availability of skills, resources, and opportunities. Perceived facilitation is the individual's assessment of the importance of those resources to the achievement of outcomes. Ajzen [3] differentiates perceived behavioral controls as internal and external control factors. Internal factors are characteristics of the individual, including personality, skills and will power. External factors that depend on the situation include time, opportunity and the cooperation of others.

Research literature demonstrated support for the role of perceived behavioral control on behavioral intention. For example, Mathieson [55] showed that behavioral control influences the intention to use an information system. A positive relationship between control and intentions was also found by Taylor and Todd [72] who examined users at a computer resource center. In the context of this study, the more a computer user understands the skills and mechanism of Internet misuse avoidance, the more likely he/she is going to avoid Internet misuse. Behavioral control should have a positive effect on employees' intention to avoid Internet misuse.

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

2.3. Deterrence Theory

A person's behavior can be framed as an emergent function of the individual and the context [53]. Whereas TPB focuses more on a set of individual characteristics, Deterrence Theory provides a specific context to show how the context influences the individual and his/her behavior. General Deterrence Theory asserts that illegal behavior in the general population will vary inversely with more certain and severe punishment [57]. Laws and legal sanctions or sanction threats may lead to total prevention of a particular deviance, may change the flagrancy of its manifestations or may reduce the frequency with which such acts are done. Deterrence Theory identified punishment severity and punishment certainty as the two factors related to outcomes [74]. That is, when punishment severity and punishment certainty increase, the level of unwanted behavior should decrease. Deterrence Theory has been used to study the relationship between crime and the expected cost [26]. Straub [68] has applied Deterrence Theory to study primary strategies for reducing computer abuse. Peace et al. [58] used it to study software piracy. Henle and Blanchard [40] found that employees are more reluctant to use cyber-loafing when they perceive that there are organizational sanctions against this behavior. Deterrence Theory highlights the importance of cost. The low probability of being caught was listed in a recent survey as the seventh most important reason in decision to copy software illegally [18].

We propose that both punishment severity and punishment certainty affect employee intention to avoid Internet misuse by influencing on its three predictors, attitude towards Internet misuse avoidance, perceived behavioral control towards Internet misuse avoidance, and subjective norm towards avoidance of Internet misuse. When the Internet use policies are well-communicated and distributed in an organization, they can be well-received by employees. When the monitoring technologies are broadly understood and the chances of being caught and the level of punishment increase, the social norm of the organization against the misuse of the Internet changes. The employees will be less likely to misuse Internet because the consequences of being caught could lead to negative outcome like demotion, dismissal or other disgraceful disciplinary actions. Therefore,

H4: Punishment severity will have a significant influence on attitude towards Internet misuse avoidance.

H5: Punishment severity will have a significant influence on subjective norm towards Internet misuse avoidance.

H6: Punishment severity will have a significant influence on perceived behavior control towards Internet misuse avoidance.

H7: Punishment certainty will have a significant influence on attitude towards Internet misuse avoidance.

H8: Punishment certainty will have a significant influence on subjective norm towards Internet misuse avoidance.

H9: Punishment certainty will have a significant influence on perceived behavior control towards Internet misuse avoidance.

2.4. Theory of Ethics and Perceived Importance

Theory of Ethics posits that individual ethical decision making is primarily through one's deontological and teleological evaluations [42, 43]. While deontology focuses on the decision maker's specific behaviors, teleology emphasizes more on the consequences of those behaviors. In a teleological approach, decision makers evaluate the inherent rightness or wrongness

