Exploring Privacy and Trust for Employee Monitoring

Shuchih Ernest Chang; Anne Yenching Liu; Sungmin Lin
Institute of Technology Management, National Chung Hsing University
250 Kuo Kuang Road, South District, Taichung City 402, Taiwan

Abstract
Purpose–This study aims to evaluate privacy boundaries and explores employees’ reactions in employee monitoring.

Design/methodology/approach –The model comprised organizational culture, communication privacy management (CPM), trust, and employee performance in employee monitoring. Variables were measured empirically by administering 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. Both trust in employee monitoring policy and members had positive effects on employee commitment and compliance to employee monitoring.

Research implications- 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. Delivering messages of open and transparent employee monitoring processes is encouraged in the organization.

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: Communication Privacy, Employee Monitoring, Trust, Commitment, Compliance, Organizational Culture
Paper type: Research Paper

1. Introduction

The world has been transformed by the technologies developed throughout the Industrial Age. Since the introduction of personal computers in the late 1970s, the Information Age has ushered in the Internet, microcomputers, and information technologies that have diffused into the lives of individuals for both leisure and work (Hart, 2000). New technologies, such as email, global positioning system, wireless communication, and telematic units, have changed the conventional organizational setting and reshaped the relationship between an employee and an employer. While employers are often faced with adopting new technologies, employees, in response, should adjust their behaviors, roles, and responsibilities in a changing technological environment. The work–life boundary for employees is blurred as a consequence of failing to distinguish the difference between work and personal life. According to a recent survey performed in the United States, approximately 65% of employees spend at least some work time engaged in nonwork-related Internet activities, including personal profiles, browsing websites, and sending personal emails, during their typical workdays (Careerbuilder, 2011).

Given 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, email, and computers. For example, the American Management Association reports that 82% of employers used some form of electronic monitoring in the workplace in 2001, and 76% of organizations were engaged in tracking Internet usage in 2005 (DePree

©Copyright Reserved
Jude, 2006). In addition, Marshall (2001) reported that over three-quarters of major U.S. organizations engage in employee monitoring through various means. There is a wide range of software and hardware solutions to monitor employees in the workplace, such as keystroke logs, application and website usage, detailed file usage, incoming and outgoing chats and emails, 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% of employees were against email monitoring, 60% against telephone monitoring, and 56% against video surveillance. This suggests that while employers are concerned about monitoring any illegal actions that may jeopardize information 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 (Desprochers and Roussos, 2001; Fazekas, 2004). In American jurisdictions, an employee’s privacy expectations are only minimally recognized by the law or the courts (Mitrou, and Karyda, 2006). 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 v. Germany) and thus, employees have a legitimate expectation of privacy in the workplace. 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.

The controversial tension between managing private and publicly shared information is described by Petronio (2004) as the Communication Privacy Management (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).

Organizational culture is an important aspect for understanding employee boundary rule formulation with regard to employee monitoring. 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.

Disagreements over the information boundary in CPM often lead to negative and unpleasant feelings in information sharing. One of the negative feelings is the lack of ability to trust. 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).

Our research used the metaphor of boundary turbulence in the CPM theory to demonstrate the psychological effect on employees. The research further investigated the influence exerted by organizational culture because the fit between it and employee monitoring is undetermined. Furthermore, the research investigated how employees viewed their trust within the organization when implementing employee monitoring. As a result, employees’ compliance and commitment to the practice of employee monitoring were determined.

2. Literature Review
2.1 Communication privacy management 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 Reierison, 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 Reierison, 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 email 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 email, browsing websites 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; Townshend 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 identifies three boundary categories that lead to turbulence (Petronio, 2002). 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 (Altman, Vinsel, and Brown, 1981; McGrath, 1984).

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. There are various approaches to define and evaluate trust. The concept of trust in the social sciences, such as sociology and philosophy, is developed and summarized as “a particular level of the subjective probability with which an agent assesses that another agent or a group of agents will perform a particular action, both before he can monitor such action and in a context in which it affects his own action” (Gambetta, 2000). 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 (Hoven, 1997; Deutsch, 1958; Mayer et al., 1995; Grandison and Sloman, 2000; Bahtiyar and UfukCaglayan, 2012). Researchers use these influential factors to determine the tendency of trust (McKnight et al., 2004; Riegelsberger, 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 (Koller, 1998; McKnight, Cummings, and Chervany, 1998; Beldad et al., 2011). The feeling of vulnerability and/or uncertainty about an outcome relates to risks in trust (Doney et. al, 1998). Human relationships are filled with various risks (Sheppard and Sherman, 1998). These risks can “paralyze actions or lead to feelings of engulfment, dread, or anxiety” (Lupton, 1999). 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. For example, the control center video session recorder, access point controller, and remote client management system are each programmed to provide different levels of monitoring. 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. Workplace monitoring is intended to protect organizational assets, and organizations rely on various means to enforce its policies. Implementing spying technologies can be described as an outlook of a trusted computing base, which is “the totality of protection mechanisms within a computer system—including hardware, firmware, and software—the combination of which is responsible for enforcing a security policy” (US Department of Defense, 1985). This outlook fits the trust management theory, which defines trust as “a bridge between social needs and security solutions to cope with trust management vulnerabilities for distributed networks” (Sun et al., 2008; Bahtiyar and UfukCaglayan, 2012). In addition, trust can also be viewed as a manifestation of reasoning and judgment processes (Trcek, 2009). 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.

