2021

Effects of Employee Monitoring Notification Policies on HR Manager Opinions

Gundars Kaupins
Boise State University

Online Journal of Applied Knowledge Management
A Publication of the International Institute for Applied Knowledge Management

Volume 9, Issue 1, 2021

Effects of employee monitoring notification policies on HR manager opinions

Gundars Kaupins, Boise State University, USA, gkaupins@boisestate.edu

Abstract

As a variety of electronic monitoring methods such as global positioning systems are available, monitoring employees without notice is a consideration even though several laws ban it and ethical questions remain. Monitoring without notice has risks that Human Resources (HR) managers should consider when they set monitoring policies to enhance knowledge management. A total of 174 HR managers were asked about their top reasons to electronically monitor employees with or without notice. About half received information that a company did not notify employees of electronic monitoring and the other half received the opposite information. Prospect theory was the basis for collecting data to understand the importance of risk in setting policies. It states that people in perceived good conditions avoid risk because they feel there is more to lose than to gain. The leading reason to electronically monitor employees for both groups was computer virus and malware protection. Organizational threats associated with legal issues showed more HR support for monitoring without notice. Opportunities associated with employee productivity indicated relatively more support for monitoring with notice. As a result of this research, perceived threats in the workplace are significant reasons why HR managers might not provide notice of monitoring in the workplace. This has potential legal and ethical implications.

Keywords: Monitoring, notification, prospect theory, privacy policies, threats, opportunities.

Introduction

Electronic monitoring of employees is the umbrella term for collecting information about employees using electronic devices and not direct observation (Ofman & Sagandykov, 2020). Most employee electronic monitoring is not secret. About 80% of large enterprises in general openly monitor employees' phones, e-mails, and the Internet. About 94 percent openly monitor sensitive data access (Noll, 2018). To do such monitoring, a variety of methods can potentially lead to violations of employee privacy. They include e-mail and text message content analysis, Global Positioning Systems, artificial intelligence, Radio Frequency Identification Tags, keystroke and search engine monitoring, drones, and video and audio surveillance (Ciocchetti, 2011). As such monitoring can be hidden from employees, customers, vendors, or anyone else associated with the organization, neither the American federal government nor its states have established clear laws governing secret surveillance in the workplace. Although the Federal Wiretap Act of 1968 prohibits eavesdropping of phone conversations without court approval unless one of the parties consents, the Electronic Communications Privacy Act (ECPA) of 1986 permits employers to clandestinely hear job-related conversations. Employers then have the freedom to listen to any phone conversations because an employer can contend that it takes several minutes to decide whether a conversation is personal or job-related (ACLU, 2020). Along with legal limitations, there are ethical issues associated with privacy violations. Employers could obtain nonwork-related information about employees without their knowledge and act inappropriately by making false claims, sharing embarrassing information, and harassing, demoting, or firing the employee. Monitoring might go too far if individuals consider it unfair or not needed for the common good. It may violate human rights by hurting the employees' quality of life and treating employees similarly to property (West & Bowman, 2016). Mutual respect might be eroded (Hodson et al., 1999). Individuals see electronic monitoring as fairer if there is advance notice (Hovorka-Mead et al., 2002). With all of the legal and ethical issues, organizations can be tempted to disregard them because monitoring employees without notice can be done easily. Cameras are becoming smaller, location monitoring devices can go inside bodies, and many programs can monitor each employee's keystroke. Understanding organizational motivations to monitor employees without notice might be part of the means to limit such monitoring (Gheorghe, 2017; Rosenberg, 2010).

Rationale for the Paper

HR managers are at the forefront of creating policies associated with notifications and methods of employee surveillance. Notifications involve providing employees information about why surveillance will be used and how the data will be collected. Some methods of notification may include e-mail, privacy policies, employee handbooks, and training on the subject (Yerby, 2013). One role of HR managers is to facilitate the development and use of employee monitoring systems that can support knowledge management in enhancing productivity and reducing financial and physical threats in the workplace (Yerby, 2013) as well as minimize knowledge management risks (Durst & Zieba, 2019). They can set policies to observe, receive and otherwise obtain information from all relevant sources in HR-related matters (Society for Human Resource Management, 2020; U. S. Department of Labor, 2019). Given the legal and ethical implications of secret monitoring, knowing in what situations HR managers decide to not notify or notify employees that they are being electronically monitored can be useful on several fronts. This information also might help human research managers, researchers, and policymakers eventually understand the motivation and patterns behind secret surveillance (Edwards et al., 2018). Knowing the motivations can lead to legislation to manage, reduce or provide justification for covert practices (Gheorghe, 2017; Hugl, 2013), develop transparent organizational privacy policies (Cox et al., 2015), and gain appropriate knowledge exchanges and trust associated with corporate security measures and intensive employee monitoring organizations (Durst & Zieba, 2019). This paper's main contribution to filling a gap in the knowledge management literature is understanding how human resource managers who receive information that monitoring is done with notice or without notice will consider opportunity enhancement or risk reduction as a reason to monitor employees. The unique and exploratory nature of the paper investigates a wide variety of situations not covered by prior research such as the relationship between employee time(clock) keeping and monitoring notification. Some other situations include increasing opportunities to enhance corporate productivity and the work environment and decreasing corporate threats such as loss of property and computer viruses.