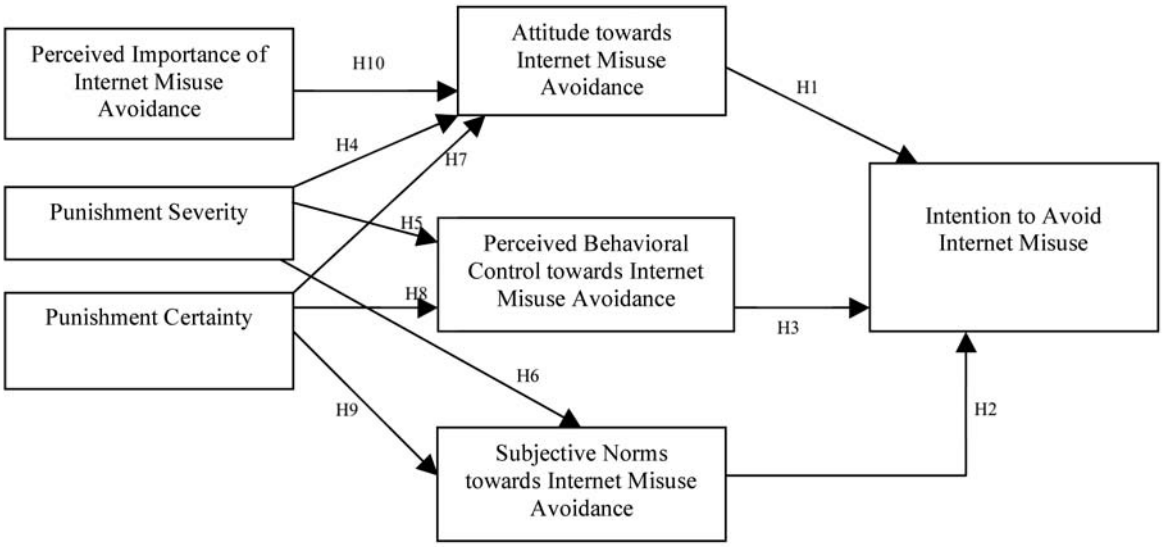

FIGURE 1: Research Model

of various behaviors, which are determined by the application of universal moral principles that have been established through objective reason [78]. Whereas deontological theories focus on the rightness or wrongness of specific actions and therefore lack practical application in day-to-day situations, the Hunt-Vitell model treats teleology as a consequentialist perspective where the issue of moral over immoral consequences depends on who is affected. As such, it has been suggested that individuals within business organizations must first perceive ethics and social responsibility to be important before their behavior is likely to become more ethical and reflects greater social responsibility. For an individual employee, the perceived importance of ethics and social responsibility for organizational performance is likely to be a key background factor and a critical determinant of whether an ethical problem is perceived in a given situation, as well as a determinant of other critical variables.

In the arena of social ethics, Jones [44] birthed *moral intensity* which consists of magnitude of consequences, social consensus, probability of effect, temporal immediacy, proximity, and concentration of effect. He posited that moral intensity can influence ethical decision-making in business. Robin et al. [60] further extended the research on moral intensity and empirically developed and validated a similar construct termed PIE (perceived importance). Defined as *the perceived personal relevance or importance of an ethical issue to an individual*, PIE parallels the concepts of user and social involvement. They argued that PIE differs from Jones' [44] moral intensity in that he focused on exogenous characteristics of the issue rather than individual perceptions. For an ethical decision-making process, after the individual recognizes that the issue has moral ramifications, the degree of importance of the issue is expected to influence his/her judgment as to what constitutes moral or immoral behavior under the circumstances.

Robin et al. [60] defined PIE as *an individual state construct that is believed to be closer to the behavioral intention and behavior decisions than the moral intensity construct suggested by Jones* [44]*, and hence, is likely to be a better predictor of those decisions*. Haines et al. [34] found that PIE does a decent job of capturing the personal internal state aspect of the moral involvement concept since it recognizes that what is truly important is the decision-makers' perceptions of the issue's characteristics, not just the characteristics in and of themselves. Using different computing scenarios describing IT ethical problems and a survey, Cronan et al. [22] validated and extended the perceived importance work of Robin et al. [60] and assessed the role of PIE in ethical decision-making. They acknowledged that PIE is a critical component of ethical decision-making, which is a function of ethical judgment.

From a teleological perspective, Singhapakdi [64] argued that the ethical judgment involves a process wherein an individual evaluates alternative actions by considering what he/she perceives as probable consequences, the desirability of those consequences, and the relative importance of various stakeholders. Drawing on Hunt and Vitell's Theory of Ethics which depicts perception of an ethical problem as the catalyst of the whole ethical decision process, we believe that individuals who are more sensitive ethically would tend to take certain actions to remedy an ethical problem. When applying TPB into this ethical decision-making process, we postulate that individuals who perceive ethics and social responsibility to be important would generally have a higher degree of moral attitude toward their behavioral intentions than their counterparts. As such, we posit that attitude serves as a mediator between PIE and one's behavioral intention in an ethical decision-making situation. That is, the greater the perceived importance of an ethical issue the greater the attitude toward immoral activities avoidance which in turn corresponds with a greater degree of intention to behave ethically. In this context, the perceived importance could refer to perception of the benefits of Internet misuse avoidance, privacy sacrificed and the effectiveness of the Internet monitoring. This leads to the following hypothesis:

H10: Perceived importance will have a significant influence on attitude towards Internet misuse avoidance.

3. RESEARCH METHOD

3.1. Sample

To test the proposed research hypotheses, as shown in Figure

1, we used data collected from surveys. Participants were asked to evaluate their responses regarding their company's Internet use monitoring system. Before the final survey instrument was administered, it was pilot-tested. The approximate time taken for completing the survey was around 10 minutes. Based on the feedback, some items were reworded for clarity.

For the final study, email invitations to participate in the web survey were sent to contacts in various companies with requests to distribute it to their colleagues. The email notification outlined the purpose of the study and contained a link to the web survey which could be completed anonymously. The survey was completely voluntary and the participants could exit the survey at any time. Of the 500 respondents contacted, 249 started the survey but only 205 completed it. Therefore, the dataset for analysis was 205.

