Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America

Moussa, Mahmoud

Published Version: https://doi.org/10.1177/2158244015580168

Moussa, M. (2015). Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America. Sage Open, 5(2), 1–13. https://doi.org/10.1177/2158244015580168

Document Version: Published Version

Published Version: https://doi.org/10.1177/2158244015580168

Repository homepage: https://researchrepository.rmit.edu.au

© The Author(s) 2015
Downloaded On 2023/10/23 00:19:25 +1100
Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America

Mahmoud Moussa

Abstract
Despite the historic American love for privacy that has enhanced innovation and creativity throughout the country, encroachments on privacy restrain individual freedom. Noticeable, advances in technology have offered decision makers remarkable monitoring aptitudes that can be used in numerous tasks for multiple reasons. This has led scholars and practitioners to pose a significant number of questions about what is legitimate and illegitimate in the day-to-day affairs of a business. This article is composed of (a) research about electronic monitoring and privacy concerns; (b) definitions of, critiques of, and alternatives to electronic performance monitoring (EPM); (c) motives behind employee monitoring and leadership behaviors; (d) advice that makes monitoring less distressful; (e) employee monitoring policies; (f) reviewing policies and procedures; (g) the role of human resource development (HRD) in employee assessment and development; and (h) conclusion and recommendations for further studies.

Keywords
employee, employer, information, monitoring, privacy, organization

Research About Electronic Monitoring and Privacy Concerns
Monitoring increased concerns about employee privacy; therefore, employers must find a balance between monitoring gains and the costs of invading employee privacy (Jackson, Schuler, & Werner, 2009). However, the use of emerging technologies in monitoring employee practices is raising concerns that the privacy rights of employees are vulnerable, and it is becoming more challenging to balance employer security rights with employee privacy issues (Mathis & Jackson, 2000). Consequently, significant privacy issues are being debated in business and government, for example, (a) violation of privacy: examining and retrieving private e-mails, records, and information about employees from their access to particular Internet websites; (b) computer monitoring: continually knowing where the employee is; (c) computer matching: synthesizing information obtained from different sources to enhance your marketing services; and (d) unauthorized personnel files: gathering telephone numbers, e-mail addresses, credit card numbers, and other private information to develop customer profiles (O’Brien & Marakas, 2006). Technological advancements enabled employers to enhance employee productivity and put employee privacy under siege. Robbins and Coulter (1999) presented some perplexing questions, such as the following:

1. Is the e-mail system for business purposes only?
2. Is an employee allowed to e-mail work information to a colleague along with some personal chatting?
3. What is the acceptable use of the system?
4. Who possesses the information that is produced from the network?

Organizations regulate Internet use, or website visits by their workforce, through two regular ways: by restricting access to particular links, and by monitoring employee actions (Alampay & Hechanova, 2010). In this study, it also is revealed that monitoring policies and controlling websites vary from one country to another; for example, China, Vietnam, and Singapore not only block certain sites but also proscribe access to political and linguistic affairs. Everett, Wong, and Paynter (2006) found that a significant number of subjects related to employee and employer rights should be taken into consideration in further studies: (a) A significant issue is concerned with building trust between employers and employees in the workplace; another vital topic is linked

1Rajamangala University of Technology Lanna, ChiangMai, Thailand

Corresponding Author:
Mahmoud Moussa, Rajamangala University of Technology Lanna, 105/13 Ornsinir 1, Nongjom, Sansai, ChiangMai 50210, Thailand.
Email: rmutlhrd@gmail.com

Creative Commons CC BY: This article is distributed under the terms of the Creative Commons Attribution 3.0 License (http://www.creativecommons.org/licenses/by/3.0/) which permits any use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access page (http://www.uk.sagepub.com/aboutus/openaccess.htm).
with the establishment of pertinent legislation that manages privacy issues in workplace surveillance forthrightly; (b) a thorny factor is the growing occurrence of satellite, communal facility, and work at home, which urge employers to monitor their employees; (c) the diversification and capacities of the Internet for communication provide new topics for research; (d) the possibility to ascribe all small electronic devices in the workplace that could be used to e-mail firms’ secrets to an external beneficiary; and (e) enlarging the international comparison and probing the rising position of international standards and “harmonization agreements,” concerning policies developed by the European Union and the United Nations, as well as standards propagated by the International Organization for Standardization, the national defense agencies, and government branches of criminal investigation.

Everett et al. (2006) referred to certain issues potentially leading to greater employer use of the perception that such monitoring is needed. For example, government efforts to crush terrorism, assure the proliferation of govern nuclear weapons knowledge, hinder money laundering, and limit drug traffickers, both unlawful and pharmaceutical. More recently, employers have begun tracking their employees by using global positioning system (GPS) technology, which uses an assemblage of satellites to specify the precise location of the GPS-enabled device. Therefore, Townsm and Cobb (2012) recommended realistic steps when applying GPS tracking as follows: incorporate GPS tracking with other policies; preserve the right to monitor; do not create a conclusive evidence with GPS tracking documents; limit the use of GPS technology to monitor; rigorously outline appropriate use of company cell phones, vehicles, and so on; develop a consent language; continually check GPS equipment; and consider safeguarding records.

Another study by Ciocchetti (2011) classified each of the top monitoring practices into one of the following types: (a) best practices (e.g., monitoring that presents the greatest protection and minimizes invasion of employee privacy), (b) risky practices (e.g., monitoring that offers rather low protection and minimally attacks employee privacy), (c) borderline practices (e.g., monitoring that provides high protection, yet is also highly insidious), and (d) poor practices (e.g., monitoring that provides low protection and is extremely invasive). This classification system is likely to assist lawmakers to balance both employer and employee interests when legalizing workplace technology. Ciocchetti viewed that the American legal system has been sluggish to react effectively and efficiently to the increasing invasiveness of modern monitoring technology and that all monitoring practices are disturbing and fall into the four categories just mentioned. However, Bennett and Locke (1998) stated that an effective way to avoid liability for privacy assault is to presuppose that if an employee can litigate for such a tort, the employee will.

Research showed that employees can find an inclusive source of privacy protection resulting from the common law right to privacy, which consists of three misdeeds relevant to the employment relationship: intrusion on seclusion, which arises an encroachment is an intrusion on the property of another without that person’s permission; publicity given to one’s private life, which exists when an individual gives publicity to an issue regarding the private life of another; and publicity placing a person in a false light, which occurs when an individual heedlessly disregards the falsity of the revealed issue and the false light in which the other person would be placed (Hames & Diersen, 1991). Alternatively, a set of reforms developed by Conlon (1997) protect individual privacy concerns in the workplace:

- No monitoring should be done in restrooms, locker rooms, and employee lounges; however, time spent outside the workplace can be monitored in less odious ways.
- Offsite monitoring should be banned; allow employees to access all information collected through monitoring methods or techniques and consider their reflection on such information; and limit the duration of monitoring each day with a suggested (maximum of 2 hr per day).
- Employees should be aware of the devices that will be used to monitor them, how the data will be used, and when exactly they will be monitored; and employees and customers should be notified when telephonic monitoring is taking place through the use of a specific tone that can be heard by both employee and customer.
- Employers should collect only information relevant to making critical decisions; and it is not enough to justify monitoring by the need to increasing productivity or enhancing performance, but also, employers should be able to demonstrate how the goal was accomplished through the monitoring process.

