Industrial Management & Data Systems
Exploring privacy and trust for employee monitoring
Shuchih Ernest Chang Anne Yenching Liu Sungmin Lin

Article information:

Users who downloaded this article also downloaded:

For Authors

If you would like to write for this, or any other Emerald publication, then please use our Emerald for Authors service information about how to choose which publication to write for and submission guidelines are available for all. Please visit www.emeraldinsight.com/authors for more information.

About Emerald www.emeraldinsight.com

Emerald is a global publisher linking research and practice to the benefit of society. The company manages a portfolio of more than 290 journals and over 2,350 books and book series volumes, as well as providing an extensive range of online products and additional customer resources and services.

Emerald is both COUNTER 4 and TRANSFER compliant. The organization is a partner of the Committee on Publication Ethics (COPE) and also works with Portico and the LOCKSS initiative for digital archive preservation.

Exploring privacy and trust for employee monitoring

Shuchih Ernest Chang, Anne Yenching Liu and Sungmin Lin
*Institute of Technology Management, National Chung Hsing Unviersity,
Taichung, Taiwan*

Abstract

Purpose – The purpose of this paper is to evaluate privacy boundaries and explores employees' reactions in employee monitoring.

Design/methodology/approach – The research used the metaphor of boundary turbulence in the Communication Privacy Management (CPM) theory to demonstrate the psychological effect on employees. The model comprised organizational culture, CPM, trust, and employee performance in employee monitoring to further investigated the influence exerted by organizational culture and how employees viewed their trust within the organization when implementing employee monitoring. Variables were measured empirically by administrating questionnaires to full-time employees in organizations that currently practice employee monitoring.

Findings – The findings showed that a control-oriented organizational culture raised communication privacy turbulence in CPM. The communication privacy turbulence in CPM mostly had negative effects on trust in employee monitoring policy, but not on trust in employee monitoring members. Both trust in employee monitoring policy and trust in employee monitoring members had positive effects on employee commitment and compliance to employee monitoring.

Research limitations/implications – This research applied the CPM theory in workplace privacy to explore the relationship between employees' privacy and trust. The results provide insights of why employees feel psychological resistance when they are forced to accept the practice of employee monitoring. In addition, this study explored the relationship between CPM and trust, and offer support and verification to prior studies.

Practical implications – For practitioners, the findings help organizations to improve the performance of their employees and to design a more effective environment for employee monitoring.

Originality/value – A research model was proposed to study the impacts of CPM on employee monitoring, after a broad survey on related researches. The validated model and its corresponding study results can be referenced by organization managers and decision makers to make favorable tactics for achieving their goals of implementing employee monitoring.

Keywords Organizational culture, Compliance, Trust, Commitment,
Communication privacy management, Employee monitoring

Paper type Research paper

1. Introduction

The world has been transformed by the technologies developed throughout the Industrial Age. New technologies, such as e-mail, global positioning system, wireless communication, and telematic units, have changed the conventional organizational setting and reshaped the relationship between an employee and an employer. Due to the fact that employees have a diverse range of work ethics, knowledge, and intentions, employers are inclined to monitor their employees' activities while providing them access to various communication technologies, such as the internet, e-mail, and computers. There is a wide range of software and hardware solutions to monitor employees in the workplace, such as keystroke logs, application and web site usage, detailed file usage, incoming and outgoing chats and

e-mails, packages transmitted over internet connections, windows interacted with internet packet data, desktop screenshots, software installations, and so on (Yerby, 2013). There are numerous reasons why employers believe employee monitoring is necessary for the workplace, and the most advocated three justifications are protecting the organization from liability risks, protecting organizational assets, and ensuring employees' job performance (Smith and Tabak, 2009).

However, employees' viewpoint on employee monitoring may differ from that of their employers. Holland *et al.* (2012) performed a survey on employee attitudes to electronic monitoring and surveillance in an Australian workplace and found that 50 percent of employees were against e-mail monitoring, 60 percent against telephone monitoring, and 56 percent against video surveillance. This suggested that while employers are concerned about monitoring any illegal actions that may jeopardize security systems, employees need to know that their private information will remain private.

Some scholars argue that employees cannot have a "reasonable expectation of privacy" as they are hired to attend company business (Desrochers and Roussos, 2001; Fazekas, 2004). Conversely, the opposing opinion is that "it is not always possible to distinguish clearly which of an individual's activities form part of their professional life and which do not" (European Court of Human Rights, Niemitz vs Germany). Ethical and legal opinions have no impact on the issues regarding privacy in employee monitoring. Thus, this study uses a different perspective to explore how the tension between the employee's right to privacy and the employer's need to safeguard organizational resources affects the result of employee monitoring.

Our research used the metaphor of boundary turbulence in the Communication Privacy Management (CPM) theory to demonstrate the psychological effect on employees. The controversial tension between managing private and publicly shared information is described by Petronio (2004) as CPM theory. An information boundary is created when individuals filter what information to disclose and with whom they share information (Petronio, 1991). Organizations socialize their employees to accept the information boundary of employee monitoring through everyday interactions and conversations. Employees develop their understanding and use of employee monitoring and responses to it using the advocacy of security policy, instructions given by managers, restrictions from work contracts, peer pressure among coworkers, and so on. However, disagreements regarding the ownership of private information occur when employees confront the violation of information boundaries. CPM is a practical theory that evaluates privacy boundaries and explores employees' reactions to employee monitoring (Allen *et al.*, 2007).

The research further investigated the influence exerted by organizational culture because the fit between it and employee monitoring is undetermined. Hagberg and Heifetz (1997) asserted that organizational culture is like "the operating system" to guide employees' thoughts, actions, and feelings. By incorporating the element of organizational culture in this research, the influence of how organizations socialize employees into the concept of employee monitoring can be better understood and explored. Also, trust is an important indicator that reflects the relationship between employees and employers. The action of employers' breaching employees' privacy influences the level of trust in the workplace. Trust is also a stimulator of voluntary compliance and commitment to organizational authority and rules (De Cremer and Tyler, 2007; Morrow *et al.*, 2012). As a result, employees' compliance and commitment to the practice of employee monitoring were determined.

2. Literature review
2.1 CPM theory
The CPM theory explores information disclosure among individuals across a privacy boundary. The theory uses a metaphor to explain the decision by drawing a boundary line, or limitation, between individuals when disclosing information. Subconsciously, individuals often make decisions to disclose information or to maintain privacy when communicating with each other. Dialectical tensions are often experienced in these relationships (Baxter and Montgomery, 1996). This dialectic tension, as interpreted in the CPM theory, is regarded as the tension between revealing and concealing private information. Consequently, an information boundary is created when individuals filter what information to disclose and with whom they share information (Petronio, 1991).