In the data sample, 55.61% comprised of male while 44.39% were female. The age distribution was as follows: 2.5% were under age 20; 38% between 20 and 29; 40% between 30 and 39; 15.5% between 40 and 49; and 4% were over 50. The industries represented by the respondents are given in Table 1. The survey instrument was administered to employees in companies from a variety of industries. Pharmaceutics, banking, financial service, and insurance have comparatively higher information security requirement and high rate of active monitoring [25]. As for internet experience, 5.37% had up to 5 years; 47.5% up to 10 years; and 47.13% had over 10 years. 74.13% of the respondents reported having an internet use policy at their companies; 11.44% reported not having any internet use policy while 14.43% were unsure if they had one in their companies.

3.2. Instrument

The constructs measured in this study are perceived importance of Internet misuse avoidance, punishment severity, punishment certainty, attitude, subjective norms, perceived behavior control, and intention of IS misuse avoidance. The instrument was adapted from prior studies [60, 16, 55, 58]. All items used are five-point Likert scales (see Appendix for survey questions).

TABLE 1. Industry Representation of the sample

Industry	Percentage
Airlines/Aviation	2.52%
Architecture and Engineering	3.36%
Banking, Insurance & Financial services	15.13%
Education	24.37%
Government	4.20%
Healthcare & Pharmaceuticals	7.56%
Industrial & Mfg	10.92%
Non-profit	2.52%
Telecommunications	1.68%
Hotel & Tourism	2.52%
Real Estate/ Property mgmt	1.68%
Retail	6.72%
International business	4.20%
IT and services	9.24%
Other	3.36%

4. DATA ANALYSIS AND RESULTS

Partial Least Squares (PLS) was employed to test the research model since it is best suited for complex models, with many constructs hypothesized in different relationships. PLS estimation is based on ordinary least squares iterations on subsets of model parameters thus requiring few distributional measurements [20, 29]. For resampling, bootstrap method with 200 resamples was used to test the significance of the path coefficients in the structural model.

4.1. Measurement Model

The measurement model was validated by assessing internal consistency and the convergent and the discriminant validity of the instrument items. A scale is deemed reliable if its composite reliability (CR) is above 0.7 and the average variance extracted (AVE) is above 0.5 [10]. Table 2 lists the scales and their internal consistencies. One item, SN1 did not meet the requirements and was dropped. The rest of the items met the suggested threshold of composite reliability and average variance extracted. The convergent validity is established when each measurement item correlates with its related theoretical construct. As suggested by Bagozzi and Yi [10], all indicators of latent constructs exceeded the threshold of 0.6, which is shown by item loadings in Table 2, thus maintaining convergent validity. The discriminant validity is inferred when each measurement item correlate weakly with all the constructs except for its theoretically linked construct. The discriminant validity can be tested by examining if the square root of AVE of each construct is higher than the inter-construct correlation [29]. Table 3 shows that the square root of AVE of each construct is greater than the inter-construct correlation. These tests demonstrated that the measures have adequate convergent and discriminant validity. The data were also tested for multicollinearity by examining values for variance inflation factor (VIF) and tolerance values. The result of the test is shown in Table 4. Based on results for all the cases, the VIF values of below 10 and tolerance values indicated that multicollinearity among the independent variables was not a problem.

4.2. Structural Model

The structural model was tested through estimates of the path coefficients, coefficient of determination (R^2) values which collectively show whether data support the hypothesized model. Figure 2 summarizes the results of hypotheses testing. Perceived importance of Internet misuse avoidance, attitude, punishment certainty, perceived behavior control and subjective norms were significant predictors of intention of misuse avoidance. The variance in the intention as accounted by the predictors was 42.2%. Perceived importance had significant relationship with attitude. However, there was no support for the relationship of punishment severity and punishment certainty with attitude. Punishment severity had significant relationship with subjective norms while punishment certainty was not significant with subjective norms. In congruence with prior research, attitude, subjective norms and perceived behavior control showed significant relationship with the intention. A summary of the results from hypotheses testing is shown in Table 5.

TABLE 2. Item Loadings, Composite Reliabilities and Average Variance Extracted

Construct	Item	Loadings	CR	AVE
Perceived Importance of Internet Misuse Avoidance (PIE)	PIE1 PIE2 PIE3 PIE4	0.9313 0.9252 0.9053 0.8683	0.949	0.824
Punishment Severity (PS)	PS1 PS2	0.9230 0.9722	0.947	0.899
Punishment Certainty (PC)	PC1 PC2	0.8764 0.8991	0.882	0.788
Attitude towards Internet Misuse Avoidance (ATT)	ATT1 ATT2 ATT3 ATT4	0.8521 0.8954 0.8979 0.8820	0.933	0.778
Subjective Norms towards Internet Misuse Avoidance (SN)	SN2 SN3	0.9380 0.7482	0.835	0.720
Perceived Behavior Control towards Internet Misuse Avoidance	PBC1 PBC2	0.8544 0.8953	0.867	0.766
Intention to avoid Internet Misuse (IAM)	IAM1 IAM2 IAM3	0.9027 0.8818 0.8039	0.898	0.746