Howsoever, the lawful foundation of the right to privacy has a theoretical underpinning for legal intellectuals that may be complex for the public to recognize or value (C. L. Swanson, 1988). Despite the different schools of thought among academics, numerous propositions have been offered for management’s contemplation: formulate why, how, and when electronic monitoring is applied; gather only work-related information; gather only information for the purpose of raising employee performance; provide timely feedback to employees so that corrective actions to performance can be done; secure awards to individuals or group performance; educate employees about the behavioral and social features of electronic monitoring; accentuate qualitative characteristics of performance not accounted for by electronic monitoring; a trial period for all new applicants or new electronic systems should be provided; avoid being too quick in developing new standards or monitoring methods unless proven to be effective; and use brainstorming sessions whenever possible to enhance the
electronic monitoring system in the organization (Vaught, Taylor, & Vaught, 2000). Nevertheless, too much monitoring and the publicity of a monitoring culture throughout the organization may create emotional and behavioral problems that may ultimately thrust employees into certain activities to cheat the system (Barrett, 2008).

Intriguingly, Dillon and Thomas (2006) exposed that there is a great need for universal consciousness and indulgence of accessibility, personal use, and administrative oversight issues involving e-mail and computers in the workplace; otherwise, employees are unlikely to understand privacy policies and procedures adequately. Wen, Schwieger, and Gershom (2007) reviewed surveillance technologies and discussed the related federal and state laws along with U.S. judicial decisions, and found that no U.S. federal or state law prohibits employers from monitoring their electronic workplace. Their scientific investigation also provided the following strategies that are likely to be most effective and productive for both employees and employers, and help employers prevent the negative aspects of monitoring: designating privacy policy oversight and execution should be implemented by an authority; consider a legal stand-point to legally guide the development of all policies and procedures; develop a formal policy and keep all employees informed of all modifications to the policy; notify employees of the electronic monitoring system; avoid an aggressive work environment; develop clear rules on the use of e-mail; decide which data should and should not be accessed; specify online time limits; maintain a software running in the background of every computer, such as popup blockers or spam filters; and communicate a policy that is acceptable for instant messaging, blogging, and chat room use in and out of the organization.

Haller (2002) also proposed the main ingredients of effective privacy policies: (a) notice, firms should provide stakeholders with a prominent notice vis-à-vis its information practices; (b) consumer choice, firms should give stakeholders the freedom to choose whether it may divulge personal data about them to unaffiliated third parties; (c) access and correction, firms should accept their stakeholders to make some corrections if necessary about personal data that they have gathered about them; (d) security, firms should espouse practical security measures to protect the privacy of personal information, and these measures may comprise administrative, physical, and technical security; and (e) enforcement, firms should develop a system that can enforce its privacy policy and ensure compliance with their own and external standards. Moreover, maintaining a balance between employers’ propensity to productivity and compliance with legislative procedures, corporations may be most successful in practicing the following: creating unambiguous privacy boundaries, developing privacy formula and principles, and defending personal data (Townsend & Bennett, 2003).

Employers are less vulnerable regarding certain issues of invasion of privacy, if written policies are communicated effectively; however, Kovach, Jordan, Tansey, and Framinan (2000) argued that too much monitoring generates a workplace filled with gridlock, blame, cynicism, and distrust. Practically speaking, to circumvent violations of employee privacy in the workplace, employers should never promote a culture of privacy within every quarter of an organization because it may be essential to monitor some practices when issues occur (Guffey & West, 1996). An ethical employer will monitor employees’ work within the provisions of a particular policy (Cowan, 2008). Corporations must enroll if they are coping with personal information for any of the following purposes: private investigation, health administration, policing crime avoidance and trial of delinquents, legal services, debt administration, trading, public casework, education, research, administration of justice, consultancy services, or a credit reporting system (Grupe, Kuechler, & Sweeney, 2002).

Summed up briefly, Zachary (2013) acknowledged the following: Workplace encroachment to privacy is of immense concern to both employers and employees in the United States, and violation of privacy has been augmented in employment proceedings. Invasion of privacy may fall into four categories: (a) information leakage that denigrates others, (b) using someone else’s name without consent, (c) inappropriate communication of private data, and (d) when a perpetrator purposefully intrudes, physically, electronically, or otherwise, on the private space of others. Courts vary according to when the illegal intrusion exists, and employers should be extremely vigilant to dissimilar types of invasion of privacy. Remarkably, disputes to privacy rights in the United States, which some view as a threat to eroding primary American values, have had an upsurge in controversy over the degree to which rights formerly untouched may are reduced because of the employer–employee relationship (Anton & Ward, 1998). In the following section, the author presents possible alternatives to electronic performance monitoring (EPM).

**Definitions of, Critiques of, and Alternatives to, Electronic Performance Monitoring (EPM)**

According to Belcourt, Bohlander, and Snell (2008), employee monitoring acts involve monitoring Internet links, review of e-mails, telephone use, video surveillance for security purposes, storage and review of computer files, video recording of employee job performance, recording and review of telephone conversations, and storage and review of voice-mail messages. Dessler (2011) noted that EPM systems are intended to allow employers access to their employees’ computers and telephones to monitor the amount of time spent working on the Internet, to enhance productivity. This paradox necessitates the establishment of a security system for all data garnered by employers to thwart the theft of sensitive information, particularly to those outside the organization (Mello, 2006). In a similar vein, new information technologies allow
employers to monitor employee work performance, even when the employee is not notified about the monitoring process (Nelson & Quick, 2006). Nonetheless, Mathis and Jackson (1997) verified that employee performance is not driven by management, but eventually by the employees themselves. For instance, ethical behavior is not based solely on the decisions and actions of an organization’s authorities, but also encompasses the actions of every employee (Dlabay, Burrow, & Egglan, 2006). They construed that ethical behavior consists of the actions of individuals and groups and the results of those actions.

Moreover, performance criteria for measuring job performance can be categorized as “trait-based,” “behavior-based,” or “results-based.” However, courts in the United States declared and affirmed that evaluations based on traits such as flexibility are too blurred and indistinct (Mathis & Jackson, 1997). Although it can be argued that employers should measure performance criteria in terms of time versus productivity. In other words, employees can be paid or compensated for time spent on particular tasks or on the amount of work produced. Aside from this, Mathis and Jackson claimed that a performance evaluation should be contemplated regarding assessment to achieve its purpose objectively and subjectively. Objective measures may be in terms of counted quantities or amounts; whereas, subjective measures may be apposite for casual or informal mistakes. Other performance measures acknowledged by Mathis and Jackson (2000) were category rating methods, a graphic rating scale, a checklist, or a combination of methods. Employers should articulate what they want to accomplish from a performance appraisal system to obtain the desired advantages with regard to perceptions and rights of the organization’s employees.