The CPM theory through privacy boundary provides a framework in understanding "privacy and confidentiality work as a tension" and "the concomitant needs for privacy and granting access function to influence the choices people make to reveal or conceal" (Petronio and Reierson, 2009). There are five core principles in the CPM theory (Petronio, 2002). First, individuals believe that they own their private information. The ownership of information defines the boundary of information flow. Second, individuals assume that they have a right to control their private information. They can decide what and to whom their private information is disclosed. Third, individuals depend on privacy rules control their information flow. The privacy rules are the reasons observed in a pattern when individuals make choices conceal or to reveal private information. There are five factors influencing the way individuals to develop their private rules: culture, gender, motivation, context, and risk-benefit ratios. Fourth, private information is co-owned when the private information is exposed to the other party. This co-ownership cannot be reversed; thus, careful consideration must be taken before revealing private information. Last, co-owners of private information need to negotiate collectively on mutual agreeable privacy rules for the third-party dissemination. They have to negotiate who decides revelation of the information (boundary ownership), whom the information is revealed to (boundary linkage), and how much information can flow (boundary permeability). Subsequently, boundary turbulence may result when co-owners of private information do not effectively negotiate agreeable privacy rules. Boundary turbulence is a metaphor explaining "disruption in the way that co-owners control and regulate the flow of private information to third parties" (Petronio and Reierson, 2009).

The CPM theory has been applied in research into the disclosure of private information, mostly in family relationships. The work of Stanton and Stam (2003) first integrated the application of the CPM theory in the workplace. These researchers viewed information about employees as a valuable organizational resource that can be retrieved through various technological means within the organization. Stanton and Stam described that employees may consider revealing information in exchange for reward or sanction in organizations. Allen *et al.* (2007) further explored boundary ownership and turbulence in a wide range of organizations using surveillance technologies. In addition, Snyder (2010) investigated e-mail privacy in the workplace using boundary regulation perspective. These studies contribute to understanding the influence of implementing workplace surveillance, based on information disclosure and boundary turbulence. By including information disclosure and boundary turbulence, this study modifies the CPM theory to observe the impact on employee monitoring within the organization.

2.2 Privacy boundary turbulence in the workplace
Private information about employees involve various business activities, such as communication via phone and e-mail, browsing web sites to maintain relationships, and many other actions (Fairweather, 1999). Organizations claim the ownership of employee information in the workplace, yet employees may disagree with the organization's ownership of their privacy (Lee and Kleiner, 2003; Townsend and Bennett, 2003). Therefore, boundary turbulence arises when both employers and employees contest for boundary ownership over private information about employees. Privacy boundary turbulence occurs when implementing employee monitoring in a workplace.

To illustrate the CPM theory, Petronio (2002) identifies three boundary categories that lead to turbulence. First, fuzzy boundaries occur when the information boundary is vague and unclear. Information owners may come into conflict with each other. In the workplace, the fact that employers implement employee monitoring may cause concern about the organizational infringement of employees' privacy. Second, mistakes involving the disclosure of private information to an uninvited third party may also lead to turbulence. Employees may feel disappointed in the employee monitoring process when they are confronted with the inability to maintain privacy. Third, intentional breaches of boundary ownership also lead to boundary turbulence. Excessive employee monitoring causes individuals to feel distrust and a loss of control (Cooper and Hecker, 2012).

2.3 Trust
Boundary turbulence in CPM often leads to negative and unpleasant feelings about information sharing. One of the negative feelings is not being able to trust. Trust is an individual's belief or an expectation of others' ethical behaviors under various influential factors, such as subjective norms, risk, confidence, and security (Mayer *et al.*, 1995; Grandison and Sloman, 2000; Bahtiyar and Çağlayan, 2012). Researchers use these influential factors to determine the tendency of trust (McKnight *et al.*, 2004; Riegelsberger *et al.*, 2005) and construct trust as a central aspect in all types of relationships (Gefen *et al.*, 2003).

Studies have shown that risk is also associated with trust in relationships (Beldad *et al.*, 2011; Laurence *et al.*, 2013). The feeling of vulnerability and/or uncertainty about an outcome relates to risks in trust (Doney *et al.*, 1998). Thus, our study uses the disclosure of privacy as the risk factor in the working relationship. Employees' behaviors are observed and recorded with the help of technologies designed to monitor employees in the workplace. However, unauthorized third-party access to personal data in organizational electronic databases poses risk in workplace trust relationships. Meanwhile, how the actions of employers breaching employees' privacy influence trust in the workplace is stressed in the research.

Spying on employees' privacy has significantly damaged the trust relationship. The implementation of spying technologies can be described as a manipulation or an outlook of a trusted computing base, which is viewed as "a bridge between social needs and security solutions to cope with trust management vulnerabilities for distributed networks" (Sun *et al.*, 2008; Bahtiyar and Çağlayan, 2012). However, researchers highlight that justifying the system and policy to manipulate trust is not as necessary as experimenting in practice (Gollmann, 2006). Therefore, understanding how the monitoring process can attribute the levels of trust among employees is important.

3. Research model and hypotheses

Figure 1 shows the research model. Variables comprise organizational culture, CPM, trust, and employee performance in employee monitoring.

3.1 Antecedents of CPM: organizational culture

Individuals tend to use their own privacy rules to guide the disclosure of private information when privacy boundary turbulence occurs. In the workplace, employers seek to socialize employees into accepting the organization's privacy rules through policies and training practices (Petronio, 2002). On one hand, policies can be used as coercive and formalized practices for changing individuals' expectations regarding privacy. On the other hand, culture is not so formalized and is still an influential factor in forming privacy rules (Petronio, 2002). Milberg *et al.* (2000) showed a positive relationship between cultural values, corporate privacy policies, and government regulations. For the workplace policy, Allen *et al.* (2007) and Schumacher (2010) found that cultural paradigm is linked to the existing practices in organizations. Also, Hagberg and Heifetz (1997) asserted that organizational culture is like "the operating system" that guides employees' thoughts, actions, and feelings. Employees are assimilated into monitoring practices through organizational culture. Hence, organizational culture is related to formulating the privacy rules between employers and employees in the workplace.

Moreover, scholars have attempted to relate organizational culture to the perspective of managerial administration. Quinn and Spreitzer (1991) developed a typology based on two categorizing dimensions, including the internal/external orientation and the flexibility/control orientation, and identified four cultural archetypes: group culture, developmental culture, hierarchical culture, and rational culture. Boggs (2004) followed up by applying organizational culture to total quality management. Similarly, organizational culture is classified according to the four culture traits, including mission, consistency, adaptability, and involvement in evaluating effectiveness (Denison *et al.*, 2004). Moreover, Chang and Lin (2007) categorized the characteristics of organizational culture into four constructs, including cooperativeness, innovativeness, consistency, and effectiveness. Chang and Lin's
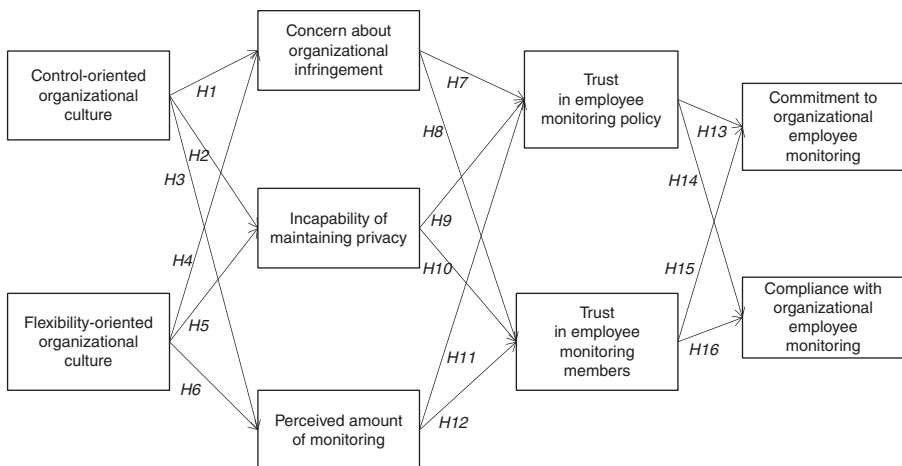

Figure 1.
Proposed model

Downloaded by TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES At 01:51 10 November 2016 (PT)

research used two groups of dimensions, including the internal/external orientation vs the flexibility/control orientation, to categorize organizational culture. As employee monitoring is practiced within an organizational system, internal/external orientation is removed in our research. This research simplifies to a single category, the flexibility/control orientation, to study the effect of organizational culture on CPM in employee monitoring. Flexibility-oriented organizational culture contains characteristics of cooperativeness and innovativeness; control-oriented organizational culture contains characteristics of consistency and effectiveness.