TABLE 3. Correlation Matrix, Mean, Standard deviations and the Square Root of Average Variance Extracted for Constructs

	Mean	SD	PIE	PS	PC	ATT	SN	PBC	IAM
Perceived Importance (PIE)	2.21	.97	**.908**						
Perceived Severity (PS)	2.81	1.22	.250	**.948**					
Perceived Certainty (PC)	3.05	1.08	.027	.455	**.888**				
Attitude (ATT)	4.00	.96	.287	-.082	-.073	**.882**			
Subjective Norms (SN)	3.09	1.12	.031	.324	.213	.009	**.849**		
Perceived Behavior Control (PBC)	1.83	.95	.203	.023	-.076	.307	.104	**.875**	
Intention to avoid Internet Misuse (IAM)	2.03	.98	.374	.220	.219	.535	.154	.377	**.864**

Note: The square roots of AVEs are shown on diagonals. Off-diagonal elements are the correlations among constructs

TABLE 4. Testing for Multicollinearity

Variable	Tolerance	Variance Inflation Factor (VIF)
Perceived Importance (PIE)	.841	1.189
Punishment Severity (PS)	.698	1.432
Punishment Certainty (PC)	.783	1.277
Attitude (ATT)	.845	1.184
Subjective Norms (SN)	.887	1.127
Perceived Behavior Control (PBC)	.866	1.154

TABLE 5. Summary of Hypothesis Tests

Hypothesis	Path Coefficient	P-value	Support
H1: ATT → IAM	.466	< .001	y
H2: SN → IAM	.127	< .05	y
H3: PBC → IAM	.221	< .01	y
H4: PS → ATT	.026	n.s.	x
H5: PS → PBC	.077	n.s.	x
H6: PS → SN	.287	<.001	y
H7: PC → ATT	.077	n.s.	x
H8: PC → PBC	.109	n.s.	x
H9: PC → SN	.082	n.s.	x
H10: PIE → ATT	.291	< .001	y

Legend: y = Supported; x = Not supported; n.s. = Not significant

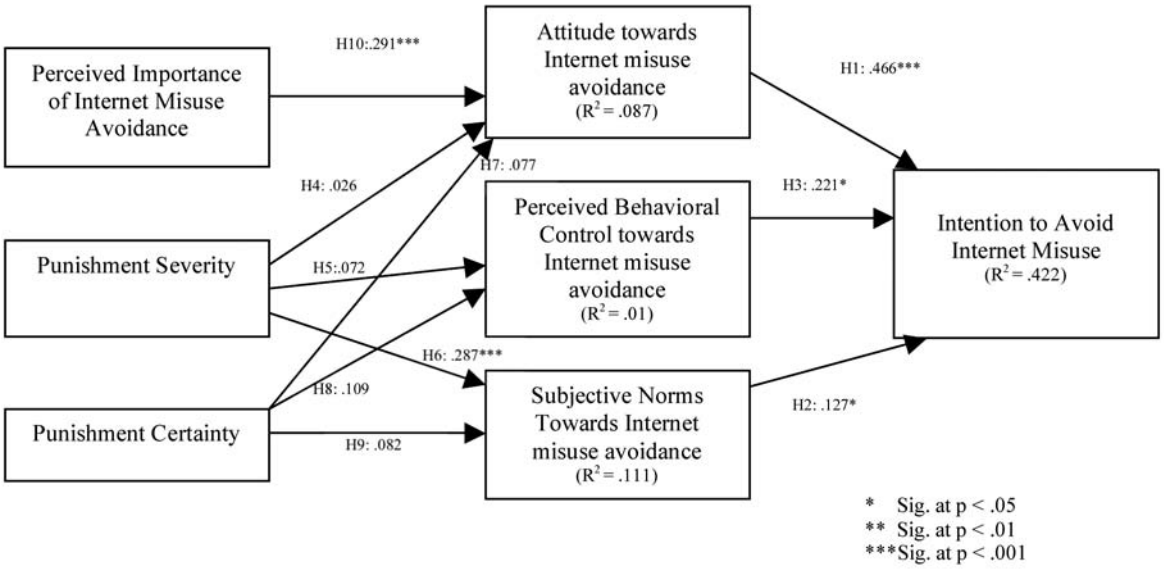

FIGURE 2. Results of Data Analysis

4.3. Post-hoc Analysis

To ascertain that our proposed model is competent in comparison with other alternate models, we ran an alternative model without the constructs from the TPB. In essence, we tested the model with four variables, such as, perceived importance, punishment severity, punishment certainty and intention. The alternative model explained 18.6% of the variance in intention as compared to 42.2% of the variance in our proposed model. In the alternative model, perceived importance and punishment certainty were significant with the intention while perceived severity was not. The model suggested that perceived importance and punishment certainty were significant factors in predicting intention and further supported our contention of incorporating these variables in our model. Therefore, we can conclude that perceived importance is an important factor in our model since it may influence intention indirectly through attitude as well as directly. We can also conclude that punishment certainty is another important factor that can indirectly influence intention.