Literature Review

Prior research has focused on managerial perceptions of employees that affect overt and secret electronic monitoring. Such research has found that managers are more likely to do secret monitoring when they have a high dependence on their employees and their trust level is low (Alge et al., 2004). Perceptions of electronic monitoring can be a function of the perceived fairness of the system and employee performance (Moorman, & Wells, 2003), the role of culture, job competition, consistency, prior experience with monitoring, time to deal with monitoring problems, and amount of control desired (Al-Hitmi & Sherif, 2018), policy violations (Zweig, & Scott, 2007), perceived privacy violations, procedural justice, leave intentions (Hung-Yue, 2018), and perceived organizational justice (Stanton, 2000). Prospect theory was chosen as the lens of analysis for this research as it appears to relate to the rationale for electronic notifications and no notifications. It states that people in perceived gain conditions avoid risk because they feel there is more to lose than to gain. If people are faced with decisions that might lead to gains, they would be averse to risk (Fox & Tversky, 1995; Kahneman & Tversky, 1979). In the context of prospect theory, not notifying employees about electronic monitoring might be risky because of potential legal problems, ethical issues, and employee complaints about secrecy. If there are gain conditions in which the focus is on opportunities rather than threats, no notice of monitoring might be too much of a risk. In contrast, people in perceived losing conditions find more risky activities acceptable because they feel there is less to lose (Fiegenbaum & Thomas, 1988). Not notifying employees of electronic monitoring might be more acceptable to reduce threats in the workplace. Secrets tend to form to avoid disapproval (Vrij et al., 2002). For example, secret surveillance of potential violence in the workplace might reduce liability. Violent acts are recorded and the employee(s) who committed such acts might have less defense. The company might not be liable for the acts of an individual. A reason for keeping monitoring secret is to reduce threats of negative events. Threats are defined as "Any menace of such a nature and extent as to unsettle the mind of the person on whom it operates, and to take away from his acts that free voluntary action which alone constitutes consent" (R. v Keegstra, 1990, p. 829). A threat is the anticipation of harm. It is a psychological condition that is an interpretation of a situation by an individual (Baldwin, 1971; Lazarus, 1968). Threats can be known by the salience of lost risk. The proneness to quick action to reduce anxiety can lead to reduced emphasis on ethical reasoning and therefore there might be a focus on one's own needs (Chattopadhyay et al., 2001). Threats tend to get people to focus on their own needs (Mead et al., 2009). They overlook prosocial goals to enhance self-interest (Sheldon & Kasser, 2008). If some personal activities are revealed, then negative actions by others or internal anxiety might occur. Some events that might not be shared involve lies, financial impropriety, violations of trust, discontent at work, sexual behavior, theft, violations of trust, self-harm, and addictions (Slepian et al., 2017; Slepian et al., 2012). According to Jackson and Dutton (1988), threats can be distinguished from opportunities due to significant negative connotations of not dealing with threats. Organizations should be protected from threats through reduction, control, or elimination. Threats should be reduced and controlled. While threats have clearer negative connotations, opportunities are more linked with positive, "my win" can be "your win," and a means to resolve issues. Individuals feel more in control. However, threats and opportunities have some similar characteristics such as the need for urgency, difficulty, and large stakes.

Threat-Based Organizational Monitoring

With Notice

Though examples of threat-based organizational monitoring without notice exist, there is considerably more research on why organizational monitoring with notice occurs. The list in Table 1 focuses on research for monitoring with notice. The research comes from a variety of academic, empirical, and anecdotal studies associated with monitoring employees that focus on aspects of an organization that need to be protected or reduced. Keywords such as monitoring, surveillance, privacy, notification, employees, and legal were used. Some of the list covers legal issues such as reducing audit, compliance, and copyright problems. Information security is involved with the leakage of financial, personal, and confidential information. The largest group of studies focus on minimizing poor employee behaviors such as abuse, sexual harassment, and turnover. Use of financial data, intellectual property, and confidential information are among several topics covered that are related to processes associated with supporting knowledge management.

Without Notice

There are examples of threat-related reasons for monitoring without notice in Federal, state, and for-profit organizations. Federal reasons for electronic surveillance without notice tend to focus on issues such as safety, security, intellectual property protection, and crime prevention. The United States government has been secretly monitoring journalists at the Mexican border as part of a national security investigation. Marshals in the United States have been monitoring airline passengers who raise red flags such as frequently going to the restroom (Ryan & Halsey III, 2018).

On the state and local level, a University of California Berkeley monitoring kit secretly captures and analyzes all network traffic coming in and out of the campus (Thomson, 2016). A Kentucky attorney general requested that the Lexington police department release records of its secret surveillance cameras. The department continues to provide arguments to hide information from the state government (Duke, 2018). Corporate examples of secret surveillance exist. Shook et al. (n.d.) noted that about 55% of companies admit they haven't asked for anyone's permission to monitor employees from a sample of 1400 C-Suite executives. Though published corporate examples of no notice have not frequently appeared, Google employees have accused its management that it has developed a secret internal surveillance tool to monitor their attempts to organize protests and talk about labor rights even though Google says it is used to stop calendar and meeting spam (Epstein, 2013). Coicchetti (2011) mentioned that often GPS and RFID trackers can be covertly placed on company equipment such as cars and cell phones, and directly on employees as risky moves that reduce theft.

Table 1. Threat-Based Research of Reasons for Employee Monitoring With Notice

Reduced legal problems
1. Illegal operations (Amesen & Weis, 2007; Burns, 2019).
2. Liability protection (Nikolaev, 2018; Smith & Tabak, 2017).
3. Sex discrimination (Cioccetti, 2011; Lewis & Gardner, 2000; Miller, 2019).
4. Audit and compliance problems (Noil, 2018).
5. Employee fines and imprisonment (Kohen, 2018).
6. Crime in general (Cioccetti, 2011).
7. Accident reduction (Katz, 2015; Coiccetti, 2011; LaMarco, 2019)
8. Copyright infringement (Dorval, 2004).
9. Possession of weapons (Lewis & Gardner, 2000).

10. Drug and alcohol use (Lewis & Gardner, 2000).
Reduced leakage of information
1. Leakage of trade secrets (Cioccetti, 2011; Friedman & Reed, 2007; Rosenberg, 1999). 2. Misuse of intellectual property (Amesen & Weis, 2007; Friedman & Reed, 2007; Rosenberg, 1999). 3. Leakage of financial data (credit card numbers, Social Security numbers, etc.) (Amesen & Weis, 2007; Cioccetti, 2011). 4. Leakage of personal data (Cioccetti, 2011; "Electronic Business Communications," 2009; Noil, 2018). 5. Leakage of confidential information (Cioccetti, 2011; LaMarco, 2019). 6. Theft protection (Noil, 2018). 7. Insider threat protection (Noil, 2018). 8. Spyware (Amesen & Weis, 2007).
Reduced employee behavioral issues
1. Workplace violence (Cioccetti, 2011; Lewis & Gardner, 2000; Whitfield, 2013). 2. Abusive behavior reduction (Ekramsystem.com, 2017; Miller, 2019; Schwartz, 2015) 3. False rumors (Schwartz, 2015). 4. Inappropriate access to the Internet (Amesen & Weis, 2007; Noil, 2018). 5. Distractions (Katz, 2015; Schwartz, 2015). 6. Personal use of business resources (McDonald & Thompson, 2016; Schwartz, 2015; Thomas et al., 2014) 7. Turnover and absenteeism (Lewis & Gardner, 2000; Whitfield, 2013). 8. Misuse of time (Amesen & Weis, 2007; Cioccetti, 2011; LaMarco, 2019; Miller, 2019; Schwartz, 2015).
Other
1. Cost reduction (Amesen & Weis, 2007). 2. Computer viruses (Amesen & Weis, 2007; Cioccetti, 2011; Noil, 2018)

Opportunity-Based Research on Organizational Monitoring

But threats are only a part of why monitoring with or without notice might occur. Most companies monitor employees for either information security or to enhance productivity as part of customer service or quality improvement programs (Bolton, 2001). Opportunities are positive events that, if pursued, can lead to positive outcomes (Bush, 2016). This relates to the relationship between monitoring and knowledge management. Demarest (1997) mentions that knowledge management involves a group of processes and systems that benefit an organization's value creation. Monitoring processes can support the firm's value-creating activities by collecting data involving productivity, opportunities, and threats. Monitoring also relates to the knowledge management infrastructure. Monitoring might enhance the effectiveness of the value creation process by indicating possible opportunities for improved performance.