Our research uses the scaled concern about organizational infringement, incapability of maintaining privacy, and perceived amount of monitoring instruments to assess boundary turbulence in workplace employee monitoring:

H1. Control-oriented organizational culture significantly relates to employees' concern about organizational infringement.

H2. Control-oriented organizational culture significantly relates to employees' incapability of maintaining privacy.

H3. Control-oriented organizational culture significantly relates to employees' perceived amount of monitoring.

H4. Flexibility-oriented organizational culture significantly relates to employees' concern about organizational infringement.

H5. Flexibility-oriented organizational culture significantly relates to employees' incapability of maintaining privacy.

H6. Flexibility-oriented organizational culture significantly relates to employees' perceived amount of monitoring.

3.2 CPM and trust in employee monitoring systems

The CPM theory emphasizes individual autonomy in relationships while maintaining connections with others (Petronio *et al.*, 1997). Individuals feel the need to manage the opening and closing of information boundaries to establish and maintain control in the relationship (Petronio, 2002). Revealing private information might strengthen relationships with others; however, when the co-owners of private information break the mutually agreeable privacy rules, boundary turbulence occurs and negative feelings may arise in individuals, such as distrust, unfairness, exhaustion, and so on. The struggles of individuals in maintaining their boundaries are similar to a concept called the fundamental social dilemma: "members of groups, organizations, and societies face a dilemma when deciding whether to invest in social collectives" (Lind, 2001; Kramer, 1996; van Dijke and Verboon, 2010). In the situation of social dilemma, individual contribution and involvement in the social collectives may lead to better outcomes, such as improved self-identity and a sense of belongingness; on the other hand, individuals also risk exposure to possible exploitation and identity damage from authorities who abuse their power (van Dijke and Verboon, 2010). In response to the social dilemma, the CPM theory reinstates that boundary turbulence can quickly destroy the trust between individuals built up over time. Thus, boundary turbulence is considered to have a negative impact on the trust between employees and employers.

Employees distrust the organization when the organizational employee monitoring extends beyond the employees' expectations. This difference in the perception of privacy on monitoring the work environment leads to a distrusting relationship between employees and the organization.

Trust management is "a unified approach to specify and interpret security policies, credentials, and relationships" (Blaze *et al.*, 2003), and it values policy administration more than checking an access control list stored with a protected resource (Gollmann, 2006). Employee monitoring may have various designs to control access and keep track of records, and it needs a policy to enforce the implementation of monitoring. The rationale behind monitoring policies relates to the trust of personnel and technologies, and it also relates to other factors, such as the need-to-know and contractual agreements among cooperating entities (Gollmann, 2006). The possibility of exposing organizational infringements and breaches of privacy and the use of overwhelming monitoring poses an indication of distrust. With excessive policies and monitoring mechanisms, the existence of distrust is obvious. Thus, our study uses trust in employee monitoring members and trust in employee monitoring policy to distinguish relationships between organizational members and authorities:

H7. Employees' concern about organizational infringement significantly relates to trust in employee monitoring policy.

H8. Employees' concern about organizational infringement significantly relates to trust in employee monitoring members.

H9. Employees' incapability of maintaining privacy significantly relates to trust in employee monitoring policy.

H10. Employees' incapability of maintaining privacy significantly relates to trust in employee monitoring members.

H11. Employees' perceived amount of monitoring significantly relates to trust in employee monitoring policy.

H12. Employees' perceived amount of monitoring significantly relates to trust in employee monitoring members.

3.3 Employee performancee: commitment and compliance
Employees are more likely to align their values and expectations with the organization's goal under a trustworthy relationship. Trust reduces conflict and increases cooperation among individuals (Anderson and Narus, 1990). Cooperation is a general concept of compliance, which is measured by cooperative adoption. Cooperative adaptation involves employees complying with the requests of organizational conformity (Hausman and Johnston, 2010). Compliance with employee monitoring is also a form of cooperative adaptation.

The study of De Cremer and Tyler (2007) showed that trust in authorities makes individuals cooperate with them submissively. Trust stimulates voluntary compliance with organizational authority with respect to organizational policies and rules. Yang *et al.* (2009) showed that employee compliance with guidance and instructions demonstrates "a way of reinforcing positive interpersonal relations" and further

encourages employees to help supervisors and supervisor-oriented improvement in the workplace (Colquitt and Greenberg, 2003). Employees are more likely to comply with requests and suggestions made by the organization if they trust the organization. Otherwise, if there is distrust, employees may be reluctant to cooperate.

Organizational commitment encourages employees to identify with an organization and emphasizes the bond between the employee and the organization (Morrow *et al.*, 2012). Studies have shown that employees with low organizational commitment are likely to engage in behaviors that are counterproductive to the organization (e.g. theft, sabotage, or aggregation) (Luchak and Gellatly, 2007). The purpose of implementing employee monitoring is to increase employee productivity and involvement at work; as a result, understanding the influence of employee monitoring on employee commitment within the organization is important.

Trust is discussed in terms of employee commitment by many researchers. Commitment entails vulnerability, and thus, individuals need to careful when evaluating the trustworthiness of partners with whom they share commitments (Hausman and Johnston, 2010). Similarly, employees are likely to commit to the organization if they trust in the organization's ability to guide and facilitate employees' work efforts. In contrast to employee commitment, organizational commitment is significantly required to obtain and maintain trust during employee monitoring in return for employees' work commitments:

H13. Trust in employee monitoring policy significantly relates to employees' commitment to organizations' employee monitoring.

H14. Trust in employee monitoring policy significantly relates to employees' compliance with organizations' employee monitoring.

H15. Trust in employee monitoring members significantly relates to employees' commitment to organizations' employee monitoring.

H16. Trust in employee monitoring members significantly relates to employees' compliance with organizations' employee monitoring.

4. Research methods and results
4.1 Data collection
Empirical data were collected through a questionnaire survey instrument, which comprised two sections. The first section comprised demographic variables. The second section was related to items under the constructs of the model. Items for organizational culture were developed to include different cultural characteristics (Quinn and Spreitzer, 1991; Denison *et al.*, 2004; Boggs, 2004). Items for CPM were borrowed from Eddy *et al.*'s (1999) measure of perceived privacy invasion, Botan's (1996) measure of workplace privacy, and Snyder's (2010) revised version on the measurement of e-mail privacy. Items for trust were taken from Hsu *et al.*'s (2011) measurement of trust in systems and members. Ifinedo's (2011) measurement of compliance and Ifinedo's (2014) measurement of commitment were also adopted in and adjusted for this study.