Comprehensively, Dessler (2003) discussed achievable and indispensable factors that might lead to developing a legally justifiable performance appraisal system, as follows: (a) make certain what a successful performance means, undertake a job analysis to recognize the critical requirements needed, and amalgamate these criteria into a rating tool; (b) define job performance magnitude, write and communicate performance criteria to all employees and employers, and avoid broad terms, such as “integrity” and “hardworking,” unless you can lead by example or model the behavior you desire; (c) use subjective supervisory ratings as only one part of the overall evaluation process, train evaluators how to use the rating instrument effectively, authorize evaluators to approach the employees they are evaluating, and conclude your evaluation on different measures for each of the job’s performance criteria; (d) have more than one evaluator and perform all evaluations independently to reduce biases and errors, employees should be given the freedom to review their appraisals and make comments before completion, and supplement your personnel decisions with documents and reasons; and (e) whenever possible, provide supervision to aid low performers at work. In addition, a workforce should attempt to be consciously and intently aware of the idea that high-performance work systems are likely to fail without timely and accurate communication (Bohlander & Snell, 2004).

Norton (2006) disclosed that people should realize that their interests and practices are being monitored automatically and routinely because the monitoring can be accomplished through programs running on their computers or a connected server. Norton also reported that there are commercial profiles for most people in the United States based on the browsing activity of a particular IP address. This address is tied to the name of the owner of that address no matter who is doing the actual browsing. The reports contain information about browsing habits and may contain accompanying marketing conclusions, called psychographic data. (p. 541)

Computer technology today supports many performance management systems, and employers frequently accumulate records of employee performance measures, punitive actions, and work rule violations in electronic files (Noe, Hollenbeck, Gerhart, & Wright, 2007). They also added that Congress has developed laws to legalize computer monitoring, but in the meantime, employers should consider employee feedback to this type of performance analysis. Once critical issue is that social forecasting, opinion surveys, social audits, issue management, and social/executive scanning can systematically measure the economic performance of an organization (Bartol & Martin, 1991). Thus, here, the author argues that many alternatives to electronic monitoring may be effective and are likely to satisfy an employer’s vision or objectives without violating rights of privacy. Employers should not disregard the three feasible interpretations of the job satisfaction and performance relationship: satisfaction leads to performance, performance leads to satisfaction, and rewards lead to both performance and satisfaction (Schermershorn, 2011).

Other alternatives to electronic monitoring may include the primary measures of productivity, such as total product (TP), the highest level of outcome that can be accomplished within a specific amount of inputs; average product (AP), an assessment of the outcome achieved per unit of input; and marginal product (MP), the change in total output divided by the change in capital (Baye, 2009). Arguably, employers who justify electronic monitoring by boosting productivity in the workplace may want to exercise the following: assuage or eliminate bureaucracy, revise all systems and recognize high quality employees, overcome problems, share your vision throughout the organization, question your employees and listen to them carefully, be honest and have integrity, turn customers into strategic partners, and develop effective performance-based pay plans (Moss, 2006).

What is more, the increasing use of e-mail and voice-mail augmented every employer’s risks of being legally responsible if they monitor or check employee electronic communications. As a result, the Electronic Communications Privacy
Act (ECPA) was passed in 1986. This is the only federal law that has permitted listening to, or detecting, employee electronic communication for business purposes, only if there is consent provided by the employee for this act (Mathis & Jackson, 2000). Although the ECPA proscribed the intentional interception of employees’ oral, wire, and electronic communication, it included two significant workplace exceptions, which are as follows:

- The “business purpose exception,” which constitutes consent to monitoring as long as the employer is capable of showing genuine business reasons for this action.
- The “consent exception” allows employers to monitor employee communications when employees have given their permission to do so (Dessler, 2011; Mello, 2011).

According to the Bureau of National Affairs (2012),

In the United States, only Maryland, Illinois, and California have laws that limit employer access to employee social media accounts. Fourteen states considered such legislation in 2012, according to materials provided at the webcast, and federal bills have been introduced. (p. 8)

The close auspices and supervision by employers are, perhaps, the major benefit from an electronic monitoring system; however, some employees appreciate them because they benefit them, whereas others consider them a violation of privacy (DuBrin, 2009). DuBrin (2006) articulated that high-technology monitoring devices can be useful with employees who carry out quantifiable tasks during working hours, such as employees in financial institutions and call centers. Another view presented by Robbins and Coulter (1999) was that many individuals consider electronic monitoring as just a technologically complicated type of eavesdropping, or a surveillance method to catch employees who are practicing illegal activities during their working hours. Critics also declare that electronic monitoring can backfire and raise employee stress because of being watched continually (Dessler, 2011). The next part of this article is a discussion of some reasons behind employee monitoring and leadership behaviors in organizations.

**Motives Behind Employee Monitoring and Leadership Behaviors**

Belcourt et al. (2008) found that motives behind employee monitoring are varied, such as, to prevent inappropriate actions of employees; to emphasize the need for the effective use of the organization’s time; to minimize employee gossip; to abolish the viewing of pornographic webpages; and to protect employees’ personnel information from becoming accessible to hackers who are likely to use the information inappropriately. Moreover, abuses by some employees, such as using the organization’s computer for gambling, engaging in private businesses, playing computer games, or pursuing personal affairs, have led to many employers engaging in a greater policing role (DeCenzo & Robbins, 2005). However, monitoring systems can be used to accumulate, process, and give performance feedback about employees’ work that can assist managers with performance improvement propositions and with employee development (Robbins & Coulter, 1999).

Employers justify their interference into employee privacy by stating their genuine interest in some of the employees’ personal matters, especially when those matters such as drug and alcohol use, criminal activity, or dating a colleague may directly affect workplace productivity, safety, and ethical standards (Bohlander & Snell, 2004).

Another significant issue is that employers need to monitor decision execution to ensure that things are making progress as planned, and that problems have been identified and resolved (Bartol & Martin, 1991). Today, monitoring is far beyond spying on employees’ phones and e-mails. For instance, Dessler (2000, 2011) mentioned that location monitoring has become pervasive, which involves following the location and movement of employees, because as Dubrin (2006) stated, a major factor to electronic monitoring is that employees often work far from their managers, including at home, hotels, or in coffee shops. One solid reason behind monitoring employees is that employers can be sued for what their employees send to each other and to individuals outside the organization (Haag & Cummings, 2010; Mathis & Jackson, 2000). Haag and Cummings also enumerated employers’ motives behind seeking and storing personal data about their employees, such as the need to recruit the best staff possible and prevent being charged for employees’ practices in the organization, and to ensure that employees are not wasting or misusing the organization’s resources. They reported the FBI’s statement that 78% of selected organizations indicated that employees download pornography, pirate software, and engage in other activities unrelated to their work, and 60% of employees use the Internet for personal use at work. Organizations reportedly lost $5.3 billion because of frivolous web activities in 1999 (Dessler, 2003).