5. IMPLICATIONS

The findings from this study have both theoretical and practical implications. This study examined the effects of perceived importance of avoiding Internet misuse, punishment severity, and punishment certainty on attitude, perceived behavior control, and subjective norms which would consequently influence the intention to avoid Internet misuse. Our attempt should be viewed as a positive step towards explaining the important factors that can influence employee Internet misuse avoidance in the workplace.

Consistent with previous finding by Alder et al. that formal characteristics of monitoring implementation were less important than the organizational climate in determining employee reactions to Internet monitoring [6], employee subjective norm had a significant influence on intentions to avoid Internet misuse. Perceived importance was also found to be positively related to intention to avoid Internet misuse. This may also be the reason why studies [6] found that having an Internet use policy is insufficient but failure to cultivate an organization environment that welcomes such policy is more detrimental in preventing workplace Internet misuse.

The study showed that perspectives of Deterrence Theory are useful in understanding the punishment-related factors in Internet monitoring/policy research. While punishment severity only significantly influenced subjective norm towards Internet misuse avoidance, the results did not support positive relationship between punishment certainty and any of the antecedents of intention to avoid Internet misuse in the TPB. This coincides with the finding by De Manrique Lara and his colleagues [24] that although organizational control decreases cyber-loafing, perceived fear of formal punishment actually increases. The results suggested that the high probability of being caught did not affect the intentions to avoid Internet misuse but punishment severity did influence the subjective norm, which in turn affected intention to avoid Internet misuse. Employees seemed more concerned about the actual severity of the punishment than being caught. This may be explained by the fact that most companies are lenient with their Internet use policies and many disciplinary incidents were not communicated with the employees [14, 54]. Therefore, the leniency on Internet misuse and the reluctance to expose any disciplinary incidents by the company can create illusive impressions to other employees. They don't perceive the policies as a reinforced one so that they can avoid the disciplinary action and social ostracization and may not think it necessary to alter their Internet misuse behavior. Only when there is some serious disciplinary actions taken, they may think about changing their Internet misuse behavior because the "reference others" are modifying their behavior as a result of the action.

This also indicated that there may be other important factors that could explain the intention to avoid Internet misuse. The Internet misuse behavior is a complex social phenomenon which needs to be studied with more sophisticated models to fully understand the motivational factors, consequences, and organizational contexts. As organizations encourage social computing such as wikis and blogs, it may be more challenging to control Internet misuse behavior.

For industry decision makers, our results provide insight to organizations and managers in stipulating Internet use policies

and in choosing the more effective discipline regime. More effective security policies and practices should be designed along with the use of monitoring application in organizations. Security policies need to clearly outline disciplinary actions that will be taken against violators. Routine checks for security practices should be conducted and disciplinary actions taken should be properly communicated to employees because the results of this study suggested that the general deterrence of perceived severity can influence subjective norm towards Internet misuse avoidance, which may lead to change in Internet misuse intention. The communication of security policies should be widely dispersed throughout the organization because the effectiveness of these policies would be limited if employees are not aware of them, and they may not take it seriously if nobody has ever been known to be disciplined. Organizational culture and behavior norms can be established by employee training programs to alleviate the load on actual monitoring. A better communicated Internet policy will be more acceptable to employees and that may lead to voluntary avoidance of Internet misuse, reduced monitoring costs, alleviating employee negative attitudes towards Internet use policies, lower workplace stress with minimum monitoring investment, and eventually voluntary employee Internet use behavioral change.

6. LIMITATIONS AND DIRECTIONS FOR FUTURE STUDIES

Due to the convenience sample used in this study, we were not able to investigate how employees in difference industries react differently in their attitudes towards Internet misuse avoidance and behavior intention to avoid workplace Internet misuse. Certain industries may have stricter Internet use policies and monitoring which may induce different employee compliance and reaction process with different factors involved.

Although this study contributes to the field using a one-point field survey rather than the lab studies, a longitudinal study may reveal different insights about the change of employee attitude and behavior intentions. Since the manner in which monitoring was conducted is more important than the characteristics of monitoring implementation, organizational factors (trust, organizational climate, scope of monitoring, etc.) as well as employee factors (perceived fairness, seclusion of office, workload, historical acceptance of company policies etc.) should be included in future studies.

7. CONCLUSION

Using TPB, Deterrence Theory and PIE, this study identified several factors that may influence employees' workplace Internet misuse behavior intention. Policy-related factor such as punishment certainty was found insignificant in determining employee attitude, behavioral control and subjective norm towards Internet misuse, but punishment severity has a significant impact on subjective norm towards Internet misuse avoidance. The Internet misuse avoidance can be more effective should there be a pleasant and legally defensible working environment instead of a hostile atmosphere. By strengthening their perceived importance, subjective norms and perceived behavioral control towards Internet misuse avoidance, employees may be more willing to accept monitoring and avoid Internet misuse that may protect or benefit themselves and the company in the long run.