With Notice

Research showing opportunities involving monitoring with notice is more frequent than without notice. Opportunities are good aspects of an organization that should be enhanced. Table 2 focuses on opportunity-based research with notice. Leading examples of such research include improved corporate results such as productivity and profitability, improved processes such as performance appraisals, timekeeping, budget handling, and client billing, and improved employee focus such as a better work environment, flexible work schedules, and employee wellbeing.

Without Notice

On the surface, the secret monitoring of employees to help with productivity and fairness seems odd. How would employees change their behavior if they do not know that they are being observed? If employees perceive no one is watching them, there might be little motivation to change behavior. On the other hand, secret monitoring might be beneficial to increase productivity and employee health. Being monitored can create greater stress, higher boredom levels, psychological tension, depression, anger, heart difficulties, and anxiety among employees (Smith et al., 1992). Performance can be enhanced with secret shopper programs. Such programs involve users of a product or service to create a full report about both the good and bad of the organization. One secret shopper program focused on enhancing collective engagement to secure competitive advantage through secret shoppers (Eldor, 2018).

Hypotheses

Though the lists of threats and opportunities are not comprehensive, they indicate the many reasons why employers might monitor employees with or without notification. Will human resource managers provide different reasons for monitoring if there is a notice or no notice of the monitoring? This may eventually lead to discovering motivations for secret surveillance. Prospect theory provides the basis for two hypotheses. Threats might lead individuals to do riskier behavior related to monitoring without notice. Opportunities might lead individuals to be less willing to do riskier behavior. No notices are related to riskier behavior because of ethical and legal problems. Threats focus on aspects of an organization that should be reduced or protected. Opportunities are aspects of an organization that should be enhanced. As Jackson and Dutton (1988) indicated, threats and opportunities are not necessarily opposites of each other and may be viewed as a continuum (partially threats, partially opportunities). As a result, the hypotheses are analyzed on an exploratory basis.

Table 2. Opportunity-Based Research of Reasons for Employee Monitoring

Employee improvement
1. Productivity (Cioccetti, 2011; LaMarco, 2019; Lewis & Gardner, 2000; McParland & Connolly, 2019; Nicolaev, 2018; Noil, 2018; Vessella, 2015; Whitfield, 2013;). 2. Employee effectiveness (Amesen & Weis, 2007; Cioccetti, 2011; McParland & Connolly, 2019). 3. Learning (Burns, 2019; Vessella, 2015,). 4. Employee privacy (Balfanz et al., 2016). 5. Personal productivity (Kohen, 2018). 6. Flexible work schedule (Kohen, 2018). 7. Employee wellness (Kohen, 2018).
Employee and employer relationships
1. The degree to which employees identify with the organization (Alder & Tompkins, 1997). 2. Timekeeping simplification (Cioccetti, 2011; Ekransystem.com, 2017; Katz, 2015; Miller, 2019). 3. Learn how employees can work best (Cioccetti, 2011) 4. Attract new job applicants (Fombrun, 1996; Roberts & Dowling, 2002; Turban & Greening, 1997). 5. Handle employees fairly (LaMarco, 2019). 6. Employer and employee relationships (LaMarco, 2019). 7. Performance appraisals (Katz, 2015; LaMarco, 2019; Noil, 2018). 8. Work environment (Cioccetti, 2011). 9. Training tool (Burns, 2019; Katz, 2015). 10. Perceptions of organizational justice through better investigations (Alder & Tompkins, 1997; Burns, 2019).
Organizational results
1. Profitability (Amesen & Weis, 2007). 2. Activities for business purposes only (McDonald & Thompson, 2016; Thomas et al., 2014). 3. Process improvement (McParland & Connolly, 2019). 4. Innovation (McParland & Connolly, 2019).

5. Quality customer service (Levy, 2018, Miller, 2019).
6. Budget handling (Vessella, 2015).
7. Reputation (Ettenson & Knowles, 2008).
8. Client billing accuracy (Vesella, 2015).
9. Consumer-friendly prices (Fombrun, 1996; Roberts & Dowling, 2002; Turban & Greening, 1997).

H1: HR managers who receive information that monitoring is done without notice (independent variable) will consider aspects of the organization that should be protected or reduced (dependent variables) as a reason to monitor more than HR managers who receive information that monitoring is done with notice. The hypothesis is analyzed on a variable-by-variable basis. For example, computer virus/malware protection is categorized as a threat due to its negative connotations and use of the words "protect" or "reduce." As a labeled threat, the hypothesis is that computer virus/malware protection will be considered as a reason to monitor without notice more than the "with notice" condition.

H2: HR managers who receive information that monitoring is done with notice (independent variable) will consider opportunity enhancement as a reason to monitor (dependent variables) more than HR managers who receive information that monitoring is done without notice. This hypothesis also is analyzed on an exploratory variable-by-variable basis.

Methodology

Sample

Total 174 members of the Society for Human Resource Management (SHRM) chapters in Texas responded to a survey covering HR managers' perceptions of their employer's monitoring activities. The society provides networking, education, and advocacy services for the HR profession throughout the world. The Texas locations are a convenience sample due to adequate access to sufficient numbers of human resource managers. Local chapters surveyed include Abilene, Amarillo, Brownsville, Dallas, Fort Worth, San Antonio, and Wichita Falls. The respondents completed a paper survey and submitted their responses at the end of their monthly meeting. Though total chapter meeting attendance counts were not calculated, roughly 40 percent of attendees completed the survey. Data was collected by Malcolm Coco from the Fall of 2016 to the Fall of 2017 as part of a larger study on monitoring locations not related to the current research.

The surveys were split between the monitoring with no notice and monitoring with notice. In both cases, "no notice" and "with notice" were shown in bold and all-caps on separate lines. A copy of the "with notice" survey is shown in the appendix. That survey also provided questions used in another study that showed non-experimental results (Kaupins & Coco, 2017). The sample was about 75% female. This corresponds to the national average of about 75% for human resource managers based on the Bureau of Labor Statistics (Torpey, 2017). The mode age of the respondents was 35-44 with the majority under 44. About 60% came from companies with under 500 employees. Roughly 80% of their organizations monitored their employees and 42% did not give notice of monitoring.