Employee monitoring is intended to measure the amount of work produced, to check for theft, or to enforce an organization’s rules and policies (Mathis & Jackson, 1997). Experts have estimated that employee theft (e.g., theft of merchandise, embezzlement, industrial espionage, computer crime, acts of sabotage, and misuse of time on the job) causes U.S. businesses to spend more than $400 billion annually (Gomez-Mejia, Balkin, & Cardy, 2004). Therefore, employers are struggling to fight against various types of theft by using electronic surveillance gadgets to monitor employees, which some would call spying on employees. Gomez-Mejia et al. (2004) urged employers to do the following: provide guidelines to all employees for the rules regarding exchanging messages and information, and the acceptable use of the
Internet; discover positive uses for electronic monitoring tools that are valuable and advantageous to both employers and employees; create an “anti-theft policy” and post it throughout the organization; and prevent secret monitoring, except in specific cases (i.e., only with a court order).

In addition, technology has facilitated employees acting in immoral, irrelevant, and illegal ways, which created ethical, productivity, and legal dilemmas for organizations and forced employers to monitor employee practices (Belcourt et al., 2008). However,

Work rules that are too strict or confining will impede the fulfillment of such human needs as those for affiliation, cooperation, autonomy, and self-actualization and may lead to subterfuge and resentment. Rules that are too lax may lead to inefficiencies as well as moral problems. Work rules that tend to protect jobs, may provide job security in the short run but, if too restrictive, may have serious consequences for organizational effectiveness and survival in the long run. (French, 1994, p. 204)

In addition, several court decisions acknowledged an avowed policy of monitoring employees and employers of both private and public sectors to conduct workplace investigation for theft and other banned practices (Mathis & Jackson, 2000). Therefore, more than 80% of large corporations are now using such technology that can be used to monitor not only Internet usage but also e-mails, computer files, voice-mail, and telephone usage (Mello, 2006).

It also has been found that employees waste time when they extend lunch periods, when they use the telephone for personal matters, when they abuse sick leave, when they use unauthorized absenteeism, or when they work for another employer on their primary employer’s time. Thus, Gomez-Mejia et al. (2004) noted that employers use unseen microphones and transmitters linked to telephones and tiny fish eye video lenses fixed behind pinholes in walls and ceilings to spy on employees to eradicate such wastage. Needless to say, many employees consider this close management and supervision very dehumanizing (Stair & Reynolds, 2008). Thus, it can be said that overwhelmingly, monitoring has a dubious reputation because of cases of abuse and overuse. Baltzan and Phillips (2009) mentioned that a primary goal of information technology monitoring is tracking employee assignments by such measures as the frequency of errors made on a particular task and the number of tasks performed within a specific period.

Above all, two pertinent questions should be taken into consideration in organizations that advocate and implement monitoring technology: (a) What does this technology add to the organization? and (b) Does the organization trust its employees? According to Gomez-Mejia et al. (2004), augmenting trust can be difficult, particularly in organizations with a culture of cynicism. There are many arguments about centralization versus decentralization management approaches, in the sense where employees may have maximum restrictions concerning operations and minimum autonomy, or minimum restrictions and maximum autonomy. Furthermore, corporations should continually obtain answers to the following questions (McCalman & Paton, 1992): How autonomous are the systems? What relationships exist? How relevant are they? Will developments lead to re-definition of boundaries? Can the complexities of the change environment be simplified? Having determined the general environment, employers could then emphasize irrelevancies or deficiencies in the system as a whole.

Undoubtedly, the rise of technology causes ethical challenges in organizations. The rise and the use of technology cohere with and emerge from an organizational culture, values, and leadership style. Yet, relatively little effort has been made to study and compare leadership approaches systematically, in the context of how leaders should react to employee monitoring through technology. Luthans and Doh (2009) distinguished between three types of leadership as follows: (a) authoritarian leadership (i.e., the use of one-way communication from top to bottom with an emphasis on work progress and procedures that diminish work output, and final decisions usually made by the upper-level of management); (b) paternalistic leadership, or belief in reciprocity (i.e., work hard and the organization will offer a person more bonuses); and (c) participative leadership (i.e., authority is greatly decentralized). Certo and Certo (2009) also distinguished between four types of leadership as follows: (a) superleadership (i.e., leading by example), (b) servant leadership (i.e., the perception that a leader’s primary duty is to help subordinates to fulfill their desires, or interests), (c) entrepreneurial leadership (i.e., the perception that the leader is self-employed), and (d) transformational leadership (i.e., leadership that has the capability to inspire organizational success and influence followers’ beliefs in what can shape a successful organization.

Accordingly, the focal point is that the most effective leadership style to monitor employee performance using technology remains unidentified. Predominantly, the behaviors of employers are being scrutinized, and corporate governance models increasingly commit to selecting only those with high ethical conducts to be held responsible for their practices and the consequences of those practices (Griffin, 2008). According to Gomez-Mejia et al. (2004), the use of electronic monitoring has posed serious questions about how it may lead to a great deal of stress and dehumanizing effects on employees. The following is related to strategies that may reduce stress resulting from monitoring practices in organizations.

**Advice That Makes Monitoring Less Distressful**

First, Griffin (2008) succinctly presented causes and consequences of stress. Griffin elaborated that “organizational stressors” involve (a) task demands (i.e., rapid decisions, inadequate information for decisions, and critical decisions),
(b) physical demands including environmental factors (e.g., poor offices, temperature), (c) role demands (i.e., role conflict and role ambiguity), and (d) interpersonal demands (i.e., group pressures, leadership paradigms, and disharmony among individuals). Griffin added that the consequences of stress can be both positive and negative, and the negative ones involve behavioral, psychological, or medical matters. Logically, employee level of satisfaction, motivation, commitment, loyalty, and integrity in the workplace can be affected as a result of extreme levels of stress. The crucial point here is that the use of EPM has created a great deal of tension and pressure among individuals in organizations. Nelson and Quick (2006) made three recommendations that can help make electronic workplace monitoring less distressful. These include orientating employees about the monitoring system; setting fair performance standards; and using documentation, or records, for benign purposes rather than for sanctions. Alternatively, another school of thought articulated that reducing stress causes some problems for employers; thus, stress is recommended for healthy organizations and without it, employees lack energy (DeCenzo & Robbins, 2005). Schermerhorn (2011) also reflected that stress is comprised of two types: (a) "constructive stress," and sometimes called "eustress," is personally energizing and performance-enhancing, urges greater endeavors, inspires creativity, and enhances commitment, while still not devastating the individual or causing undesirable consequences, and (b) "destructive stress," which arises when there is a severe stress that may affect an individual’s physical and mental systems and lead to job burnout or aggressive behavior toward others in the workplace.