REFERENCES

[1] Agarwal, R. and Prasad, J. "The Role of Innovation Characteristics and Perceived Voluntariness in the Acceptance of Information Technologies," *Decision Sciences* 28(3), 1997, 557-582.

[2] Ajzen, I. and Fishbein M. *Understanding Attitudes and Predicting Social Behavior*, Prentice Hall, Eaglewood Cliff, NJ, 1980.

[3] Ajzen, I. "From Intentions to Actions: a Theory of Planned Behavior," In J. Kuhl & J. Beckmann (eds.), *Action control: From Cognition to Behavior*, Springer, Heidelberg, Germany, 1985, 1139.

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

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

[6] Alder, G. S., Ambrose, M. L., and Noel, T. W. "The Effect of Formal Advance Notice and Justification on Internet Monitoring Fairness: Much About Nothing?" *Journal of Leadership and Organizational Studies* 13(1), 2006, 93-108.

[7] Alder, G. S., Schminke, M., Noel, T., and Kuenzi, M. "Employee Reactions to Internet Monitoring: The Moderating Role of Ethical Orientation," *Journal of Business Ethics* 80(3), 2008, 481-498.

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

[9] American Management Association "2005 Electronic Monitoring and Surveillance Survey: Many Companies Monitoring, Recording, Videotaping- Firing-Employees," *2005 AMA Survey, Summary of Key findings*. Retrieved January 27, 2006 from http://www.amanet.org/press/amanews/ems05.htm

[10] Bagozzi, R. P. and Yi, Y. "On the Evaluation of Structural Equation Models," Academy of Marketing Science 16(1), 1988, 74-94.

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

[12] Blau, G., Yang, Y., and Ward-Cook, K. "Testing a Measure of Cyberloafing," *Journal of Allied Health* (35), 2004, 9-17.

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

[14] Case, C. J. and Young, K. S. "Employee Internet Management: Current Business Practices And Outcomes," *CyberPsychology & Behavior* 5(4), 2002, 355-361.

[15] Chalykoff, J. and Kochan, T. "Computer-Aided Monitoring: Its Influence On Employee Job Satisfaction And Turnover," *Personnel Psychology* (42), 1989, 807-834.

[16] Chau, P. Y. K. and Hu, P. J. "Investigating Healthcare Professionals' Decisions To Accept Telemedicine Technology: An Empirical Test of Competing Theories," *Information & Management* 39(4), 2002, 297-311.

[17] Chen, J. V., Chen, C. C., and Yang, H.-H. "An Empirical

Evaluation of Key Factors Contributing to Internet Abuse In The Workplace," *Industrial Management & Data Systems* 108(1), 2007, 87-106.

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

[19] Chiasson, M. W. and Lovato, C.Y. "Factors Influencing the Formation of a User's Perception and Use of a DSS Software Innovation," *Database for Advances in Information Systems* 32(3), 2007, 16-35.

[20] Chin, W. W. "The Partial Least Squares Approach to Structural Equation Modeling," In G. A. Marcoulides (Ed.) *Modern Methods for Business Research*, Lawrence Erlbaum, Mahway, New Jersey, 1998, 295-336,

[21] Cohen, C. and Cohen, M. "On-Duty and Off-Duty: Employee Right to Privacy and Employer's Right to Control the Private Sector," *Employee Responsibilities & Rights Journal* 19(4), 2007, 235-246.

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

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

[24] De Manrique Lara, P. Z. "Fear in Organizations: Does Intimidation by Formal Punishment Mediate the Relationship between Interactional Justice and Workplace Internet Deviance?" *Journal of Managerial Psychology* (21), 2006, 580-592.

[25] Dzamba, A. "AMA Reveals Monitoring of Employees' Online Activity Rises Sharply," *IOMA's Report on Managing HR Information Systems* 7(45), 2001, Available from: <www.worldatwork.org/pub/E158673055X_smp.pdf >.

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

[27] Firoz, N. M., Taghi, R., and Souckova, J. "Emails in the Workplace: the Electronic Equivalent of 'DNA' Evidence," *Journal of American Academy of Business* (8), 2005, 71-78.

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

[29] Fornell, C. and Larcker, D. F. "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research* 18(1), 1981, 39-50.

[30] French, J. R. P. and Raven, B. *The Bases of Social Power, in Studies in Social Power*, D. Cartwright (Ed.), Institute for Social Research, Ann Arbor, MI, 1959, 150-167.

[31] Galletta, D. F. and P. Polak, "An Empirical Investigation of Antecedents of Internet Abuse in the Workplace," Proceedings of the 2nd Annual Workshop on HCI Research in MIS, Seattle, WA, Dec. 12-13, 2003.

[32] George, J. F. "Computer-Based Monitoring: Common Perceptions and Empirical Results," *MIS Quarterly* 20(4), 1996, 459-480.

[33] Guthrie, R. and Gray, P. "Junk Computing: Is It Bad for an Organization," *Information Systems Management* 13(11), 1996, 23-28.

