Workplace Surveillance and Managing Privacy Boundaries

Myria Watkins Allen
Kasey L. Walker
University of Arkansas, Fayetteville
Stephanie J. Coopman
San Jose State University
Joy L. Hart
University of Louisville

According to communication privacy management (CPM) theory, people manage the boundaries around information that they seek to keep private. How does this theory apply when employees are monitored electronically? Using data from 154 face-to-face interviews with employees from a range of organizations, the authors identified various ways organizations, employees, and coworkers describe electronic surveillance and the privacy expectations, boundaries, and turbulence that arise. Privacy boundaries are established during new-employee orientation when surveillance is described as coercive control, as benefiting the company, and/or as benefiting employees. Correlations exist between the surveillance-related socialization messages interviewees remember receiving and their attitudes. Although little boundary turbulence appeared, employees articulated boundaries that companies should not cross. The authors conclude that CPM theory suppositions need modification to fit the conditions of electronic surveillance.

Keywords: electronic surveillance; employee privacy; communication privacy management theory

We’ve given up a lot of our privacy in the workplace . . . and we didn’t even know we were doing it as we did it. . . . Slowly the “this is the way things are done,” that whole attitude. . . . New information is just given to us and we go with it. Then we realize, “Wow, this has really changed. I don’t think I would have gone in for this if this is how I knew the outcome would be.”

Female hospital worker
The use of new communication technologies to monitor employee behavior is clearly on the rise, particularly since the September 11, 2001, attacks on the World Trade Center and the U.S. Pentagon building (Alge, 2001; D’Urso, 2006; King, 2003; Lane, 2003). The 2005 American Management Association’s (AMA) survey of 526 companies, representing a wide range of sizes and types, found that more than three fourths of the companies monitor employees’ Web site connections and half use video surveillance primarily to guard against theft and sabotage. When compared with AMA surveys conducted in 2001, 2003, and 2004, employee surveillance increased significantly.1

Sophisticated electronic surveillance technologies increasingly offer managers the ability to map and influence employee communication (D’Urso, 2006). For example, ETelemetry’s Metron Enterprise Behavior Analysis (EBA) appliance easily traces who talks to whom within an organization via various communications media (Dubie, 2007). The Metron EBA helps managers identify how employees communicate, locate groups of employees who interact frequently, link employee communication groups to their business productivity, identify communication liaisons and isolates, and spot communication that may threaten a company. Humans have an “almost compulsive desire to know all there is to know about people and use this knowledge to regulate their behavior” (Sewell & Barker, 2006, p. 5), and the Metron EBA can be used toward that end.

Accompanying the expansion of electronic surveillance is a corresponding growth in the frameworks, models, and theories used to understand it, including agency theory (e.g., Sewell & Barker, 2006), procedural justice theory (e.g., Alge, 2001), information boundary theory (e.g., Stanton & Stam, 2003), and the structural–perceptual model (e.g., D’Urso, 2006). However, additional theory and research are needed because current scholarship often focuses on surveillance as either good or bad (Sewell & Barker), and both employers and employee have little clear direction on how to use or respond to electronic surveillance (D’Urso).

This study focuses on communication related to the primary tension between employer interests in surveillance and employee interests in privacy. It extends the limited research that uses communication privacy management (CPM) theory (Petronio, 2002) to better understand the privacy boundaries surrounding employee information capable of being captured electronically. Organizational members develop their understanding, use of, and responses to electronic surveillance through everyday interactions and conversations. In this study, the researchers explored the privacy boundary socialization messages employees receive, what coworkers say about
electronic surveillance, how employees feel about electronic surveillance, and what boundaries employees draw regarding surveillance.