DeCenzo and Robbins (2005) discovered employee involvement and participation, making certain that employees are properly matched in their jobs and fully aware of the extent of their authority, and familiarizing them with what is expected are all factors that eliminate stress, conflict, and ambiguity in organizations. Similarly, two-way communication and employee involvement in the structural system or frame reduce stress and enhance perceptions of fairness or justice (Mathis & Jackson, 1997). However, we should differentiate between three types of organizational justice: (a) distributive justice—derived from the evaluation of the product of the business interactions; (b) procedural justice—derived from the procedures, or actions that generate the results; and (c) interactional justice—derived from the evaluation of the communication process used in business contacts (Ferrell, Fraedrich, & Ferrell, 2009).

Portolese-Dias and Shah (2009) noted that employers can listen to employees’ telephone communication, monitor e-mail in a search for clandestine trade, listen to harassing messages, monitor non-work related traffic, and monitor conflicts of interest. In short, to deal with the latent vulnerabilities where information technology (IT) negatively affects the satisfaction of employees, management needs to consider that employee satisfaction should be the highest priority and strategic objective (Thompson & Cats-Baril, 2003). Toward this end, privacy and security issues are contemporary challenges that IT individuals and businesspeople must confront and understand. Next, employee monitoring policies will be discussed.

**Employee Monitoring Policies**

The frequent anxiety in a monitored organization is generally not whether monitoring should take place, but how it should be performed, how the information should be utilized, and how feedback should be communicated to all individuals in the organization. However, employers should reduce ethical concerns by considering the following policies: (a) Voice-mail, e-mail, and computer files provided by the organization are solely for business purposes, (b) all computer passwords must be accessible to the employer, and (c) the employer has the right to monitor any practice without prior notification for business purposes only (Mathis & Jackson, 1997). DeCenzo and Robbins (2005) succinctly stated that whatever employers consider reasonable, they should proffer for employees in a written policy. The main theory behind communicating employers’ policies to all employees is that employees are more likely to accept electronic monitoring if their employers’ main purpose is to improve performance (Noe, Hollenbeck, Gerhart, & Wright, 2007).

Similarly, electronic monitoring seems preferable when policy statements create expectations of job performance in the mind of the employee (French, 1994). Thus, the best path for an organization planning to engage in employee monitoring involves open communication; formulating the appropriate monitoring policies and putting them into practice; and unequivocally stating how, when, and where the company monitors its employees (Baltzan & Phillips, 2009). In other words, Belcourt et al. (2008) informed that human resources experts and legal authorities strongly encourage employers to develop clear policies that elucidate how e-mail and the Internet are to be used, including when and under what circumstances employees can be monitored. Thus, employees could realize that the use of their organization’s Internet to shop, browse, view inappropriate webpages, or conduct personal business during work hours is an illegal action that is likely to cause undesirable consequences.

Moreover, Mello (2006, 2011) suggested that employers should develop a lucid and succinct policy and communicate it to all employees, if they choose to monitor their employees’ use of telecommunications equipment. Above and beyond, monitoring should be consistent with both the overall objectives of the organization and performance dilemmas; nonetheless, employers’ policies should not create stress and distrust on their employees. From a moral and legal perspective, employers need to consider the following tasks to minimize potential revelation to lawsuits: (a) develop an electronic communication policy, (b) notify employees and have them sign a consent form, and (c) rigorously...
implement every segment of the policy and monitor usage for business practices only (Mathis & Jackson, 2000). Another ethical dilemma is the balancing of improvements in productivity and efficiency versus dehumanization of the workplace (Thompson & Cats-Baril, 2003).

Not surprisingly, there are variations in how employers expect their employees to use computers in a working day; therefore, employees should be informed of the rules and consent to abide by them (Baltzan & Phillips, 2009). Nevertheless, people will continue to live on the edge of intolerable frustration and always be exasperated by computers as long as technology proposes alluring products and services (Odlyzko, 1999). Hence, the best path for an employer planning to be involved in employee monitoring is open communication surrounding the issue (Baltzan & Phillips, 2009). Moreover, Baltzan and Phillips enumerated the following policies:

- An information privacy policy includes general criteria regarding information privacy.
- “Acceptable use policy” (AUP) is a policy that a user must accept to pursue to gain access to a network, or the Internet.
- The development and implementation of an “e-mail privacy policy” allows employers to lessen various risks.
- “Internet use policy” involves guidelines in how to use the Internet properly.
- With an “anti-spam policy,” users are not allowed to send unwelcomed e-mails to others.

With the purpose of reducing ethical concerns, Mathis and Jackson (1997) claimed that employers should consider some policies. These include the following: electronic devices are provided by the employer for business purposes only, the use of such electronic devices for personal use is forbidden, all computer passwords must be in the hands of the employer, and the employer has the right to monitor such practices for business purposes without further notification. Quite simply, if the employer clarifies the purpose of electronic monitoring in the organization and links it to performance improvement, the employees are more likely to embrace such a policy (Noe, Hollenbeck, Gerhart, & Wright, 2007). Legal action appears most effective when employment processes and policy proclamations have aided in building expectations of job performance in the mentality of the employees (French, 1994). Finally, it is strongly recommended that employers distribute feedback on monitoring outcomes, to assist employees in improving their performance or to praise them for good performance. The following section involves reviewing policies and procedures in organizations.

Reviewing Policies and Procedures

To ascertain whether employees in an organization are following customary procedures, the next step is to review practices and implement curative actions if required. For example, a significant number of organizations conduct internal audits to measure current results against established objectives. Stair and Reynolds (2008, p. 387) recommended that people pose the following questions to specify whether present policies and procedures are satisfactory:

- Do current policies cover existing practices adequately? Were any problems or opportunities uncovered during monitoring?
- Does the organization plan any new activities in the future? If so, does it need new policies or procedures concerning who will handle them and what must be done?
- Are contingencies and disasters covered?