Survey

The 28 threats and 26 opportunities listed in the literature review were narrowed down to 18 variables (nine threats and nine opportunities) shown in Table 3. The nine threats involve aspects of an organization that should be protected, reduced, or prevented. The nine opportunities involve aspects of an organization that should be enhanced. Some of the threats and opportunities from the literature were reduced to one variable due to similar wording (e.g., productivity and personal productivity; perceptions of organized justice and handling employees fairly; learning how employees work best and process improvement). Others were eliminated based on pretesting with undergraduate students. They received a survey that asked them to mark what are their top five reasons to support employee monitoring. Reasons (possible variables) receiving the fewest or no marks were eliminated from the study. Those variables might not be in the top five of the HR managers' survey and therefore would have insufficient variance and information power. Information power can be increased by incorporating a sample of participants who have characteristics and experiences (e.g., human resource management) and variables more relevant to the study (Malterud et al., 2015).

Table 3. List of Threats and Opportunities

Threats	Opportunities
Liability Protection	Employee Productivity
Legal Requirement Satisfaction	Learning How Employees Work Best
Computer Virus/Malware Protection	Timekeeping Simplification
Property Protection	Product or Service Quality
Crime Prevention	Professionalism
Employee Safety	Employee Wellness
Cost Reduction	Performance Evaluation Quality
Employee Privacy	Fairness in Handling Employees
Employee Protection	Innovation

Results

Table 4 shows the correlations between the nine threats and nine opportunities. It showed 37 significant correlations based on 171 possible. The highest was 0.456 ($p < 0.01$) between learning how employees work best and innovation. The next highest was -0.419 ($p < 0.01$) between computer virus/malware protection and performance evaluation quality. The variable that correlated (at least $p < 0.05$) with the most variables was professionalism/reputation with satisfying legal requirements, property protection, employee productivity, employee wellness, and liability protection. Though there were 29 significant correlations at $p < 0.01$, none other than the two had correlations above 0.3. Table 5 shows the top reasons to monitor employees. The results for the total sample are shown along with the "notice" and "no notice" experimental conditions. Among the top seven variables, six of them were associated with threats regardless of whether there was notice or no notice of surveillance. Variables associated with threats occurred about 37% of the time in the top five whereas variables associated with opportunities were included in about 19% of the top five. The top reason to electronically monitor employees for all groups was

Table 4. Correlations Between Threats and Opportunities Variables

		Variables								
V[1]	**Variable Description**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
T	1 Computer virus or malware Protection	**1**								
T	2 Liability Protection	**-0.02**	**1**							
O	3 Employee Productivity	**-0.01**	**-0.24****	**1**						
T	4 Property Protection	**0.22****	**0.01**	**-0.12**	**1**					
T	5 Crime prevention	**0.04**	**-0.22****	**0.20***	**0.08**	**1**				
T	6 Legal requirements	**-0.09**	**0.15**	**-0.36****	**0.01**	**-0.01**	**1**			
O	7 Employee Safety	**0.27****	**-0.11**	**-0.32****	**-0.24****	**0.12**	**0.08**	**1**		
O	8 Perf. Eval Quality	**-0.42****	**0.08**	**0.10**	**-0.22****	**-0.23****	**-0.12**	**-0.04**	**1**	
O	9 Product or service quality	**-0.06**	**-0.07**	**0.15**	**-0.22****	**-0.30****	**-0.15***	**-0.26****	**0.01**	**1**
O	10 Professionalism	**-0.14**	**-0.20***	**-0.22****	**0.23****	**-0.07**	**-0.24****	**0.13**	**0.06**	**0.06**
T	11 Employee protection	**0.18***	**-0.06**	**-0.30****	**-0.06**	**0.18***	**0.13**	**0.27****	**-0.29****	**-0.19***
O	12 Employee wellness	**-0.36****	**-0.07**	**-0.10**	**-0.27****	**-0.19***	**0.13**	**0.15***	**0.28****	**-0.09**
T	13 Cost reduction	**0.02**	**-0.12**	**-0.18***	**-0.10**	**0.10**	**-0.12**	**0.02**	**-0.10**	**-0.05**
O	14 Learning how employees work best	**-0.08**	**-0.20***	**0.12**	**0.00**	**-0.22****	**-0.20***	**-0.06**	**0.07**	**0.07**
O	15 Handling employees fairly	**0.08**	**-0.07**	**-0.00**	**-0.08**	**-0.10**	**-0.14**	**-0.10**	**-0.08**	**0.09**
O	16 Innovation	**0.00**	**-0.11**	**0.06**	**0.08**	**-0.14**	**-0.10**	**-0.02**	**-0.09**	**0.06**
T	17 Privacy Protection	**0.04**	**-0.04**	**-0.15***	**0.13**	**-0.04**	**0.10**	**-0.06**	**-0.12**	**-0.15**
O	18 Simplifying timekeeping	**-0.11**	**-0.14**	**-0.14**	**-0.13**	**-0.11**	**-0.28****	**-0.06**	**0.18***	**0.08**

		Variables								
V[1]	**Variable Description**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
O	10 Professionalism	**1**								
T	11 Employee protection	**-0.15**	**1**							
O	12 Employee wellness	**-0.18***	**-0.15**	**1**						
T	13 Cost reduction	**-0.04**	**0.04**	**0.05**	**1**					
O	14 Learning how employees work best	**0.02**	**0.01**	**-0.08**	**0.08**	**1**				
O	15 Handling employees fairly	**-0.14**	**-0.11**	**0.02**	**0.21****	**-0.06**	**1**			
O	16 Innovation	**-0.09**	**0.07**	**-0.05**	**-0.05**	**0.46****	**-0.04**	**1**		
T	17 Privacy Protection	**-0.04**	**0.07**	**-.06**	**-0.06**	**-0.05**	**0.10**	**-0.03**	**1**	
O	18 Simplifying timekeeping	**0.14**	**0.11**	**0.17**	**-0.10**	**-0.08**	**0.09**	**-0.05**	**-0.06**	**1**

[1]V = Variable Type: T = Threats; O = Opportunities; * - p<0.05, **p<0.01

computer virus and malware protection. Employee productivity was the third most important consideration with the “with notice” condition and in second place with the “without notice” condition. Table 6 shows t-tests comparing the threat and opportunity-related variables to notice and no-notice conditions. Only six of 18 variables showed significant differences between the notice and no-notice conditions. For example, liability protection was labeled as dealing with a threat. It was part of the top 5 variables significantly more in the no-notice condition rather than the notice condition. With this variable, the first hypothesis was supported. Legal requirement protection and employee protection also support the hypothesis.