[34] Haines, R., Street, M. D., and Haines, D. "The Influence of Perceived Importance of an Ethical Issue on Moral Judgment, Moral Obligation, and Moral Intent," *Journal of Business Ethics* (81), 2008, 387-399.

[35] Harrington, S. J. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," *MIS Quarterly* 20(3), 1996, 257-278.

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

[37] Hartwick, J. and Barki, H. "Explaining the Role of User Participation in Information System Use," *Management Science* 40(4), 1994, 404-465.

[38] Haythornthwaite, C. and Wellman, B. "Work, friendship, and Media Use for Information Exchange in A Networked Organization," *Journal of American Society for Information Science* 49(12), 1998, 1101-1114.

[39] Haythornthwaite, C., Wellman, B., and Garton, L. "Work and Community via Computer-Mediated Communication" in J. Gackenbach (Ed.) *Psychology and the Internet: Intrapersonal, Interpersonal, and Transpersonal Implication*s, Academic Press Inc., San Diego, CA, 1998.

[40] Henle, C. A. and Blanchard, A. L. "The Interaction of Work Stressors and Organizational Sanctions on Cyberloafing," *Journal of Managerial Issues* XX(3), 2008. 383-400.

[41] Hoffer, J. A., and Straub, D. W. "The 9 to 5 Underground: Are You Policing Computer Crimes?" *Sloan Management Review* 30(4), 1989, 34-44.

[42] Hunt, S. D. and S. J. Vitell "A General Theory of Marketing Ethics," *Journal of Macromarketing* 8(Spring), 1986, 5-16.

[43] Hunt, S. D. and Vitell, S. J. "The General Theory of Marketing Ethics: A Retrospective and Revision" in Smith and Quelch (Eds.), *Ethics in Marketing*, Irwin, Homewood, IL, 1993.

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

[45] Kamins, A. "Cyber-loafing: Does Employee Time Online Add Up to Net Losses?" *New York Daily News*, July 16, 1995.

[46] Karahanna, E., Straub, D. W., and Chervany, N. L. "Information Technology Adoption across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs," *MIS Quarterly* 23(2), 1999, 183-213.

[47] Kim, S. "Economics of Employee Internet Management," *The Bottom Line: Managing Library Finances* (19), 2006, 124-138.

[48] Klein, K. E. "Setting a Realistic Web-Use Policy," *Business Week Online*, July 28, 2007, 18-18.

[49] Lara, P. Z. M. D., Tacoronte, D. V., and Ding, J.-M. T. "Do Current Anti-Cyberloafing Disciplinary Practices Have a Replica in Research Findings? A Study of the Effects of Coercive Strategies on Workplace Internet Misuse," *Internet Research* 16(4), 2006, 450-467.

[50] Lara, P. Z. M. D. "Relationship between Organizational Justice and Cyberloafing in the Workplace: Has "Anomia" a Say in the Matter?" *CyberPsychology & Behavior* 10(3), 2007,8.

[51] Lee, Z., Lee, Y., and Kim, Y. "Personal Web Page Usage in Organizations," in M. Anandarajan and C. Simmers (eds.), *Personal Web Usage in the Workplace: A guide to Effective*