Answers to these questions are likely to assist and enhance a company’s performance and productivity, as well as being alert to unpredictable information that could have negative influences on the organization’s system. Hence, organizations should make a thorough effort to guarantee that all employees are responsive to existing policies, through formal training, for example (Baltzan & Phillips, 2009). Cascio and Aguinis (2011) shared that employers should thoroughly review their policies and acknowledge the following: (a) the number and types of documents an organization sustains concerning employees, former employees, and applicants; (b) the information preserved in each type of document or record; (c) the uses of information inside the organization; (d) the exposure made to the external environment (e.g., external stakeholders, suppliers, stockholders); and (e) the degree to which employees are familiar with and accredited of the utilization and exposure of information about them in the records department. In addition, and perhaps most importantly, Cascio and Aguinis advised employers to express, converse, and execute fair information-practice policies by the following means: gather information about individuals who are likely to have an influence on the organization’s decision; acknowledge the ways information is to be used by employers; advocate and champion practical methods for achieving accuracy, timeliness, and richness of information about employees; restrict the use of such records by applying security gauges; control information leakage to unauthorized parties; and ensure compliance with expressed fair information-practice policies. The last section in this article is a discussion about the role of human resource development (HRD) in employee assessment and development.

The Role of HRD in Employee Assessment and Development

This study focuses on ideas and competencies that can be associated with the HRD and human resource management (HRM) roles or functions in organizations. The author of this article believes that HRD is a field of study that emphasizes fundamental aspects of behavioral and developmental issues.
in organizations. In this sense, HRD efforts can be critical in monitoring employee behavior and performance in organizations. According to Megginson, Banfield, and Joy-Matthews (2001),

It is as important to know when a HRD response is appropriate to a particular situation as it is to recognize when it is not. The implementation of HRD strategies must, therefore, be based on a clear and accurate understanding of the problems and needs that require managerial action, and of what HRD can realistically contribute to these. (p. 134)

McGuire and Jorgensen (2011) noted that “the relationship of HRD with HRM has attracted some comment, although a consensus is emerging regarding the separate and distinct identity of HRD” (p. 9). They also added that it would be foolish to disavow that there are no relationships between HRM and HRD.

The literature used to argue the case in this article was drawn from areas that are pertinent to HRD, such as workplace productivity and organizational effectiveness; perceptions and rights of the organization’s employees; employee feedback, motivation, creativity, commitment, loyalty, integrity, and level of satisfaction; coaching and supervision to aid low performers at work; performance improvement provisions; employee involvement, development, and participation; irrelevancies or deficiencies in the organization’s system; and perceptions of fairness or justice in organizations. Evidently, the discussion of multifaceted topics concerning ethical or unethical behavior in organizations has become prominent in HRD literature in recent years (Ardichvili, Mitchell, & Jondle, 2009). Hence, HRD efforts could emphasize as well as protect the value of individual privacy in organizations and promote cherished organizational values. From a theoretical point of view, several questions extend the HRD field as it reflects on the impact of performance management systems in organizations (Buchner, 2007). Two of these questions were posed in this article to promote and stimulate further investigation and discussion. First, why do employers often recognize the value of installing sophisticated computer systems to perform more effectively, instead of spending time or money in developing the organization’s individuals? According to Megginson et al. (2001), thinking of HRD as an investment rather than a cost can help change mind-sets; however, spending time or money on developing an individual is often perceived as a cost. Second, do employers trust their employees in organizations? Effron, Gandossy, and Goldsmith (2003) noted that organizations that succeed are those that evoke our greatest human capacities: our need to be in good relationships and our desire to contribute to something beyond ourselves. These qualities cannot be evoked through procedures and policies; they are available only in organizations in which people feel trusted and welcome and in which people know that their work matters. (p. 194)

The purpose of some HRD factors is to tutor, develop, and educate individuals in organizations, with a vision to boost employee productivity and enhance organizational effectiveness (Metcalf & Rees, 2005). Another working definition is that HRD is concerned with the perceptions that organizations are human-made entities that count on human expertise to create and accomplish their objectives, and that HRD professionals are advocates of the organization’s individuals, work processes, and organizational integrity (Hassan, 2006). Likewise, the HRD function contributes to the preservation of the well-being of the organization as a social entity, and its support and development of the organization’s performance as an economic entity (Yorks, 2005). According to Garavan, McGuire, and O’Donnell (2004), HRD is a multidisciplinary construction with multiple perspectives. Therefore, HRD professionals are required to think differently, respond to new and unique problems, and use special lenses, as their jobs and duties become increasingly challenging (Garavan, O’Donnell, McGuire, & Watson, 2007). Similarly, Torraco and Swanson (1995) noted that

HRD serves a broad range of interests and outcomes in organizations. The primary purposes to be served by HRD can range from programs intended to meet the personal development needs of individuals (e.g., identifying individual learning styles or personal financial planning) to HRD programs necessary for everyone in the organization (e.g., programs addressing a new performance appraisal method or role changes secondary to structural reorganization. (p. 9)

A critical issue where HRD can provide valuable insight is the area of employee performance evaluation. Ethical commitment in performance evaluation will maintain integrity around the intricacy of learning and performance processes (Short, Bing, & Kehrhahn, 2003). A leader’s ability to act with integrity is crucial for building trust among individuals in organizations (Wooten & James, 2008). Interestingly, Hatcher (2002) argued that technology is driving the need for ethical HRD, because technology challenges our ethics and what we consider valuable. In addition, what technology can do in HRD can be perceived in terms of strategies in the full application of technology and the human need for personal connection (R. A. Swanson & Holton, 2001). Moreover, HRD professionals must guarantee that both human (employees) and technological processes (monitoring through the use of technology) work effectively and in line with the overall organizational strategies.

More importantly, to play a primary role in promoting ethical business cultures, HRD will need to thoroughly engage in a system of interrelated and well-coordinated activities (Ardichvili & Jondle, 2009). This includes the amalgamation of ethics in leadership development programs that promote ethical culture, and strengthen ethical decision-making skills and review of codes of ethics, as illustrated earlier in this article. In addition, because the practice of HRD involves enlightening the workforce to actively participate in the marketplace,
HRD as a domain has a chance to approach leadership development and culture in the current global economy (Kowske & Anthony, 2007).

Noticeably, HRD studies should inspire organizations how to maintain the psychological well-being of their employees and examine the following questions that concern the organization’s employees’ well-being: (a) What makes people happy in their organizations? and (b) What is a good architecture for HRD programs that should stimulate passion and energy among the workforce? (Van der Sluis, 2007). Thus, employers should recognize employee rights, determine an individual’s contribution to the organization, inform employees how well they are performing their tasks, reveal their criteria in their performance management system, and provide ongoing feedback on the employees’ performance, as well as coaching and supervising low performers on a regular basis. It is also recommended that an HRD professional’s first challenge is to cautiously investigate the performance dilemma and to build a diagnostic framework. Yorks (2005) thoroughly interpreted how to build the diagnostic framework as follows: (a) describing the problematic performance state (e.g., what has been occurring based on data and observation without any analysis), (b) identifying symptoms (e.g., critical incidents and behaviors related to the situation), (c) identifying the problem (e.g., determine the source of the symptoms), and finally (d) matching the solution to the problem. In short, HRD performs significant role in improving employee performance and looks at making the organizational system more effective through a plethora of tactics (McGuire & Jorgensen, 2011).