Each questionnaire item was measured on a seven-point Likert scale, ranging from "strongly disagree" (extremely unimportant) to "strongly agree" (extremely important). To ensure that the questionnaire items could be understood and provide valid

measurements, a small number of surveys were distributed as a pre-test. The pre-test adopted the exploratory factor analysis to analyze the collected data and to ensure all items were appropriately grouped into expected common (latent) factors. Based on the comments received from the pre-test, modifications were made to the questionnaire items to improve readability before the formal surveys were sent.

This study was conducted in Taiwan because researchers demographically observed that the ratio of computers per employee is 73 percent in Taiwan (Taiwan National Statistics, 2012) – the highest among the East Asian countries. In addition, Taiwan passed the "Personal Information Protection Act" in 2012, which is applicable to all commercial activities, including conventional businesses in all industries, that involve personal information. Furthermore, work privacy issues have been researched in Taiwan due to the "westernized" business environment and tight relationships in the Pacific Rim market (Taylor, 2013). Therefore, this study was significant in investigating the effect of monitoring on employees characterized by high usage of information technology and high levels of privacy awareness.

The surveys were distributed and collected in the first quarter of 2014. Surveys were distributed using the snowballing sampling technique. The participants were full-time employees in organizations that currently practice employee monitoring in Taiwan. Survey collection began by recruiting ten students in the research team. These students were instructed to ask individuals who were full-time employees and were aware of their organizations' current employee monitoring practices. These participants were then asked to refer other individuals fitting the same criteria. The survey period ended when the sample size reached 90, which was at the end of the first quarter of 2014.

4.2 Sample characteristics

A total of 90 surveys were collected, of which 81 were valid. The number of male respondents was 48 and that of female respondents was 33. Respondents were from organizations in various industries (information technology 32.1 percent, manufacturing 25.9, service 19.8 percent, legal 8.6 percent, education 2.5 percent, financial 4.9 percent, and miscellaneous 6.2 percent) and represented a variety of job categories (R&D 46.9 percent, legal 6.2 percent, accounting 11.1 percent, sales 16.1 percent, administration 7.4 percent, and miscellaneous 12.3 percent). Company sizes were below 100 employees ($n = 22$, 27.2 percent), above 101 and below 1,000 employees ($n = 34$, 41.9 percent), and above 1001 employees ($n = 25$, 30.9 percent). Most respondents ($n = 72$, 88.9 percent) were not in managerial positions. The analysis of the frequency distribution by age showed that most of the respondents ($n = 39$, 48.1 percent) were between 31 and 40 years, 33.3 percent ($n = 27$) between 20 and 30 years, and 18.6 percent ($n = 15$) above 41 years. Respondents represented a range in tenure with their current organization, including less than five years ($n = 49$, 60.5 percent), six to ten years ($n = 22$, 27.2 percent), 11-15 years ($n = 6$, 7.4 percent), and more than 16 years ($n = 4$, 4.9 percent).

4.3 Data analysis

Data analysis followed the partial least squares method of structural equation modeling (PLS-SEM). The PLS-SEM method was used to examine the reliability of individual items, internal consistency between items and the model's convergent, and discriminate validity. First, the model was assessed for reliability of individual item that is correlated to the items with their respective latent variables. Items with

a loading below 0.7 are recommended to be dropped off by many researchers (Fornell and Larcker, 1981; Hulland, 1999). In this study, five indicators were removed from the initial model because they exhibited loadings below 0.70. The rest of items were retained as they demonstrated reliability with satisfaction.

Second, convergent validity of the measured constructs was assessed by Cronbach's α, composite reliability score and average variance extracted (AVE). Cronbach's α is the coefficient of reliability and is used to measure the unidimensionality of a single one-dimensional latent construct. Composite reliability score is similar to Cronbach's α. The dimensional latent construct is considered as unidimensional when its Cronbach's α value and composite reliability score are larger than 0.7 (Tenenhaus et al., 2005). Further, AVE was used to measure the convergent validity of the latent variables and suggested being higher than 0.5. All AVE scores in this study ranged from 0.577 to 0.975, passing the threshold value of 0.5. As shown in Table I, the statistics for assessment satisfied the reliability standards.

To assess the discriminant validity, the square root of the AVE measure on each construct must exceed the estimated correlations shared between the construct and other constructs in the model (Fornell and Larcker, 1981). As shown in Table II, the discriminant validity for the constructs used in our study was acceptable since the

	AVE	Composite reliability	Cronbachs α
Comm	0.918855	0.985492	0.98231
COI	0.763909	0.976653	0.973656
Comp	0.816876	0.956685	0.941012
Control	0.603934	0.923913	0.910429
Flexibility	0.716382	0.96798	0.963904
IMP	0.975458	0.99375	0.991619
PAM	0.808927	0.962073	0.952517
TEMP	0.80121	0.941573	0.917234
TEMM	0.811727	0.945162	0.923368

Notes: Comm, commitment to organizational employee monitoring; COI, concern about organizational infringement; Comp, compliance to organizational employee monitoring; Control, control-oriented organizational culture; Flexibility, flexibility-oriented organizational culture; IMP, incapability of maintaining privacy; PAM, perceived amount of monitoring; TEMP, trust in employee monitoring policy; TEMM, trust in employee monitoring members

Table I. Composite reliabilities, Cronbach's α values and average variance extracted

	Comm	COI	Comp	Control	Flexibility	IMP	PAM	TEMP	TEMM
Comm	0.959								
COI	−0.304	0.874							
Comp	0.847	−0.301	0.904						
Control	0.012	0.450	0.080	0.777					
Flexibility	0.109	−0.374	0.125	−0.278	0.846				
IMP	−0.400	0.699	−0.354	0.369	−0.183	0.988			
PAM	−0.500	0.598	−0.485	0.327	−0.075	0.768	0.899		
TEMP	0.575	−0.479	0.594	−0.235	0.413	−0.364	−0.500	0.895	
TEMM	0.587	−0.537	0.595	−0.367	0.361	−0.550	−0.542	0.599	0.901

Table II. Inter-construct correlations and square root of AVE measure

square root of AVE on each construct was greater than the correlations of the construct with other constructs.

The inner model which specified the relationships between latent variables was then estimated. The path coefficients for the endogenous latent variables and R^2 statistics were derived. The inner model results are presented in Table III.