Table 5. Top Reasons to Electronically Monitor Employees

		Both notice conditions			**With notice**			**Without notice**		
V[1]	**Variable description**	**Rank**	**Mean**	**SD**	**Rank**	**Mean**	**SD**	**Rank**	**Mean**	**SD**
T	Computer virus and malware protection	1	0.746	0.437	1	0.767	0.424	1	0.716	0.454
T	Liability protection	2	0.592	0.493	3	0.540	0.501	2	0.662	0.476
O	Employee productivity	3	0.560	0.498	2	0.626	0.486	4	0.473	0.503
T	Property protection	4	0.500	0.501	5	0.460	0.501	3	0.554	0.500
T	Crime prevention	5	0.493	0.498	4	0.485	0.502	6	0.378	0.488
T	Satisfy legal requirements	6	0.397	0.491	6	0.360	0.482	5	0.446	0.500
T	Safety protection	7	0.305	0.461	7	0.301	0.460	9	0.311	0.466
O	Performance evaluation quality	8	0.270	0.445	10	0.230	0.423	8	0.324	0.471
O	Product or service quality	9	0.270	0.445	8	0.300	0.463	11	0.230	0.423
O	Professionalism	10	0.259	0.439	9	0.260	0.441	7	0.357	0.440
T	Employee protection	11	0.184	0.389	11	0.140	0.348	10	0.243	0.432
O	Employee Wellness	12	0.087	0.282	14	0.080	0.273	12	0.096	0.296
T	Cost reduction	13	0.086	0.281	13	0.100	0.302	14	0.068	0.252
O	Learning how employees work best	14	0.058	0.233	15	0.051	0.223	14	0.068	0.253
O	Handling employees fairly	15	0.052	0.222	16	0.050	0.219	16	0.054	0.228
O	Innovation	16	0.023	0.150	18	0.020	0.141	17	0.027	0.163
T	Privacy Protection	17	0.035	0.183	17	0.040	0.197	17	0.027	0.163
O	Simplifying timekeeping	18	0.103	0.305	12	0.120	0.326	13	0.081	0.275
		Both notice conditions			**With notice**			**Without notice**		
Variable means			**Mean**			**Mean**			**Mean**	
Threat-related			0.371			0.355			0.378	
Opportunity-related			0.186			0.186			0.189	

[1]V = Variable Type: T = Threats, O = Opportunities; [2]Mean percentage of time that the variable was mentioned among the top five reasons to notify or not notify the employee of electronic surveillance

Three of the opportunity-related variables showed significant differences between the notice and no-notice conditions. All three were the variables that were mentioned the most in the top five namely employee productivity, performance evaluation, and product or service quality. The first and third variables correspond to the second hypothesis. The second variable results are significantly opposite of the second hypothesis.

Discussion

The results in Table 5 show a greater percentage of respondents mark threats among the top five most important reasons to monitor employees rather than opportunities. Among the reasons for monitoring with notice, seven of the eight top variables involved threats marked by 30% or more of the respondents. Among the reasons for monitoring without notice, six of nine top variables involved threats marked by 30% or more. Threats seem to be a dominant factor in monitoring regardless of whether there is a notice or no notice of monitoring.

Table 6. T-Tests for Independent Samples

Variable type	Variable description	F	t	Significance	Hypothesized direction
Threats					
	Computer Virus or Malware Protection	2.281	-0.766	0.133	
	Liability Protection	9.392	1.625	0.003**	Yes
	Property Protection	0.137	1.225	0.049*	Yes
	Crime Prevention	5.836	-0.396	0.631	
	Legal Requirement Protection	4.029	1.143	0.046*	Yes
	Cost Reduction	2.306	-0.750	0.131	
	Safety Protection	0.092	0.152	0.762	
	Employee Protection	12.06	1.743	0.003**	Yes
	Privacy Protection	0.850	-0.461	0.355	
Opportunities					
	Employee productivity	4.376	-2.022	0.038*	Yes
	Performance evaluation quality	7.216	1.385	0.008**	No
	Product or service quality	4.447	-1.029	0.036*	Yes
	Professionalism or reputation	0.009	-0.048	0.924	No
	Employee wellness	0.531	0.365	0.716	No
	Learning how employees work best	0.959	0.490	0.329	No
	Handling employees fairly	0.056	0.119	0.913	No
	Innovation	0.370	0.304	0.544	No
	Timekeeping simplification	2.837	-0.830	0.094	No

*p<0.05; **p<0.01

Based on the data shown in Table 6, four of the nine threat-related variables (liability protection, legal requirement, property protection, and employee protection) supported Hypothesis 1 and thereby supporting the tenants of prospect theory. Company managers who perceive bad conditions find more risky activities acceptable because they feel there is less to lose. Not notifying employees of electronic monitoring might be more acceptable to reduce threats in the workplace regarding those three variables. Two of the significant variables (liability protection and legal requirements) are associated with legal issues. A possible explanation for those results includes the need to spot illegal activities of employees. If there was a notice for monitoring, there might be alternative ways employees might do illegal activities that might be missed. Better productivity and product or service quality coincided with Hypothesis 2 and thereby supporting the tenants of prospect theory. As two significant threat-related variables were associated with law, two significant opportunity-related variables were associated with positive employee outcomes. Other variables seem to focus on organizational issues relating to processes and organizational image. One of the processes, performance evaluation quality, is an organizational issue that significantly was counter to Hypothesis 2. This might be because of the need to calibrate performance appraisal methodologies without bias or complaints. A possible explanation that supports Hypothesis 2 for the positive employee outcomes includes the need to make sure that employees know that they are being monitored so they can see that the employer is acting fairly. Another possible explanation is that if outcomes are going well for a company, there is no need to secretly monitor employees and get into potential trouble doing so. Other explanations for the results can be made due to other variables. The definition of what is a threat versus opportunity is fluid. A person who sees performance quality as an opportunity could also see it as a threat because they could focus on negative performance rather than positive performance. Threats and opportunity conditions might not be important when it comes to determining whether no notices or notices will occur. Each threat and opportunity variable could have confounding demographic (e.g., gender and race), organizational factors (e.g., presence of privacy policies and electronic monitoring, and respondent perceptions of the organization and its people. For example, providing employees with advance notice and justification of monitoring could enhance trust which is related to higher job satisfaction and lower turnover. Climate may be more important than advanced notices to improve employee perceptions of fairness (Alder et al., 2006).