Following this line of thought, and the various definitions of HRD capabilities, the author of this article comfortably justifies that HRD efforts and contributions in monitoring employee behavior and performance can stimulate and develop numerous aspects of the workforce, in line with the organization’s goals, without encroaching on individuals’ privacy.

**Recommendations for Further Studies**

Further studies may explore the most effective leadership styles, traits, and behaviors required to monitor employee performance using technology in organizations. It would also be useful if we could realize how far employers should go concerning monitoring employee behavior in organizations. Another significant issue that can be explored in future studies is the cost associated with the use of software and technological devices to monitor employee performance. Practitioners may also need to be aware of what kind of software packages can be the most relevant to particular projects in small, medium, and large organizations. In addition, DeCenzo and Robbins (2005) found that there are a number of questions that remained unanswered in various studies, such as the following:

1. How much should managers know about their employees and how far should they go in controlling their behavior in and out the workplace?
2. When does an employer’s need for information about employee performance invade an employee’s right to privacy?
3. Do employers have the right to monitor whatever they want as long as employees are notified in advance that they will be monitored?
4. What about the delimitation or the boundary between monitoring work and non-work behavior?
5. Do employers have the right to monitor their employees at home during evenings and weekends?

Further studies may explore social media, smart phones, tablets, or other devices raising monitoring dilemmas in today’s workplace. Finally, future studies may postulate how organizations can measure their return on investment (ROI) in electronic devices and how much is enough to implement a technology venture in organizations.

**Conclusion**

By monitoring, employers often argue that they are able to protect their organizations from any harm. In this sense, monitoring is perceived as a tool to maintain the security of an organization. New technologies have not only offered organizations reasons to monitor employees’ behavior, but these technologies have also provided new methods and techniques to perform employee monitoring. Thus, technology must be treated with caution and discretion. Employers should realize that employees may retaliate against the organization for the perceived unfair monitoring practices. Therefore, it is essential when applying new technologies to monitor employee behavior to take into account many concerns (e.g., privacy, needs, and aspirations). Educating employees about the reasons behind monitoring them, developing a wide range of policies and procedures, and communicating them effectively will be vital to successfully implement a monitoring system.

The failure of employers to recognize employee rights can cause extensive loss, such as expensive lawsuits, damage to the organization’s reputation, and impairment of employee values. Hence, employers should balance the need for productivity with regard to employee rights to privacy, safety, and security. Focusing on accomplishments rather than time spent in the workplace should be the main concern for any employer. In other words, there is no need to police a workforce because no one can work 8 hr without breaks, and a culture of disloyalty and distrust within the organization may emerge. However, employees should be aware that there are numerous software packages that could key log everything they type, search, and read on their computers.

This study offers many alternatives to EPM that are likely to satisfy an employer’s objectives without violating rights
of privacy. Another significant issue raised in this study is that the most effective leadership style to monitor employee performance and behavior through technology remains unidentified. From the author’s point of view, there is no need to define what a moral behavior is in mature and healthy organizations, but it is crucial to shed light on how to use technologies without violating ethical protocols. Technology is a tool that can be used ethically and unethically. After reviewing a large number of studies on employee perceptions of electronic monitoring, the author found that the use of EPM has created a great deal of tension and pressure among individuals in organizations. Therefore, the author argued that employee level of satisfaction, motivation, commitment, loyalty, and integrity in the workplace can be affected as a result of extreme levels of stress. Hence, educating employees about the monitoring system and setting fair performance criteria, distributive justice, procedural justice, and interactional justice can make monitoring less distressful. Importantly, monitoring should be consistent with both the overall objectives of the organization and performance dilemmas; however, employers’ policies should not create stress and distrust on their employees. Above and beyond, the author of this study argued that HRD efforts can be significant in monitoring employee behavior and performance in organizations. The rationale behind this school of thought is that HRD field emphasizes crucial elements of behavioral and developmental matters in organizations.

Acknowledgment

The author of this article wants to offer his sincere appreciation to the editor and the peer reviewers for their valuable advice and suggestions.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

References

Alampay, E. A., & Hechanova, R. M. (2010). Monitoring employee use of the Internet in Philippine organizations. The Electronic Journal on Information Systems in Developing Countries, 40(5), 1-20. Retrieved from http://www.ejisdc.org/Ojs2/index.php/ejisdc/article/viewFile/648/311
Anton, G., & Ward, J. J. (1998). Every breath you take: Employee privacy rights in the workplace—An Orwellian prophecy come true? Labor Law Journal, 49, 897-911.
Ardichvili, A., & Jondle, D. (2009). Integrative literature review: Ethical business cultures: A literature review and implications for HRD. Human Resource Development Review, 8, 223-244.
Ardichvili, A., Mitchell, J. A., & Jondle, D. (2009). Characteristics of ethical business cultures. Journal of Business Ethics, 85, 445-451. Retrieved from http://files.eric.ed.gov/fulltext/ED501640.pdf
Baltzan, P., & Phillips, A. (2009). Essentials of business driven information systems. Burr Ridge, IL: McGraw-Hill/Irwin.
Barrett, S. (2008). Monitoring raises privacy issues. Employee Benefits, 48-51. Retrieved from http://connection.ebscohost.com/com/c/articles/32800523/monitoring-raises-privacy-issues
Bartol, K. M., & Martin, D. C. (1991). Management. New York, NY: McGraw-Hill.
Baye, M. R. (2009). Managerial economics and business strategy (6th ed.). New York, NY: McGraw-Hill/Irwin.
Belcourt, M., Bohlander, G., & Snell, S. (2008). Managing human resources (Fifth Canadian ed.). Toronto, Ontario, Canada: Nelson.
Bennett, S. C., & Locke, S. D. (1998). Privacy in the workplace: A practical primer. Labor Law Journal, 49, 781-787.
Bohlander, G., & Snell, S. (2004). Managing human resources (13th ed.). Mason, OH: South-Western.
Buchner, T. W. (2007). Performance management theory: A look from the performer’s perspective with implications for HRD. Human Resource Development International, 10, 59-73.
The Bureau of National Affairs. (2012). Attorneys worldwide discuss right to monitor, track workers. HR Focus, 89(11), 8-9.
Cascio, W. F., & Aguinis, H. (2011). Applied psychology in human resource management (7th ed.). Harlow, UK: Pearson Education.
Certo, S. C., & Certo, S. T. (2009). Modern concepts and skills management (11th ed.). Harlow, UK: Pearson Education.
Ciocchetti, C. A. (2011). The eavesdropping employer: A twenty-first century framework for employee monitoring. American Business Law Journal, 48, 285-369.
Conlon, K. J. (1997). Privacy in the workplace. Labor Law Journal, 48, 444-448.
Cowan, S. (2008). When private means private: The “do’s and don’ts” of employee monitoring. Credit Management, 16. Retrieved from http://connection.ebscohost.com/c/articles/28334301/when-private-means-private-dos-donts-employee-monitoring
DeCenzo, D. A., & Robbins, S. P. (2005). Fundamentals of human resource management (8th ed.). New Delhi, India: John Wiley.
Dessler, G. (2000). Human resource management (8th ed.). Upper Saddle River, NJ: Prentice Hall.
Dessler, G. (2003). Human resource management (9th ed.). Harlow, UK: Pearson Education.
Dessler, G. (2011). Human resource management (12th ed.). Harlow, UK: Pearson Education.
Dillon, T. W., & Thomas, D. S. (2006). Knowledge of privacy, personal use, and administrative oversight of office computers and e-mail in the workplace. Information technology. Learning & Performance Journal, 24(2), 23-34.
Dlabay, L. R., Burrow, J. L., & Eggland, S. A. (2006). Intro to business (6th ed.). Mason, OH: South-Western.
DuBrin, A. J. (2006). Essentials of management (7th ed.). Mason, OH: South-Western.
DuBrin, A. J. (2009). Essentials of management (8th ed.). Mason, OH: South-Western.
Effron, M., Gandossy, R., & Goldsmith, M. (2003). Human resources in the 21st century. Hoboken, NJ: John Wiley.
Everett, A. M., Wong, Y. Y., & Paynter, J. (2006). Balancing employee and employer rights: An international comparison...
of e-mail privacy in the workplace. *Individual Employment Rights, 17*, 291-310.