4.4 Empirical results

The empirical results confirm that control-oriented organizational culture significantly and positively affected employees' concern about organizational infringement ($\beta = 0.375435$, $p = 0.000337$), incapability of maintaining privacy ($\beta = 0.345114$, $p = 0.000478$) and perceived amount of monitoring ($\beta = 0.332306$, $p = 0.002488$). Flexibility-oriented organizational culture as well negatively affected employees' concern about organizational infringement, incapability of maintaining privacy, and perceived amount of monitoring. Yet, the result was only significant in concern about organizational infringement ($\beta = -0.269849$, $p = 0.004988$). Concern about organizational infringement significantly and negatively affected employees' trust in employee monitoring policy ($\beta = -0.382334$, $p = 0.000846$) and trust in employee monitoring members ($\beta = -0.267447$, $p = 0.007511$). Incapability of maintaining privacy did not significantly affect employees' trust in employee monitoring policy ($\beta = 0.274019$, $p = 0.108733$) and trust in employee monitoring members ($\beta = -0.169619$, $p = 0.241691$). Perceived amount of monitoring significantly and negatively affected employees' trust in employee monitoring policy ($\beta = -0.481956$, $p = 0.003169$) but not significantly in trust in employee monitoring members ($\beta = -0.251733$, $p = 0.111442$). Trust in employee monitoring policy significantly and positively affected employees' commitment ($\beta = 0.348448$, $p < 0.0001$) and compliance ($\beta = 0.370951$, $p = 0.000281$). Trust in employee monitoring policy significantly and positively affected employees' commitment ($\beta = 0.378402$, $p < 0.0001$) and compliance ($\beta = 0.372654$, $p < 0.0001$). Overall, *H1-H4, H7, H8, H11, H13-H16* postulated in this

	Hypothesis	Path coefficient	p-value	Inference
Control→COI	*H1*	0.375***	0.0003	Supported
Control→IMP	*H2*	0.345***	0.0005	Supported
Control→PAM	*H3*	0.332**	0.0025	Supported
Flexibility→COI	*H4*	−0.270**	0.0050	Supported
Flexibility→IMP	*H5*	−0.087	0.3587	Not supported
Flexibility→PAM	*H6*	0.018	0.8694	Not supported
COI→TEMP	*H7*	−0.382***	0.0008	Supported
COI→TEMM	*H8*	−0.267**	0.0075	Supported
IMP→TEMP	*H9*	0.274	0.1087	Not supported
IMP→TEMM	*H10*	−0.170	0.2417	Not supported
PAM→TEMP	*H11*	−0.482**	0.0032	Supported
PAM→TEMM	*H12*	−0.252	0.1114	Not supported
TEMP→Comm	*H13*	0.348***	0.0000	Supported
TEMP→Comp	*H14*	0.371***	0.0003	Supported
TEMM→Comm	*H15*	0.378***	0.0000	Supported
TEMM→Comp	*H16*	0.373***	0.0000	Supported

Notes: **,***Significance at $p < 0.01$, < 0.001, respectively

Table III.
Results of structural model

study were supported by the empirical results, though the other five hypotheses (*H5*, *H6*, *H9*, *H10*, and *H12*) were not supported.

5. Discussion
The purpose of this study was to develop a thorough understanding of employees' reactions toward employee monitoring while also exploring organizational culture, CPM, trust, commitment, and compliance.

5.1 Control-oriented organizational culture impeded CPM in employee monitoring
The results showed that control-oriented organizational culture was associated with boundary turbulence in CPM, whereas flexibility-oriented organizational culture was associated with less boundary turbulence. The inference of cultural difference can be drawn to explain that institutions with flexibility-oriented organizational culture emphasize empowerment, teamwork, creativity, information sharing, and dynamism; consequently, employees working in such flexibly oriented environments receive fewer restrictions and less monitoring.

As in previous research findings, control-oriented organizational culture supports the implementation of organizational practices; moreover, it facilitated the effective practice of information security in organizations (Chang and Lin, 2007). However, implementations aimed to control and coerce the work environment that generated poor employee communications. Our study showed that employees' psychological concerns about employee monitoring existed when both employees and employers did not reach a privacy boundary agreement. Allen *et al.* (2007) performed a survey on employees under employee monitoring and found that privacy boundaries were generally set by organizations. Mitrou and Karyda (2006) described this employment situation as asymmetric power. Employees were socialized using employee monitoring practices and organizational policies. Petronio (2002) suggested that employees often exchanged privacy control for a job and did not challenge organizations' employee monitoring activities. Therefore, employees' psychological concerns existed even when employee monitoring was effectively practiced.

Boundary turbulence was more severe in control-oriented organizational cultures than flexibility-oriented organizational culture. Control-oriented organizational culture emphasized a consistent and effective environment that strictly required employees to follow the organization's instructions, guidelines, and regulations of employee monitoring. This one-way communication through imposing procedures and rules to govern what employees do was ineffective in privacy boundary negotiations. Negative emotions accompanied forced acquiescence, as explained by psychological processes and behavior outcomes (Haws *et al.*, 2010). Flexibility-oriented organizational culture motivated through the trust, sharing, achievement, and perceptions of positive consequences. The result of our study showed that employees were less concerned about the privacy infringement of employee monitoring in a flexibility-oriented organizational culture. From the employees' perspective, a flexible organizational culture enhanced employees' power and motivated negotiated privacy rights and better CPM in employee monitoring.

5.2 Boundary turbulence in CPM results in the distrust of employee monitoring
This study tested the hypothesis of how boundary turbulence in CPM affects trust relationships between employees and employers. The results partially supported

the hypothesis. Trust in employee monitoring policy was affected by concern about organizational infringement and perceived amount of monitoring; on the other hand, trust in employee monitoring members was affected mainly by concern about organizational infringement. The negative relationship between concern about organizational infringement and trust is consistent to prior research that showed concern about organizational infringement to have a negative impact on trust (Wu *et al.*, 2012; Kim and Kim, 2011; Eastlick *et al.*, 2006; Taddei and Contena, 2013). Concern about organizational infringement is another form of risk perception. Privacy infringements in employee monitoring include allowing excessive monitoring in the workplace or an insecure design of policy and also include privacy transgressions by coworkers, security personnel, or managers. Our results showed that employees with more concern about organizational infringement tended to negatively affect trust in employee monitoring policy and trust in employee monitoring members. Previous studies also demonstrated concerns that infringements negatively affect work relationships (Snyder, 2010). A workplace environment characterized by distrust emerges when employees are concerned about an organization infringing their privacy. Thus, concern about organizational infringement is the main factor affecting trust in employee monitoring.

Trust relationships were less affected by employees' incapability of maintaining privacy and perceived amount of monitoring. Incapability of maintaining privacy showed no effect on trust relationships, and perceived amount of monitoring only affected trust in employee monitoring policy. Previous studies also demonstrated the limited effect of incapability of maintaining privacy and perceived amount of monitoring on work relationships (Snyder, 2010). Employees were uncomfortable with the direction of employee monitoring policy when they perceived an excessive amount of employee monitoring. Scholars showed that the amount of monitoring and unnecessary monitoring lead to negative perceptions of organizational policy (Botan, 1996; Cooper and Hecker, 2012). Employees questioned the purpose of organizational policies regarding excessive monitoring when the amount of monitoring was extended beyond their awareness.

5.3 Trust facilitated better employee performance in employee monitoring
Trust in employee monitoring policy and trust in employee monitoring members had significant and positive effects on employee commitment and compliance to organizations' employee monitoring, which harmonizes with previous studies in which employees commit to their organization if they are confident in and trust the organization's ability to guide and facilitate employees' work efforts (Hon and Lu, 2010), thus developing further long-term commitment to the organization (Utami *et al.*, 2014). In addition, increasing trust in a policy elevates the level of compliance (van Dijke and Verboon, 2010; Kogler *et al.*, 2013). Thus, when employees trust in the policies they are more likely to commit and comply with their organization's requirements. In addition, trust in employee monitoring showed a significant and positive relationship with employee commitment and compliance. Employees who feel secure and trust their partnership in the system tend to commit and comply with their organization.