![Figure 1. Proposed model](image-url)
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, Smith, and Burke (2000) showed a positive relationship between cultural values, corporate privacy policies, and government regulations. For the workplace policy, Allen et al (2007) found that cultural paradigm is linked to the existing practices in organizations. In accordance with these prior studies, 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.

Organizational culture is continuously constructed through a progressive process of establishing the values, meanings, and proprieties between individuals and an organization (Douglas, 1985). The establishment of organizational culture is based on individuals’ values, assumptions, and interpretations (Cameron and Freeman, 1991). 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 followed up by applying organizational culture to total quality management (Boggs, 2004). 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 in the examination of information security management. Chang and Lin’s research used two groups of dimensions, including the internal/external orientation versus 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.

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.

**Hypothesis 1:** Control-oriented organizational culture significantly relates to employees’ concern about organizational infringement.

**Hypothesis 2:** Control-oriented organizational culture significantly relates to employees’ incapability of maintaining privacy.

**Hypothesis 3:** Control-oriented organizational culture significantly relates to employees’ perceived amount of monitoring.

**Hypothesis 4:** Flexibility-oriented organizational culture significantly relates to employees’ concern about organizational infringement.

**Hypothesis 5:** Flexibility-oriented organizational culture significantly relates to employees’ incapability of maintaining privacy.

**Hypothesis 6:** 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., 1998). 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; Dijke and Verboon, 2009). 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 (Dijke and Verboon, 2009). 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.

Hypothesis 7: Employees’ concern about organizational infringement significantly relates to trust in employee monitoring policy.

Hypothesis 8: Employees’ concern about organizational infringement significantly relates to trust in employee monitoring members.

Hypothesis 9: Employees’ incapability of maintaining privacy significantly relates to trust in employee monitoring policy.

Hypothesis 10: Employees’ incapability of maintaining privacy significantly relates to trust in employee monitoring members.

Hypothesis 11: Employees’ perceived amount of monitoring significantly relates to trust in employee monitoring policy.

Hypothesis 12: Employees’ perceived amount of monitoring significantly relates to trust in employee monitoring members.

3.3 Employee performance: commitment and compliance

Moorman, Deshpande, and Zaltman (1993) defined trust as “a willingness to rely on an exchange partner in whom one has confidence.” In an organizational setting, the definition of trust is interpreted as “faith that an institution will be fair, reliable, competent, and non-threatening” (Carnevale, 1995). By establishing employees’ trust, an organization confronts fewer obstacles in implementing a policy. 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 (Allen and Meyer, 1990; 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; Allen and Meyer, 1990). 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 (Anderson, Fornell, and Lehman, 1994; Reichheld, 1996; 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.

Hypothesis 13: Trust in employee monitoring policy significantly relates to employees’ commitment to organizations’ employee monitoring.

Hypothesis 14: Trust in employee monitoring policy significantly relates to employees’ compliance with organizations’ employee monitoring.

Hypothesis 15: Trust in employee monitoring members significantly relates to employees’ commitment to organizations’ employee monitoring.

Hypothesis 16: 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, such as an organization’s name, position, tenure, and gender. The second section related to items under the construct of organizational culture, including eight items for cooperative traits, six items for innovative traits, six items for hierarchical traits, and six items for effective traits (Cameron, 1991; Quinn and Spreitzer, 1991; Denison et al., 2004; Boggs, 2004). Moreover, items for CPM were borrowed from Eddy, Stone, and Stone-Romero’s (1999) measure of perceived privacy invasion, Botan’s (1996) measure of workplace privacy, and Snyder’s (2010) revised version on the measurement of email privacy. A survey instrument for trust was taken from Hsu, Chen, and Yen’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 question items could be understood and measured validly, a pre-test was conducted in a small group. 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.