Human Resources Management, Information Sciences Publishing, Hershey, PA, 2004, 28-46.
[52] Levin-Epstein, M. "HR Plays Growing Role in Monitoring Employee Internet Use," *Staff Leader* 16(4), 2002, 34.
[53] Lewin, L. *Field Theory in Social Science; Selected Theory Papers,* Harper & RW, New York, NY 1951.
[54] Lim, V. "The IT Way of Loafing on the Job: Cyberloafing, Neutralizing, and Organizational Justice," *Journal of Organizational Behavior* (23), 2002, 675-694.
[55] Mathieson, K. "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," *Information Systems Research* 2(3), 1991, 173-191.
[56] Morris, M.G. and Venkatesh, V. "Age Difference in Technology Adoption Decisions: Implications for a Changing Workforce," *Personnel Psychology* 53(2), 2000, 375-403.
[57] Nagin, D. "General Deterrence: A Review of the Empirical Evidence, in Deterrence and in Capacitation: Estimating the Effects of Criminal Sanctions on Crime Rates," A. Blumstein, J. Cohen, and D. Nagin (eds.) *National Academy of Sciences*, Washington, D.C., 1978, 95-139.
[58] Peace, A. G., Galletta, D. F., and Thong, J. Y. L. "Software Piracy in the Workplace: a Model and Empirical Test," *Journal of Management Information Systems* 20(1), 2003, 153-177.
[59] Pomazal, R. J. and Jaccard, J. J. "An Informational Approach to Altruistic Behavior," *Journal of Personality and Social Psychology* (33), 1976, 317-326.
[60] Robin, D. P., Reidenbach, R. E. and Forrest, P. J. "The Perceived Importance of an Ethical Issue as an Influence on the Ethical Decision-Making of Ad Managers," *Journal of Business Research* 35(1), 1996, 17-28.
[61] Sandler, S. F. "Balancing Security & Privacy in the Internet Age," *HR Focus* 79(8), 2002, 13-15.
[62] Schifter, D. B. and Ajzen, I. "Intention, Perceived Control and Weight Loss: an Application of the Theory of Planned Behavior," *Journal of Personality and Social Psychology* 49(3), 1985, 843-851.
[63] Schwarz, S. H. and Tessler, R. C. "A Test of a Model for Reducing Measured Attitude-Behavior Inconsistencies," *Journal of Personality and Social Psychology* 24(2), 1972, 225-236.
[64] Singhapakdi, A. "Perceived Importance of Ethics and Ethical Decisions in Marketing," *Journal of Business Research* (45), 1999, 89-99.
[65] Stanton, J. M. "Reactions to Employee Performance Monitoring: Framework, Review, and Research Directions," *Human Performance* 13(1), 2000, 85-113.
[66] Straub, D. W. and Nance, W. D. "Uncovering and Disciplining Computer Abuse: Organizational Responses and Options," *Information Age* 10(3), 1988, 151-156.
[67] Straub, D. W. "Organizational Structuring of the Computer Security Function," *Computers & Security 7*(2), 1988, 185-192.
[68] Straub, D. W. "Effective IS Security: An Empirical Study," *Information Systems Research* 1(3), 1990, 255-276.
[69] Straub, D. W. and Nance, W. D. "Discovering and Disciplining Computer Abuse in Organizations: A Field Study," *MIS Quarterly* 14(1), 1990, 45-60.
[70] Straub, D. W., and Welke, R. J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* 22(4), 1998, 441-469.
[71] Tabak, F. and Smith, W. P. "Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development," *Employee Responsibilities and Rights Journal* (17), 2005, 173-189.
[72] Taylor, S. and Todd, P. A. "Assessing IT Usage: the Role of Prior Experience," *MIS Quarterly* 19(4), 1995, 561-570.
[73] Thompson, R. L., Higgins, C. A. and Howell, J. M. "Influence of Experience on Personal Computer Utilization: Testing a Conceptual Model," *Journal of Management Information Systems* 11(1), 1994, 167-178.
[74] Tittle, C.R. *Sanctions and Social Deviance: the Question of Deterrence*, Praeger, New York, NY, 1980.
[75] Triandis, H. C. "Values, Attitudes and Interpersonal Behavior," in H.E. Howe (Ed.), *Nebraska Symposium on Motivation*, University of Nebraska Press, Lincoln, NE, 1980, 195-259.
[76] Urbaczewski, A. and Jessup, L. M. "Does Electronic Monitoring of Employee Internet Usage Work?" *Communications of the ACM* 45(1), 2002, 80-83.
[77] Venkatesh, V. and Davis, F.D. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* 46(2), 2000, 186-204.
[78] Vitell, S. J. and Hidalgo, E. R. "The Impact of Corporate Ethical Values and Enforcement of Ethical Codes on the Perceived Importance of Ethics in Business: A Comparison of U.S. and Spanish Managers," *Journal of Business Ethics* (64), 2006, 31-43.
[79] Ward, D. B. "Surfing on Company Time? You Could Lose Your Privacy…and Maybe Your Job," *PC World* 15(11), 1997, 245-253.
[80] Warshaw, P. R. "A New Model for Predicting Behavioral Intentions: an Alternative to Fishbein" *Journal of Marketing Research* 17(2), 1980, 153-172.
[81] Zimmerman, E. "HR Must Know When Employee Monitoring Crosses the Line," *Workforce* (2), 2002, 38-45.
[82] Zweig D, Websteb, J. "Personality as a Moderator of Monitoring Acceptance," *Computers in Human Behavior* 19(4), 2003, 479-493.

APPENDIX

Perceived importance (PIE)

To avoid workplace Internet misuse is extremely important/unimportant.
To avoid workplace Internet misuse is highly significant/insignificant.
To avoid workplace Internet misuse is an issue of considerable concern/no concern.
To avoid workplace Internet misuse is a fundamental/trivial issue.

Punishment severity (PS)

If I were caught committing Internet misuse, I think the punishment would be very high/low.
If I were caught committing Internet misuse, I would/would not be severely punished

Punishment certainty (PC)

If I committed Internet misuse, the probability I would be punished is very low/high.
If I committed Internet misuse, I would/would not probably be punished.

Subject norm about avoiding Internet misuse (SNM)

If I committed Internet misuse, most of the people who are important to me would approve/disapprove.
Most people who are important to me would/would not look down on me if I committed Internet misuse.
No one who is important to me thinks it is/is not okay to commit Internet misuse

Intention of Internet misuse avoidance (IMA)

I may/may not avoid committing Internet misuse in the future
If I had the opportunity, I would /would not avoid committing Internet misuse
I would/would never commit Internet misuse

Dr. Xin Luo is the corresponding author. He can be reached at Luo@mgt.unm.edu.