6. Implications and limitations
The findings of the study provide several implications for both academic and pragmatic practitioners. For practitioners, the findings help organizations to improve

the performance of their employees and to design a more effective environment for employee monitoring. Employees feel limited CPM in control-oriented organizational culture. Organizations could avoid excessive control-oriented organizational culture for better a negotiation of the privacy boundary between employees and employers. Among communication turbulence in negotiating privacy with employees, concern about organizational infringement is the main factor influencing trust relationships. Thus, a good CPM generates trust in work relationships and encourages a strong motivation and intention of employee commitment and compliance. The aforementioned factors can also help organizations achieve higher employee performance.

Moreover, the findings provide theoretical contributions to academic research relating to the implementation of employee monitoring. Employee monitoring is practiced in organizations to help employers protect organizational assets and security systems. Previous research focussed on employee monitoring and its potential outcomes (D'Urso, 2006); however, further exploration on how to successfully implement employee monitoring is necessary. The CPM theory focussed on privacy boundary negotiation among parties, and the vast majority of previous research on CPM relates to online vendors in an attempt to improve their visitors' trust. However, CPM can also be applied in workplace privacy to explore the relationship between employees' privacy and trust. This study adopts the CPM theory to investigate employees' psychological response to privacy boundary in employee monitoring.

First, the exploration of what kind of organizational environment in fostering better privacy communication and employee monitoring in a workplace is very limited. With the empirical findings of this research provided, control-oriented organizational culture connotes negative association with CPM. Thus, the results provide insights of why employees feel psychological resistance when they are forced to accept the practice of employee monitoring. The role of organizational culture is important in preventing privacy boundary turbulence.

In addition, this study explored the relationship between CPM and trust. Our research further confirms privacy boundary turbulence to be negatively associated with trust relationships in a workplace. The result is consistent with previous studies showing the strong association between the perception of privacy boundaries and relationships (Snyder, 2010). Our results found that concern about organizational infringement is the main factor affecting trust in employee monitoring, whereas incapability of maintaining privacy and perceived amount of monitoring have fewer effects on trust.

Finally, the findings support the theory of trust relating to commitment and compliance. Numerous studies have demonstrated the positive relationship between trust and employee commitment and compliance (Utami *et al.*, 2014; van Dijke and Verboon, 2010; Kogler *et al.*, 2013). Our findings offer support and verification to prior studies. Thus, employee performance in employee monitoring is related to the trustworthiness of organizations.

The findings of this study are insightful, but the research still has some limitations. The sample size in the research is made of 81 respondents. Generally, a larger sample size provides more significant results. PLS-SEM was used in the research to alleviate the problem with a small sized sample. This research also collected data from employees from organizations with different firm sizes and industries and treated these employees as a homogenous group. Variations in firm size and industries may lead to a different perception of employee monitoring. Employee traits, such as gender,

work experience, and job category, may also lead to different privacy expectations. Future study may differentiate the effects of demographic variance on employee monitoring. Furthermore, the influence of the legal environment through organizational policy, regulations, and legal contracts is a possible direction for future study.

7. Conclusions

This study explored how employee monitoring affects employees' attitudes toward their organizations and employee performance under the practice of monitoring. A research model was proposed to study the importance of relationships among organizational culture, CPM, trust, commitment, and compliance. The findings showed that a control-oriented organizational culture raised communication privacy turbulence in CPM; the communication privacy turbulence in CPM mostly had negative effects on trust in employee monitoring policy, but not on trust in employee monitoring members; and both trust in employee monitoring policy and trust in employee monitoring members had positive effects on employee commitment and compliance to employee monitoring. The validated research model and corresponding findings can be referenced by managers and employees for enhancing employee performance through workplace monitoring.

References

Allen, M.W., Walker, K.L., Coopman, S.J. and Hart, J.L. (2007), "Workplace surveillance and managing privacy boundaries", *Management Communication Quarterly*, Vol. 21 No. 2, pp. 172-200.

Anderson, J.C. and Narus, J.A. (1990), "A model of distributor firm and manufacturer firm working partnerships", *Journal of Marketing*, Vol. 54 No. 1, pp. 42-58.

Bahtiyar, S. and Çağlayan, M.U. (2012), "Extracting trust information from security system of a service", *Journal of Network and Computer Applications*, Vol. 35 No. 1, pp. 480-490.

Baxter, L.A. and Montgomery, B.M. (1996), *Relating: Dialogues and Dialectics*, Guilford Press, New York, NY.

Beldad, A., de Jong, M. and Steehouder, M. (2011), "I trust not therefore it must be risky: determinants of the perceived risks of disclosing personal data for e-government transactions", *Computers in Human Behavior*, Vol. 27 No. 6, pp. 2233-2242

Blaze, M., Ioannidis, J. and Keromytis, A.D. (2003), "Experience with the keynote trust management system: applications and future directions", *Lecture Notes in Computer Science*, Vol. 2692, pp. 284-300.

Boggs, W.B. (2004), "TQM and organizational culture: a case study", *The Quality Management Journal*, Vol. 11 No. 2, pp. 42-52.

Botan, C. (1996), "Communication work and electronic surveillance: a model for predicting panoptic effects", *Communication Monographs*, Vol. 63 No. 4, pp. 293-313.

Chang, S.E. and Lin, C.S. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems*, Vol. 107 No. 3, pp. 438-458.

Colquitt, J.A. and Greenberg, J. (2003), "Organizational justice: a fair assessment of the state of the literature", in Greenberg, J. (Ed.), *Organizational Behaivor: The STATE of the Literature*, Lawrence Erlbaum Associates, Mahwah, NJ, pp. 165-210.

Cooper, B. and Hecker, R. (2012), *The Electronic Workplace Survey: Analysis of the First National Survey on Employee Attitudes to Electronic Monitoring and Surveillance in the Australian Workplace*, Monash University, Melbourne, available at: www.buseco.monash.edu.au/ mgt/ news/documents/electronic-report.pdf (accessed Apirl 2, 2014).

D'Urso, S. (2006), "Who's watching us at work? Toward a structural-perceptual model of electronic monitoring and surveillance in organizations", *Communication Theory*, Vol. 16 No. 3, pp. 281-303.

De Cremer, D. and Tyler, T.R. (2007), "The effects of trust in authority and procedural fairness on cooperation", *Journal of Applied Psychology*, Vol. 92 No. 3, pp. 639-649.

Denison, D.R., Haaland, S. and Goelzer, P. (2004), "Corporate culture and organizational effectiveness: is Asia different from the rest of the world?", *Organizational Dynamics*, Vol. 33 No. 1, pp. 98-109.

Desprochers, S. and Roussos, A. (2001), "The jurisprudence of surveillance: a critical look at the laws of intimacy", *Lex Electronica*, Vol. 6 No. 2, pp. 1-12, available at: www.lex-electronica. org/en/articles/v6-2/desroussos.htm (accessed August 10, 2014)

Doney, P.M., Cannon, J.P. and Mullen, M.R. (1998), "Understanding the influence of national culture on the development of trust", *Academy of Management Review*, Vol. 23 No. 3, pp. 601-620.