Petronio (2004) describes CPM as a practical theory with the aim of solving everyday problems. CPM is especially useful for exploring employee reactions to electronic surveillance. CPM explicates issues related to privacy from an individual’s perspective in contrast to surveillance researchers who often use agency theory (see Eisenhardt, 1989, for a description) to explain surveillance-related decisions and actions. According to CPM, individuals have a need for privacy, defined as “the feelings that one has the right to own private information, either personally or collectively” (Petronio, 2002, p. 6). CPM focuses on how individuals and collectives attempt to manage the dialectical tension between private and publicly shared information. Boundaries mark ownership regarding the amount of control individuals or collectives (e.g., organizations) hold over private matters. An individual’s ability to manage the boundary between private and publicly shared information can become problematic if sources that do not co-own the “private” information attempt access.

The present study answers the call for a more nuanced understanding of workplace surveillance (Sewell & Barker, 2006) and the concomitant employee privacy concerns. Through a novel integration of the workplace surveillance literature and CPM theory, we develop a more complete understanding of the arguments used to establish, discuss, and evaluate privacy boundaries and how employees respond to perceived privacy boundary violations.

New Technology and Organizational Surveillance

Many scholars use a panopticon metaphor to explain the pervasive and often unobtrusive character of organizational surveillance in an employee’s working life (e.g., D’Urso, 2006; Sewell & Barker, 2006). Consistent with the panopticon metaphor, we define surveillance as the “few watching the many.” This definition is especially useful because we are interested in employee privacy perceptions within organizations where employers have decided to use electronic surveillance to monitor any or all employee messages and physical behaviors.

Two major ideological arguments dominate the literature in workplace electronic surveillance (Sewell & Barker, 2006). The first follows two strands of thought or discursive formations: surveillance as coercive control and surveillance as caring. Coercive control assumes that surveillance is
needed to expose and coerce unruly or deviant employees to constantly work hard (Sewell & Barker, 2006). Findlay and McKinlay (2003) wrote that “the most powerful legitimation of employer surveillance is to guard the organisation against crime, fraud, theft, and to protect the integrity of business-critical information systems” (p. 310). Surveillance as a form of caring assumes that surveillance protects the many from the disruptive, lazy, or incompetent few (Findlay & McKinlay, 2003; Miller & Weckert, 2000; Sewell & Barker, 2006). Surveillance also can protect employees against unfair work distribution or accusations of dereliction and show how an employee’s performance meets or exceeds management’s expectations (Mason, Button, Lankshear, Coates, & Sharrock, 2002). Agency theory is often used to explain both positions. This theory discusses problems that arise when the desire and goals of the principal (e.g., employer) and agent (e.g., employee) conflict, and it is difficult for the principal to verify how the agent is behaving (Eisenhardt, 1989). Electronic surveillance can limit the principal’s risk and the agent’s opportunism. Sewell and Barker (2006) explicitly address agency theory in their discussion of surveillance as caring. Yet agency theory is also central to coercive control when managers use surveillance to ensure employees work at or near their maximum capacity.

The second major argument in the workplace electronic surveillance literature is that such surveillance infringes on employees’ rights to privacy. Many authors acknowledge that electronic surveillance threatens employee privacy (e.g., Findlay & McKinlay, 2003; Lane, 2003). Fewer argue that employee privacy rights are of major importance, however, and those who do generally either are European scholars (e.g., Hardy & Clegg, 1996; Thompson, 2003) or focus on ethical concerns (e.g., Fairweather, 1999; Miller & Weckert, 2000). For some, the right to privacy is more important than an organization’s right to efficiency and profitability (e.g., Miller & Weckert, 2000). For others, the argument is that “the employee should not be required to reveal their whole self to the employer; in other words, there is scope for some privacy” (Fairweather, 1999, p. 39). Given our assumption that there is room for some employee privacy at work, we discuss privacy boundaries and turbulence next.