Implications

As a result of this study, HR managers should be more aware of the impact of perceived threats to the workplace when considering monitoring without notice. Perceived threats such as liability and property protection are among the most significant reasons to secretly monitor employees. These relate to the importance of risk reduction in knowledge management research (Durst & Zieba, 2019). HR managers need to compare the value of the information gained from that monitoring versus the negative ethical and legal problems that might result. This and future related research also might help HR managers policymakers eventually understand the patterns behind instituting secret surveillance to create potential legislation, protect the company from legal liability, boost an ethical work environment and develop legal and ethical organizational monitoring policies. The policies might lead to new processes transparently described in employee handbooks, emails, or any other way of communicating with employees. The new laws and processes might be subject to international legal differences. For example, the United States has no all-encompassing federal law ensuring employee privacy and personal data protection. Protections vary by state law, administrative regulations, case law, and industry-specific (e.g., education, financial services) guidelines. On the other hand, Europe has a detailed Data Protection Directive that tends to be more protective of workers' privacy (Boyne, 2018).

Future Research and Paper Limitations

As this study is exploratory, many other studies can focus on alternative study methodologies to obtain a more detailed analysis of why no notifications of monitoring might be used. Some other variables could be the company size, and state-by-state monitoring laws, gender of the respondents, familiarity and experience respondents have with various monitoring methods, job competition, the role of culture, and trust. For example, Alge et al. (2004) found that managers are more likely to secretly monitor employees when their dependence on them is high and trust is low. There might be differences based on the topic (e.g., crime reduction, liability protection). This study only focused on human resource manager respondents from Texas. Cultural differences in management practices exist not only within the United States but in many other countries (Bloom et al., 2012). Human resource managers are not the only individuals involved in monitoring decisions. Top management and direct supervisors also can be involved. They could fill out the survey or related surveys to see how their perceptions differ from human resource managers. Some researchers might view that perceived threats can be seen as opportunities instead of changing the wording. For example, reducing theft could also mean enhancing security, reducing accidents could mean enhancing safety. Future experiments could change the wording of a survey to see if alternate statements would significantly change HR managers' notification opinions.

Conclusions

The top reasons to monitor employees are associated with threats to companies such as viruses/spyware and legal liability. Threats involving legal issues tend to be more associated with human resource manager support for monitoring without notice. Opportunities associated with employee productivity appeared positively related to monitoring with notice. These patterns appear consistent with prospect theory that associates opportunities with less risky behavior and threats with more risky behavior. Other variables measured such as those relating to some organizational processes and perceptions seemed to be not significantly related to the human resource managers' support of monitoring with or without notice. HR managers should weigh their choice of whether to secretly or openly monitor employees. This paper showed that perceived organizational threats tend to be significant motivations to secretly monitor employees. HR managers should at least be aware of this pattern to weigh the information gained from secret monitoring versus the potential ethical and legal problems.

References

ACLU (2020). Privacy in America: Electronic monitoring. https://www.aclu.org/other/privacy-america-electronic-monitoring

Alder, G. S., Ambrose, M. L., & Noel, T. W. (2006). The effect of formal advance notice and justification on Internet monitoring fairness: Much about nothing? *Journal of Leadership & Organizational Studies, 23,* 499-507. https://doi.org/10.1177/107179190701300111101

Alder, G. S., Noel, T. W., & Ambrose, M. L. (2006, October). Clarifying the effects of Internet monitoring on job attitudes: The mediating role of employee trust. *Information and Management, 43*(7), 894-903. https://doi.org/10.1016/j.im.2006.08.008

Alder, G., & Tompkins, P. (1997). Electronic performance monitoring: An organizational justice and concerted control perspective. *Management Communication Quarterly, 10*(3), 259-289.

Alge, B., Ballinger, G., & Green, S G. (2004), Remote control: Predictors of electronic monitoring intensity and secrecy. *Personnel Psychology. 57*(2), 377-410. https://doi.org/10.1111/j.1744-6570.2004.tb02495.x

Al-Hitmi, M., & Sherif, K. (2018). Employee perceptions of fairness toward IoT monitoring. *VINE Journal of Information and Knowledge Management Systems, 48*(4), 504-516.

Amesen, D., & Weis, W. (2007). Developing an effective company policy for employee internet and email use. *Journal of Organization Culture, Communications, and Conflict, 11*(2), 53-65.

Balfanz, D., Golle, P., & Staddon, J. (2016). Proactive data sharing to enhance privacy in ubicomp environments. https://www.cs.cmu.edu/afs/cs/Web/People/jasonh/courses/ubicomp-sp2007/papers/05-proactive-data-sharing-ubicompprivacy.pdf

Baldwin, D. (1971). Thinking about threats. *Journal of Conflict Resolution, 15*(1), 71-78.

Bloom N., Genakos, C., Sadun, R., & Van Reenen, J. (2012, June). Management practices across firms and countries. *National Bureau of Economic Research Working Paper 17850.* https://doi.org/10.3386/w17850

Boyne, S. M. (2018, July). Data protection in the United States. *The American Journal of Comparative Law, 66*(1)*,* 299-343. https://doi.org/10.1093/ajcl/avy016

Bush, T. (2016, June). SWOT analysis opportunities: Definition & examples. https://pestleanalysis.com/swot-analysis-opportunities-definition-examples/

Chattopadhyay, P., Glick, W., & Huber, G. (2017). Organization actions in response to threats and opportunities. *Academy of Management Journal, 44*(5), 937-955. https://doi.org/10.5465/3069439

Ciocchetti, C. (2011). The eavesdropping employer: A twenty-first-century framework for employee monitoring. *American Business Law Journal, 48,* 285-369. https://doi.org/10.1111/j.1744-1714.2011.01116.x

Cox, S., Goette, T., & Young, D. (2015). Workplace surveillance and employee privacy: Implementing an effective computer use policy. *Communications of the IIMA. 5*(2), Article 6. https://scholarworks.lib.csusb.edu/ciima/vol5/iss2/6

Demarest, M. (1997). Understanding knowledge management. *Long Range Planning, 30*(3), 374-384.

Duke, A. (2018, July). Kentucky city uses the terrorism excuse to keep the details of its surveillance equipment secret. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/kentucky-city-uses-terrorism-excuse-keep-details

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: Towards a better understanding of knowledge management. *Knowledge Management Research & Practice, 17*(1), 1-13. https://doi.org/10.1080/14778238.2018.153860

Dutton, J. & Jackson, S. (1987). Categorizing strategic issues: Links to organizational action. *Academy of Management Review, 12,* 76-90. https://doi.org/10.5465/amr.1987.4306483

Edwards, L., Martin, L., & Henderson, T. (2018, August). Employee surveillance: The road to surveillance is paved with good intentions. https://doi.org/10.2139/ssrn.3234382

Ekram System.com (2017, October). Increase employee productivity with user activity monitoring. https://www.ekransystem.com/en/blog/increase-employee-productivity

Eldor, L. (2018, August 10-12). *How collective engagement creates competitive advantage for organizations.* Academy of Management Annual Conference. https://journals.aom.org/doi/abs/10.5465/AMBPP.2018.10764abstract

Epstein, R. (2013). Google's gotcha: 15 ways Google monitors you. https://www.usnews.com/opinion/articles/2013/05/10/15-ways-google-monitors-you

Ettenson, R., & Knowles, J. (2008). Don't confuse reputation with brand. *MIT Sloan Management Review, 49*(2), 19-21.