Ferrell, O. C., Fraedrich, J., & Ferrell, L. (2009). *Business ethics: Ethical decision making and cases* (7th ed.). Mason, OH: South-Western.

Ferrell, O. C., Fraedrich, J., & Ferrell, L. (2009). *Business ethics: Ethical decision making and cases* (7th ed.). Mason, OH: South-Western.

French, W. L. (1994). *Human resources management* (3rd ed.). Boston, MA: Houghton Mifflin.

Garavan, T. N., McGuire, D., & O’Donnell, D. (2004). Exploring human resource development: A levels of analysis approach. *Human Resource Development Review, 3*, 417-441. Retrieved from http://eresearch.qmu.ac.uk/270/1/270.pdf

Garavan, T. N., O’Donnell, D., McGuire, D., & Watson, S. (2007). Exploring perspectives on human resource development: An introduction. *Advances in Developing Human Resources, 9*, 3-11. Retrieved from http://eresearch.qmu.ac.uk/262/1/262.pdf

Gomez-Mejia, L. R., Balkin, D. B., & Cardy, R. L. (2004). *Managing human resources* (4th ed.). Harlow, UK: Pearson Education.

Griffin, R. W. (2008). *Management* (9th ed.). Lewiston, NY: Houghton Mifflin.

Graeff, F. H., Kuechler, W., & Sweeney, S. (2002). Dealing with data privacy protection: An issue for the 21st century. *Information Systems Management, 19*(4), 61-70.

Guffey, C. J., & West, J. F. (1996). *Employee privacy: Legal implications for managers*. *Labor Law Journal, 47*, 735-745.

Haag, S., & Cummings, M. (2010). *Management information systems for the information age* (8th ed.). Boston, MA: McGraw-Hill.

Haller, S. C. (2002). Privacy: What every manager should know. *Information Management Journal, 36*, 33-40.

Hames, D. S., & Diersen, N. (1991). The common law right to privacy: Another incursion into employers’ rights to manage their employees? *Labor Law Journal, 42*, 757-765.

Hassan, A. (2006, December 2-5). Human resource development and organizational values. Proceeding of the 2006 Asian Conference of the Academy of Human Resource Development (AHRD), Putrajaya, Malaysia.

Hatcher, T. G. (2002). *Ethics and HRD: A new approach to leading responsible organizations*. New York, NY: Basic Books.

Jackson, S. E., Schuler, R. S., & Werner, S. (2009). *Managing human resources* (10th ed.). Mason, OH: South-Western.

Kovach, K. A., Jordan, J., Tansey, K., & Framinan, E. (2000). The balance between employee privacy and employer interests. *Business and Society Review, 105*, 289-298.

Kowske, B. J., & Anthony, K. (2007). Towards defining leadership competence around the world: What mid-level managers need to know in twelve countries. *Human Resource Development International, 10*, 21-41.

Luthans, F., & Doh, J. P. (2009). *International management: Culture, strategy, and behavior* (7th ed.). New York, NY: McGraw-Hill/Irwin.

Mathis, R. L., & Jackson, J. H. (1997). *Human resource management* (8th ed.). Minneapolis, MN: West Publishing.

Mathis, R. L., & Jackson, J. H. (2000). *Human resource management* (9th ed.). Mason, OH: South-Western.

McCalman, J., & Paton, R. A. (1992). *Change management: A guide to effective implementation*. London, England: Paul Chapman.

McGuire, D., & Jorgensen, K. M. (2011). *Human resource development: Theory and practice*. Thousand Oaks, CA: SAGE.
Van der Sluis, L. E. C. (2007). Umbrella for research into human resource development (HRD). *Human Resource Development International, 10*, 99-106.

Vaught, B. C., Taylor, R. E., & Vaught, S. F. (2000). The attitudes of managers regarding the electronic monitoring of employee behavior: Procedural and ethical considerations. *American Business Review, 18*, 107-114.

Wen, H. J., Schwieger, D., & Gershuny, P. (2007). Internet usage monitoring in the workplace: Its legal challenges and implementation strategies. *Information Systems Management, 24*, 185-196.

Wooten, L. P., & James, E. H. (2008). Linking crisis management and leadership competencies: The role of human resource development. *Advances in Developing Human Resources, 10*, 352-379. Retrieved from http://karshenasanrasmi.ir/Editor/UploadFiles/PDF%20Articles/352.pdf

Yorks, L. (2005). *Strategic human resource development*. Mason, OH: South-Western.

Zachary, M. K. (2013). Invasion of privacy: The moment of intrusion. *Supervision, 74*, 18-22.

**Author Biography**

**Mahmoud Moussa** is a lecturer at the International Business Management Program (IBM), Faculty of Business Administration and Liberal Arts in Rajamangala University of Technology Lanna (RMUTL), Chiang Mai, Thailand. He is also a member of the editorial board at *Emerald Emerging Markets Case Studies (EEMCS) Journal*, Emerald Group Publishing. He comes from Egypt and has been working and studying in Thailand for the last 8 years. He holds a BA from Helwan University (majoring in arts of philosophy) Cairo, Egypt, and an MA in the international graduate studies programs from Burapha University, Chonburi, Thailand (majoring in Human Resources Development). He has conducted research and published extensively on human–computer interaction, attitudes and perceptions of interactions within organizations, cross-cultural management, HRD, and HRM. His current research interest involves education trends in the Association of Southeast Asian Nations (ASEAN) in the ASEAN Economic Community (AEC) era.