Eastlick, M.A., Lotz, S.L. and Warrington, P. (2006), "Understanding online B-to-C relationships: an integrated model of privacy concerns, trust, and commitment", *Journal of Business Research*, Vol. 59 No. 8, pp. 877-886.

Eddy, E.R., Stone, D.L. and Stone-Romero, E.E. (1999), "The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice perspectives", *Personnel Psychology*, Vol. 52 No. 2, pp. 335-358.

Fairweather, N.B. (1999), "Surveillance in employment – the case of teleworking", *Journal of Business Ethics*, Vol. 22 No. 2, pp. 39-49.

Fazekas, P., (2004), "1984 is still fiction: electronic monitoring in the workplace and US privacy", *Duke Law & Technology Review*, Vol. 3 No. 15, pp. 1-16, available at: http://scholarship.law. duke.edu/cgi/viewcontent.cgi?article=1119&context=dltr (accessed August 10, 2014).

Fornell, C. and Larcker, D.F. (1981), "Evaluating structural equation models with unobservable variables and measurement error", *Journal of Marketing Research*, Vol. 18 No. 1, pp. 39-50.

Gefen, D., Karahanna, E. and Straub, D.W. (2003), "Trust and TAM in online shopping: an integrated model", *MIS Quarterly*, Vol. 27 No. 1, pp. 51-90.

Gollmann, D. (2006), "Why trust is bad for security", *Electronic Notes in Theoretical Computer Science*, Vol. 157 No. 3, pp. 3-9.

Grandison, T. and Sloman, M. (2000), "A survey of trust in internet applications", *IEEE Communications Survey*, Vol. 3 No. 4, pp. 2-16.

Hagberg, R. and Heifetz, J. (1997), "Corporate culture: telling the CEO the baby is ugly", Hagberg Consulting Group, San Mateo, CA, available at: www.hcgnet.com/research.asp? id=6 (accessed July 3, 2014).

Hausman, A. and Johnston, W.J. (2010), "The impact of coercive and non-coercive forms of influence on trust, commitment, and compliance in supply chains", *Industrial Marketing Management*, Vol. 39 No. 3, pp. 519-526.

Haws, K.L., Dholakia, U.M. and Bearden, W.O. (2010), "An assessment of chronic regulatory focus measures", *Journal of Marketing Research*, Vol. 47 No. 5, pp. 967-982.

Holland, P., Copper, B. and Hecker, R. (2012), *The Electronic Workplace Survey: Analysis of the First National Survey on Employee Attitudes to Electronic Monitoring and Surveillance in the Australian Workplace*, Monash University, Melbourne.

Hon, A. and Lu, L. (2010), "The mediating role of trust between expatriate procedural justice and employee outcomes in Chinese hotel industry", *International Journal of Hospitality Management*, Vol. 29 No. 4, pp. 669-676.

Hsu ,M.-H., Chang, C.-M. and Yen, C.-H. (2011), "Exploring the antecedents of trust in virtual communities", *Behaviour& Information Technology*, Vol. 30 No. 5, pp. 587-601.

Hulland, J. (1999), "Use of partial least squares (PLS) in strategic management research: a review of four recent studies", *Strategic Management Journal*, Vol. 20 No. 2, pp. 195-204.

Ifinedo, P. (2011), "An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions", *Journal of Information Security and Privacy*, Vol. 7 No. 1, pp. 25-49.

Ifinedo, P. (2014), "Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition", *Information & Management*, Vol. 51 No. 1, pp. 69-79.

Kim, K. and Kim, J. (2011), "Third-party privacy certification as an online advertising strategy: an investigation of the factors affecting the relationship between third-party certification and initial trust", *Journal of Interactive Marketing*, Vol. 25 No. 3, pp. 145-158.

Kogler, C., Batrancea, L., Nichita, A., Pantya, J., Belianin, A. and Kirchler, E. (2013), "Trust and power as determinants of tax compliance: testing the assumptions of the slippery slope framework in Austria, Hungary, Romania and Russia", *Journal of Economic Psychology*, Vol. 34, pp. 169-180.

Kramer, R.M. (1996), "Divergent realities and convergent disappointments in the hierarchic relation: trust and the intuitive auditor at work", in Kramer, R.M. and Tyler, T.R. (Eds), *Trust in Organizations: Frontiers of Theory and Research*, Sage Publications, Thousand Oaks, CA, pp. 216-245.

Laurence, G.A., Fried, Y. and Slowik, L.H. (2013), "'My space': a moderated mediation model of the effect of architectural and experienced privacy and workspace personalization on emotional exhaustion at work", *Journal of Environmental Psychology*, Vol. 36, pp. 144-152.

Lee, S. and Kleiner, B.H. (2003), "Electronic surveillance in the workplace", *Management Research News*, Vol. 26 No. 2, pp. 72-81.

Lind, E.A. (2001), "Fairness heuristic theory: justice judgments as pivotal cognitions in organizational relations", in Greenberg, J. and Cropanzano, R. (Eds), *Advances in Organizational Justice*, Stanford University Press, Stanford, CA, pp. 56-88.

Luchak, A.A. and Gellatly, I.R. (2007), "A comparison of linear and nonlinear relations between organizational commitment and work outcomes", *The Journal of Applied Psychology*, Vol. 92 No. 3, pp. 786-793.

McKnight, D. H., Kacmar, C. and Choudhury, V. (2004), "Dispositional trust and distrust distinctions in predicting high- and low-risk internet expert advice site perceptions", *e-Service Journal*, Vol 3 No. 2, pp. 35-58.

Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995), "An integrative model of organizational trust", *Academy of Management Review*, Vol. 20 No. 3, pp. 709-734.

Milberg, S.J., Smith, H.J. and Burke, S.J. (2000), "Information privacy: corporate management and national regulation", *Organization Science*, Vol. 11 No. 1, pp. 35-57.

Mitrou, L. and Karyda, M. (2006), "Employeesprivacy vs employerssecurity: can they be balanced?", *Telematics and Informatics*, Vol. 23 No. 3, pp. 164-178.

Morrow, P.C., McElroy, J.C. and Scheibe, K.P. (2012), "Influencing organizational commitment through office redesign", *Journal of Vocational Behavior*, Vol. 81 No. 1, pp. 99-111.

Petronio, S. (1991), "Communication boundary management: a theoretical model of managing disclosure of private information between marital couples", *Communication Theory*, Vol. 1 No. 4, pp. 311-335.

Petronio, S., Flores, L., and Hecht, M. (1997). "Locating the voice of logic: disclosure discourse of sexual abuse", *Western Journal of Communication*, Vol. 61, pp. 101-113.

Petronio, S. (2002), *Bondary of Privacy: Dialectics of Disclosure*, SUNY Press, New York, NY.

Petronio, S. (2004), "The road to developing communication privacy management: narrative in progress, please stand by", *Journal of Family Communication*, Vol. 4, pp. 193-208.

Petronio, S. and Reierson, J. (2009), "Regulating the privacy of confidentiality", in Afifi, T. and Afifi, W. (Eds), *Uncertainty, Information Management, and Disclosure Decision: Theories and Application*, Routledge, New York, NY, pp. 365-383.

Quinn, R.E. and Spreitzer, G.M. (1991), "The psychometrics of the competing values culture instrument and an analysis of the impact of organization culture on quality of life", *Research in Organizational Change and Development*, Vol. 5, pp. 115-142.