4.2 Sample characteristics
The surveys were distributed and collected in the first quarter of 2014. Surveys were distributed by snowballing sampling to participants who are full-time employees in organizations that currently practice employee monitoring. A total of 90 questionnaires were collected, of which 81 were valid. The number of male respondents was 48 and that of female respondents was 33. Respondents who filled the questionnaire
were from organizations in various industries and represented a variety of job categories. Most respondents (n = 72, 88.9%) were not in managerial positions. The analysis of the frequency distribution by age showed that most of the respondents (n = 76, 93.8%) were between 20 and 50 years. Respondents represented a range in tenure with their current organization, including less than five years (n = 48, 59.3%), five to ten years (n= 22, 27.2%), ten to fifteen years (n= 6, 7.4%), and more than sixteen years (n = 4, 4.9%).

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 (Formel 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 alpha, composite reliability score and average variance extracted (AVE). Cronbach's alpha 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 alpha. The dimensional latent construct is considered as unidimensional when its Cronbach’s alpha value and composite reliability score are larger than 0.7 (Tenenhaus, 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 1, the statistics for assessment satisfied the reliability standards.

Table 1 Composite reliabilities, Cronbach’s Alpha values and Average variance extracted

<table>
<thead>
<tr>
<th></th>
<th>AVE</th>
<th>Composite Reliability</th>
<th>Cronbachs Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comm</td>
<td>0.91855</td>
<td>0.985492</td>
<td>0.98231</td>
</tr>
<tr>
<td>COI</td>
<td>0.763909</td>
<td>0.976653</td>
<td>0.973656</td>
</tr>
<tr>
<td>Comp</td>
<td>0.816876</td>
<td>0.956685</td>
<td>0.941012</td>
</tr>
<tr>
<td>Control</td>
<td>0.603934</td>
<td>0.923913</td>
<td>0.910429</td>
</tr>
<tr>
<td>Flexibility</td>
<td>0.716382</td>
<td>0.96798</td>
<td>0.963904</td>
</tr>
<tr>
<td>IMP</td>
<td>0.975458</td>
<td>0.99375</td>
<td>0.991619</td>
</tr>
<tr>
<td>PAM</td>
<td>0.808927</td>
<td>0.962073</td>
<td>0.952517</td>
</tr>
<tr>
<td>TEMP</td>
<td>0.80121</td>
<td>0.941573</td>
<td>0.917234</td>
</tr>
<tr>
<td>TEMM</td>
<td>0.811727</td>
<td>0.945162</td>
<td>0.923368</td>
</tr>
</tbody>
</table>

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.

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 Lacker, 1981). As shown in Table 2, the discriminant validity for the constructs used in our study was acceptable since the square root of AVE on each construct was greater than the correlations of the construct with other constructs.

Table 2 Inter-construct correlations and square root of AVE measure

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

©Copyright Reserved
The inner model which specified the relationships between latent variables was then estimated. The path coefficients for the endogenous latent variables and R-square statistics were derived. The inner model results are presented in Table 3.

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Path coefficient</th>
<th>p-value</th>
<th>Inference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control -&gt; COI</td>
<td>H1</td>
<td>0.375***</td>
<td>0.0003</td>
</tr>
<tr>
<td>Control -&gt; IMP</td>
<td>H2</td>
<td>0.345***</td>
<td>0.0005</td>
</tr>
<tr>
<td>Control -&gt; PAM</td>
<td>H3</td>
<td>0.332**</td>
<td>0.0025</td>
</tr>
<tr>
<td>Flexibility -&gt; COI</td>
<td>H4</td>
<td>-0.270**</td>
<td>0.0050</td>
</tr>
<tr>
<td>Flexibility -&gt; IMP</td>
<td>H5</td>
<td>-0.087</td>
<td>0.3587</td>
</tr>
<tr>
<td>Flexibility -&gt; PAM</td>
<td>H6</td>
<td>0.018</td>
<td>0.8694</td>
</tr>
<tr>
<td>COI -&gt; TEMP</td>
<td>H7</td>
<td>-0.382***</td>
<td>0.0008</td>
</tr>
<tr>
<td>COI -&gt; TEMM</td>
<td>H8</td>
<td>-0.267**</td>
<td>0.0075</td>
</tr>
<tr>
<td>IMP -&gt; TEMP</td>
<td>H9</td>
<td>0.274</td>
<td>0.1087</td>
</tr>
<tr>
<td>IMP -&gt; TEMM</td>
<td>H10</td>
<td>-0.170</td>
<td>0.2417</td>
</tr>
<tr>
<td>PAM -&gt; TEMP</td>
<td>H11</td>
<td>-0.482**</td>
<td>0.1114</td>
</tr>
<tr>
<td>PAM -&gt; TEMM</td>
<td>H12</td>
<td>-0.252</td>
<td>0.0032</td>
</tr>
<tr>
<td>TEMP -&gt; Comm</td>
<td>H13</td>
<td>0.348***</td>
<td>0.0000</td>
</tr>
<tr>
<td>TEMP -&gt; Comp</td>
<td>H14</td>
<td>0.371***</td>
<td>0.0003</td>
</tr>
<tr>
<td>TEMM -&gt; Comm</td>
<td>H15</td>
<td>0.378***</td>
<td>0.0000</td>
</tr>
<tr>
<td>TEMM -&gt; Comp</td>
<td>H16</td>
<td>0.373***</td>
<td>0.0000</td>
</tr>
</tbody>
</table>