Fiegenbaum, A., & Thomas, H. (1988). Attitudes towards risk and risk-return paradox: Prospect theory explanations. *Academy of Management Journal, 31,* 85-106. https://doi.org/10.2307/256499

Fombrun, C. J. (1996). *Reputation: Realizing value from the corporate image.* Harvard Business School Press Books.

Fox, C., & Tversky, A. (1995). Ambiguity aversion and comparative ignorance. *Quarterly Journal of Economics, 110 (3), 585–603.*

Friedman, B., & Reed, L (2007). Workplace privacy: Employee relations and legal implications of monitoring employee e-mail use. *Employee Responsibilities & Rights Journal, 19*(2), 75–83. https://doi.org/10.1007/s10672-007-9035-1

Gardner, P. (2007). Moving up or moving out of the company? Factors that influence the promoting or firing of new college hires. *CERI Research Brief,* Issue 1. https://files.eric.ed.gov/fulltext/ED509852.pdf

Gherghe, M. (2017). Considerations on the conditions under which the employer may monitor their employees at the workplace. *Tribuna Juridica, 14,* 62-69. https://www.ceeol.com/search/article-detail?id=597850

Hodson, T., Englander, F., & Englander, V. (1999). Ethical, legal, and economic aspects of employee monitoring of employee electronic mail. *Journal of Business Ethics, 19,* 99-102. https://doi.org/10.1023/A:1006110324652

Hovorka-Mead, A. D., Ross, W. H., Whipple, T., & Renchin, M. B. (2002). Watching the detectives: Seasonal student employee reactions to electronic monitoring with and without advance notification. *Personnel Psychology, 55*(2), 329-362. https://doi.org/10.1111/j.1744-6570.2002.tb00113.x

Hugl, U. (2013). Workplace surveillance: Examining current instruments, limitations, and legal background issues. *Tourism & Management Studies, 9*(1), 58-63. https://www.tmstudies.net/index.php/ectms/article/viewFile/547/961

Hung-Yue, S. (2018). The effects of employer SNS motioning on employee perceived privacy violation, procedural justice, and leave intention. *Industrial Management & Data Systems, 118*(6), 1153-1169.

Jackson, S., & Dutton, J. (1988). Discerning threats and opportunities. *Administrative Science Quarterly, 33*(3), 370-387. https://doi.org/10.2307/2392714

Kahneman, D., & Tversky, A. (1979, March). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263-2. https://www.jstor.org/stable/1914185?origin=crossref

Katz, L. (2015, June). Monitoring employee productivity: Proceed with caution. https://www.shrm.org/hr-today/news/hr-magazine/pages/0615-employee-monitoring.aspx

Kaupins, G., & Coco, M. (2017, Winter). Human resource manager perceptions of reasons to electronically monitor or not monitor employees. *International Journal of Management and Human Resources, 4*, 1-18.

Kohen, I. (2018, March). 7 ways employees benefit from employee monitoring. http://customerthink.com/7-ways-employees-benefit-from-employee-monitoring/

LaMarco, N. (2019). The advantages of monitoring employees. https://smallbusiness.chron.com/advantages-monitoring-employees-18428.html

Lazarus, R. (1968). *Stress*. In D. Sills & R. Merton (Eds.), *International encyclopedia of the social sciences.* Macmillan Reference (pp. 337-48).

Lewis, K., & Gardner, S. (2000). Looking for Dr. Jekyll but hiring Mr. Hyde: Preventing negligent hiring, supervision, retention, and training. *Journal of Healthcare Protection Management: Publication of the International Association for Hospital Security, 78*(1), 14-22.

Malerud, K., Siersma, V., & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative Health Research, 26*(1), 1753-1760. https://doi.org/10.1177/1049732315617444

McDonald, P., & Thompson, P. (2016). Social media(tion) and the reshaping of public/private boundaries in employment relations. *International Journal of Management Reviews, 18*(1), 69-84. https://doi.org/10.1111/ijmr.12061

McParland, C., & Connolly, R. (2019). Employee monitoring in the digital era: The impact of innovation. Proceedings of the *2019 ENTRENOVA Conference.* https://doi.org/10.2139/ssrn.3492245

Miller, B. (2019, September). Pros and cons of employee monitoring. https://hrdailyadvisor.blr.com/2019/09/25/pros-and-cons-of-employee-monitoring/

Moorman, R. & Wells, D. (2003). Can electronic performance monitoring be fair? Exploring relationships among monitoring characteristics, perceived fairness, and job performance.

Journal of Leadership & Organizational Studies, 10(2), 2-16. https://doi.org/10.1177/107179190301000202

Noll, M. (2018, January). Employer monitoring is on the rise. https://itsecuritycentral.teramind.co/2018/01/01/employee-monitoring/

Ofman, E., & Sagandykov, M. (2020). Electronic monitoring for employees: Employer rights in the XXI century. *Journal of Legal, Ethical, and Regulatory Issues, 1,* 1-9. https://www.proquest.com/docview/2519045670?pq-origsite=gscholar&fromopenview=true

Roberts, P., & Dowling, G.R. (2002). Corporate reputation and sustained superior financial performance. *Strategic Management Journal, 23*(12), 1077-1093. https://doi.org/10.1002/smj.274

Rosenberg, K. (2010). Location surveillance by GPS: Balancing an employer's business interest with employee privacy. *Washington Journal of Law, Technology & Arts, 6*(2). https://digital.lib.washington.edu/dspace-law/handle/1773.1/479

Rosenberg, R. (1999). The workplace on the verge of the 21st century. *Journal of Business Ethics, 22*(1), 3-14. https://www.jstor.org/stable/25074185

R. v. Keegstra, 3 SCR 697, (1990).

Ryan, M., & Halsey III, A. (2018, July 29). Air marshals have conducted secret in-flight monitoring of u. s. passengers for years. https://www.chicagotribune.com/nation/ct-air-marshals-secret-program-20180729-story.html

Schwartz, A. (2015). The 5 most common unethical behaviors in the workplace. *Career & Workspace.* https://www.bizjournals.com/philadelphia/blog/guest-comment/2015/01/most-common-unethical-behaviors-in-the.html