Riegelsberger, J., Sasse, M.A. and McCarthy, J.D. (2005), "The mechanics of trust: a framework for research and design", *International Journal of Human-Computer Studies*, Vol. 62 No. 3, pp. 381-422.

Schumacher, S. (2010), "What employees should know about electronic performance monitoring", *ESSAI*, Vol. 8, available at: http://dc.cod.edu/essai/vol8/iss1/38 (accessed July 22, 2014).

Smith, W.P. and Tabak, F. (2009), "Monitoring employee e-mails: is there any room for privacy?", *Academy of Management Perpectives*, Vol. 23 No. 4, pp. 33-48.

Snyder, J.L. (2010), "E-mail privacy in the workplace: a boundary regulation perspectine", *Journal of Business Communication*, Vol. 47 No. 3, pp. 266-294.

Stanton, J. and Stam, K. (2003), "Information technology, privacy, and power within organizations: a view from boundary theory and social exchange perspectives", *Surveillance and Society*, Vol. 1 No. 2, pp. 152-190.

Sun, Y.L., Han, Z. and Liu, K.J.R. (2008), "Defense of trust management vulnerabilities in distributed networks", *IEEE Communications Magazine*, Vol. 46 No. 2, pp. 112-119.

Taddei, S. and Contena, B. (2013), "Privacy, trust and control: which relationships with online self-disclosure?", *Computers in Human Behavior*, Vol. 29 No. 3, pp. 821-826.

Taiwan National Statistics (2012), "Computer application report", Directorate General of Budget, Accounting and Statistics Executive Yuan, Taipei, available at: www.dgbas.gov.tw/public/Attachment/2103114391471.pdf (accessed August 10, 2014)

Taylor, R.E. (2013), "Privacy issues of electronic monitoring of employees: a cross-cultural examination of gender differences", *International Journal of Business and Social Research*, Vol. 3 No. 2, pp. 226-250.

Tenenhaus, M., Vinzi, V.E., Chatelin, Y.M. and Lauro, C. (2005), "PLS path modeling", *Computer Statistics Data Analysis*, Vol. 48 No. 1, pp. 159-205.

Townsend, A.M. and Bennett, J.T. (2003), "Privacy, technology, and conflict: emerging issues and action in workplace privacy", *Journal of Labor Research*, Vol. 24 No. 2, pp. 195-205.

Utami, S., Soemarno, S. and Bisri, M. (2014), "Disaster risk and adaptation of settlement along the river Brantas in the context of sustainable development, Malang, Indonesia", *Procedia Environmental Sciences*, Vol. 20, pp. 602-611.

van Dijke, M. and Verboon, P. (2010), "Trust in authorities as a boundary condition to procedural fairness effects on tax compliance", *Journal of Economic Psychology*, Vol. 31 No. 1, pp. 80-91.

Wu, K.W., Huang, S.Y., Yen, D.C. and Popova, I. (2012), "The effect of online privacy policy on consumer privacy concern and trust", *Computers in Human Behavior*, Vol. 28, No. 3, pp. 889-897.

Yang, J., Mossholder, K.W. and Peng, T.K. (2009), "Supervisory procedural justice effects: the mediating roles of cognitive and affective trust", *Leadership Quarterly*, Vol. 20 No. 2, pp. 143-154.

Yerby, J. (2013), "Legal and ethical issues of employee monitoring", *Online Journal of Applied Knowledge Management*, Vol. 1 No. 2, pp. 44-55.

Further reading

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-361.

Gambetta, D. (2000), "Can we trust trust?", in Gambetta, D. (Ed.), *Trust: Making and Breaking Cooperative Relations*, Department of Sociology, University of Oxford, Oxford, pp. 213-237, available at: www.sociology.ox.ac.uk/papers/gambetta213-237.pdf (accessed July 3, 2014).

Hausman, A. and Stock, J.R. (2003), "Adoption and implementation of technological innovation within long-term relationships", *Journal of Business Research*, Vol. 56 No. 8, pp. 681-686.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers & Security*, Vol. 31 No. 1, pp. 83-95.

About the authors

Dr Shuchih Ernest Chang is a Full Professor at the Graduate Institute of Technology Management, National Chung Hsing University (NCHU) in Taiwan. He received his MSCS and PhD Degrees from the University of Texas at Austin. Before joining the faculty at NCHU, Dr Chang worked at the UBS Financial Services Inc. in USA as a Divisional Vice President for about five years. He has 15 years of working experience in major computer and financial service firms in the USA, including Unisys, IBM, Sun Microsystems, JP Morgan, Bear Stearns, and UBS. His research interests are in electronic commerce, u-commerce, enterprise application architecture, information systems, information security management, and technology management.

Anne Yenching Liu is a PhD Student at the Graduate Institute of Technology Management, National Chung Hsing University and a Lecturer at the Department of Computer Science and Information Engineering, Hungkuang University and Chaoyang University. Her research interests are in electronic commerce, information security management, and technology management. Anne Yenching Liu is the corresponding author and can be contacted at: yench3@gmail.com

SungMin Lin is a PhD Student at the Graduate Institute of Technology Management, National Chung Hsing University and a Lecturer in the Center of General Education at the National United University and an Associate Researcher at the Patent Search Center in Taiwan. His research interests are in e-commerce, technological laws, and management.

This article has been cited by:

1. Shuchih Ernest Chang, Wei-Cheng Shen, Anne Yenching Liu. 2016. Why mobile users trust smartphone social networking services? A PLS-SEM approach. *Journal of Business Research* **69**:11, 4890-4895. [CrossRef]

2. KangMinghui Minghui Kang Minghui Kang is an Assistant Professor of Finance at the Southwest Jiaotong University. Her main research interests include corporate finance, investment, derivatives, risk management. GaoYiwen Yiwen Gao Yiwen Gao is a Graduate Student of the Information Management and Information Systems (Business Intelligence) Department at the Southwestern University of Finance and Economics. Her main research interests are internet finance and user behavior. WangTao Tao Wang Tao Wang is an Associate Professor at the School of Economic Information Engineering, Southwestern University of Finance and Economics in China. His main research interests include internet finance, Web 2.0 and Enterprise 2.0 applications. ZhengHaichao Haichao Zheng Haichao Zheng is an Associate Professor at the School of Economic Information Engineering, Southwestern University of Finance and Economics, China. His research interests include open innovation and crowdsourcing. School of Economics and Management, Southwest Jiaotong University, Chengdu, China School of Economic Information Engineering, Southwestern University of Finance and Economics, Chengdu, China . 2016. Understanding the determinants of funders' investment intentions on crowdfunding platforms. *Industrial Management & Data Systems* **116**:8, 1800-1819. [Abstract] [Full Text] [PDF]

3. Ileen E. van Vuuren, Elmarie Kritzinger, Conrad MuellerIdentifying gaps in IT retail Information Security policy implementation processes 126-133. [CrossRef]

4. Dagmara Lewicka Faculty of Management, AGH University of Science and Technology, Kraków, Poland Katarzyna Krot Department of Management, Bialystok University of Technology, Bialystok, Poland . 2015. The model of HRM-trust-commitment relationships. *Industrial Management & Data Systems* **115**:8, 1457-1480. [Abstract] [Full Text] [PDF]