*p<0.05, **p<0.01, ***p<0.001

4.4 Empirical results

The empirical results confirm that control-oriented organizational culture significantly and positively affected employees’ concern about organizational infringement (β=0.375435, p=0.000337), incapability of maintaining privacy (β=0.345114, p=0.000478) and perceived amount of monitoring (β=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 (β=-0.269849, p=0.004988). Concern about organizational infringement significantly and negatively affected employees’ trust in employee monitoring policy (β=-0.382334, p=0.000846) and trust in employee monitoring members (β=-0.267447, p=0.007511). Incapability of maintaining privacy did not significantly affect employees’ trust in employee monitoring policy (β=0.274019, p=0.108733) and trust in employee monitoring members (β=-0.169619, p=0.241691). Perceived amount of monitoring significantly and negatively affected employees’ trust in employee monitoring policy (β=-0.481956, p=0.003169) but not significantly in trust in employee monitoring members (β=-0.251733, p=0.111442). Trust in employee monitoring policy significantly and positively affected employees’ commitment (β=0.348448, p<0.0001) and compliance (β=0.370951, p=0.000281) to employee monitoring. Trust in employee monitoring policy significantly and positively affected employees’ commitment (β=0.378402, p<0.0001) and compliance (β=0.372654, p<0.0001) to employee monitoring. Overall, hypotheses H1, H2, H3, H4, H7, H8, H11, H13, H14, H15 and H16 postulated in this 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 supported a favorable environment for information security practice; 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, Dholakis and Bearden, 2010; Jin, 2014). 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, and 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, information 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. Botan (1996) showed that the amount of monitoring and unnecessary monitoring lead to negative perceptions of organizational information security. 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; Morgan and Hunt, 1994). In addition, increasing trust in a policy elevates the level of compliance (Dijke and Verboon, 2010; Kogler et al., 2013). Thus, employees with trust in policy are generally more committed and complied with their organization. In addition, trust in employee monitoring showed a significant and positive relationship with employee commitment and compliance. Trust is an important factor in a strategic partnership and requires partners to be trustworthy in a relationship (Wilson and Mummaliani, 1988). 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. Although most employee monitoring practices are legitimate, concerns over privacy infringement still exist for employees. Delivering messages of open and transparent employee monitoring processes is the organization’s first task. Moreover, organizational messages emphasizing positive consequences are preferred over the negative consequences because it subdues the negative psychological feelings of employees. Excessive monitoring delivers a negative message of privacy protection and leads to employees’ distrust toward the organization’s employee monitoring policy. Furthermore, legislation, contracts, and policies may force employees to accept the organization’s employee monitoring practice. However, employees’ psychological resistance to employee monitoring may still exist. 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 information security systems. Previous research focused on employee monitoring and its potential outcomes (Botan, 1996; D’Urso, 2006); however, further exploration on how to successfully implement employee monitoring is necessary. The CPM theory focused 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 antecedent of privacy boundary turbulence has been rarely investigated in previous studies. These studies demonstrated that different organizational cultures have different effects on the implementation of information security management (Chang and Lin, 2007; Chang and Ho, 2006); however, 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. Researchers in the past showed that employees’ concerns over privacy infringement are associated with negative relationships within organizations and negative emotions, such as exhaustion and distrust (Snyder, 2010; Laurence et al., 2013). Petronio (2002) suggested that privacy boundary turbulence puts relationships at risk. 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 (Botan, 1996; 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. Trust is important in relationships and can be adopted strategically to create partnerships (Wilson and Mummalaneni, 1988). Numerous studies have demonstrated the positive relationship between trust and employee commitment and compliance (Utami et al., 2014; Morgan and Hunt, 1994; 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 position, may also lead to different privacy expectations. Future study may differentiate the effects of demographic variance on employee monitoring.

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 (1) a control-oriented organizational culture raised communication privacy turbulence in CPM, (2) 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 (3) 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 information security department staffs for enhancing employee performance through workplace monitoring.

Acknowledgement

This work was supported by the Ministry of Science and Technology, Taiwan, under contract number MOST-103-2221-E-005-050-MY2.

References:


Petronio, S., &Reierison, J. (2009), “Regulating the Privacy of Confidentiality”, *Uncertainty, Information Management, and...*