Slepian, M., Chun, J., & Mason, M. (2017). The experience of secrecy. *Journal of Personality and Social Psychology, 113*(1), 1–33. https://doi.org/10.1037/pspa0000085

Slepian, M., Masicampo, E., Toosi, N., & Ambady, N. (2012). The physical burdens of secrecy. *Journal of Experimental Psychology, General. 141*(4), 619-624. https://doi.org/10.1037/a0027598

Society for Human Resource Management (2019, March). Managing workplace monitoring and surveillance. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/workplaceprivacy.aspx?_ga=2.20738232.1416576486.1571861460-884906973.1571680522

Shook, E., Knickrehm, M., & Sage-Gavin, E. (n.d.). Putting trust to work: Decoding organizational DNA: Trust data and unlocking value in the digital workplace. *Accenture Strategy.* https://www.accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-WF-Decoding-Organizational-DNA.pdf#zoom=50

Smith, M., Carayon, P., Sanders, K., Lim, S., & LeGrande, D. (1992, February). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics, 23*(1), 17-27. https://doi.org/10.1016/0003-6870(92)90006-h

Smith, W., & Tabak, F. (2017). Monitoring employee e-mails: Is there any room for privacy? *Academy of Management Perspectives, 23*(4), 33-48. https://doi.org/10.5465/amp.23.4.33

Stanton, J. (2000). Traditional and electronic monitoring from an organizational justice perspective. *Journal of Business and Psychology, 15*(1), 129-147. https://doi.org/10.1023/A:1007775020214

Thomas, S., Rothschild, P., & Donegan, C. (2014). Social networking, management responsibilities, and employee rights: The evolving role of social networking in employment decisions. *Employee Responsibilities & Rights Journal, 27*(4), 173- 189. https://doi.org/10.1007/s10672-014-9250-5

Thomson, I. (2016, February 5). UC Berkeley profs blast secret IT monitoring kit on campus. https://www.theregister.co.uk/2016/02/05/uc_berkeley_profs_up_in_arms_about_secret_monitoring_system_on_campus/

Torpey, E. (2017, March). Data on display: Women in management. https://www.bls.gov/careeroutlook/2017/data-on-display/women-managers.htm

Turban, D., & Greening, D. (1997). Corporate social performance and organizational attractiveness to prospective employees. *Academy of Management Journal, 40*(3), 658-672. https://doi.org/10.2307/257057

U. S. Department of Labor (2019). Details report for 11-3121.00 – human resource managers. *O*NET.* https://www.onetonline.org/link/details/11-3121.00

Vessella, V. (2015, October). 6 benefits of employee monitoring. https://www.business2community.com/human-resources/6-benefits-of-employee-monitoring-01347304

Vrij, A., Nunkoosing, K, Paterson, B., Oosterweigel, A., & Soukara, S. (2002). Characteristics of secrets and the frequency, reasons, and effects of secrets keeping and disclosure. *Journal of Community and Applied Social Psychology, 12,* 56-70. https://doi.org/10.1002/casp.652

West, J., & Bowman, J. S. (2016). Electronic surveillance at work: An ethical analysis. *Administration and Society, 48*(5), 628-651. https://doi.org/10.1177/0095399714556502

Yerby, J. (2013). Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management, 1*(2), 44-55. https://www.iiakm.org/ojakm/articles/2013/OJAKM_Volume1_2pp44-55.php

Zweig, D. & Scott, K. (2007). When unfairness matters most: Supervisory violations of electronic monitoring practices. *Human Resource Management Journal*, *17*(3), https://doi.org/10.1111/j.1748-8583.2007.00040.x

Author Biography

Gundars Kaupins, Ph.D., SHRM-SCP is a Professor of Management at Boise State University. His work includes over 80 journal articles in privacy policies, human resource ethics, training and development, and autism in the workplace. He has published in journals such as the Academy of Management Perspectives, International Journal of Technology and Human Interaction, and Training and Development Journal. He has published four books including a textbook on Design Thinking and Strategy. He has served as a human resource management consultant for about 700 organizations.

Appendix: Electronic Employee Monitoring Survey

1. ***Rate the following scenario based on the following scale:***
   1 = very unethical, 2 = unethical, 3 = neutral, 4 = ethical, 5 = very ethical.

WITH NOTICE and during work hours, a company monitors employee…….
______ a. Websites visited
______ b. E-mail content
______ c. Location inside the company
______ d. Heart rate
______ e. Daily walking/running steps
______ f. Downloads
______ g. Time in the bathroom
______ h. Phone calls
______ i. Location while on call
______ j. Time in the breakroom
______ k. Body temperature
______ l. Speed while driving a company vehicle
______m. Social media activities
______n. Location inside the company building
______o. Location while on a company-related trip

2. ***Mark (with an "x") the top five reasons to electronically monitor employees WITH NOTICE.***

______ a. Employee wellness
______ b. Cost reduction
______ c. Learning how employees work best
______ d. Timekeeping simplification
______ e. Liability protection
______ f. Privacy protection
______ g. Professionalism/reputation
______ h. Employee productivity
______ g. Computer virus/malware protection
______ h. Handling employees fairly
______ i. Performance evaluation quality
______ j. Work inhibition

______ j. Property protection
______ k. Crime prevention
______ l. Legal requirement protection
______ m. Elimination of people from work activities
______ m. Innovation
______ n. Safety protection
______ o. Employee protection
______ p. Perpetuation of existing inequalities
______ p. Product service or quality
______ q. Perceived employee distance from management

3. ***Rate your familiarity with the following electronic monitoring methods based on the following scale:***
1 = very unfamiliar, 2 = unfamiliar, 3 = neutral, 4 = familiar, 5 = very familiar

______ a. GPS (Global Positioning Systems)
______ b. RFID (Radio Frequency Identification Tags) Similar to nametags with magnetic strip
______ c. Sensors on products/machines to assess quality
______ d. Internet monitoring software
______ e. Telephone monitoring software
______ f. Social network monitoring software
______ g. Drones
______ h. Biometric devices
______ i. Data mining
______ j. Profiling

4. ***Has your organization electronically monitored your activities?***
_____ Yes _____ No _____ Don't know

5. ***Does your organization have any policy associated with electronic employee monitoring?***
_____ Yes _____ No _____ Don't know

6. ***Number of employees at your business location.***
______ 1-100 employees ______ 101-500 employees ______ 501+ employees

7. ***What is your age?***
______ Less than 25 ______25-34 ______35-44 ______45-54 ______55-64
______65+

8. ***What is your gender?***
______Male _______Female

Thank you for completing this survey.