**Privacy Boundaries in the Workplace**

Regardless of whether electronic surveillance technologies are used by employers as a form of control or of caring, employee privacy may be eroded. CPM theory posits that because individuals and groups inherently need some privacy, they will seek to regulate the dialectical tension between
privacy and disclosure by setting boundaries around their information based on decision criteria used to generate privacy rules. Such rules are then open to negotiation, coordination, transmission, and modification (Petronio, 2002). Where electronic surveillance is used, employees’ control over privacy boundaries and rules may be severely curtailed. Turbulence can occur when problems exist with boundary coordination (Petronio, 2002).

The Foundations of CPM

In this section, we describe CPM theory’s key suppositions and then discuss the theory’s utility for understanding employee reactions to workplace surveillance. Five fundamental suppositions define the character of CPM theory (see Petronio, 2002, for an in-depth discussion of each). Supposition 1 defines private disclosures as revealing aspects of the self not publicly known. Irrespective of legal rights, individuals often assume they have the right to control their private information, including when at work. Such information might involve personal business conducted at work (e.g., phone conversations with professionals such as health care providers), personal crises and intimate relationships (Fairweather, 1999), or disclosures about nonwork activities.

Supposition 2 posits an important boundary demarcating the line between private, or individually owned or co-owned, information and public, or shared, information. People decide what to reveal and conceal on the basis of criteria and conditions that either are negotiated or already exist within a given context.

According to supposition 3, individuals feel vulnerable and violated when control is taken away because they realize they face potential risks regarding how their information might be managed (Petronio, 2002). Privacy invasion via surveillance can harm one’s personal identity, one’s estimation of oneself, and the image one wants to portray as well as one’s social identity in the group (Alge, 2001) and the quality of one’s work life (Stanton & Stam, 2003).

Supposition 4 proposes that when individuals reveal information, others become co-owners of that information and its boundaries (Petronio, Sargent, Andea, Reganis, & Cichocki, 2004), leading to the development of privacy rules. Privacy rules control who receives a disclosure; when, how much, and where disclosure occurs; and how a person might conceal information (Petronio, 2002). Petronio identified three privacy rule management processes: (a) privacy rule development and attributes; (b) the rules that moderate
boundary linkages, boundary ownership rights, and boundary permeability; and (c) issues related to boundary turbulence. The present study explores boundary ownership and boundary turbulence.

Supposition 5 identifies dialectical tensions that arise as people make ‘‘judgments about the degrees of privacy and publicness they wish to experience in any given interaction’’ (Petronio, 2002, p. 15).

**CPM and Workplace Surveillance**

The workplace is an excellent, yet understudied, context in which to explore issues related to CPM theory. At work, individuals manage personal, dyadic, group, and organizational boundaries and seek to coordinate the permeability, linkages, and ownership of private information (Petronio, 2002). Stanton and Stam (2003) first applied CPM theory to the study of workplace surveillance, integrating it with social exchange theory (Thibaut & Kelley, 1959). The researchers characterized information about employees as a valuable organizational resource that can be captured using technology. For companies to benefit from access to such information, they must engage in reciprocal exchanges with employees in the form of promised rewards or potential sanctions. Employees decide to reveal (boundary openness) or conceal (boundary closure) performance and non-performance information on the basis of the perceived costs or benefits of information sharing, their relationship with the company, and the expected uses of the information. The exchange elements of their theory largely were not supported by their data.

Although Stanton and Stam’s (2003) study confirmed CPM theory’s usefulness for exploring employee privacy reactions to electronic surveillance, they focused on six nonprofit organizations installing surveillance-capable technologies. The current study expands the focus to investigate intraorganizational communication within a range of organizations where surveillance technologies were in place and applies two additional aspects of CPM theory, boundary ownership and boundary turbulence.

**Boundary ownership.** Although employers typically view themselves as the owners of employees’ e-mail and voice-mail messages, visits to Web sites, movements within the company’s buildings, and so forth, employees sometimes take the opposite view (Lee & Kleiner, 2003; Townsend & Bennett, 2003). Therefore, organizations often serve as sites of contested boundary ownership (Mattson & Brann, 2002) even though
power is unevenly distributed between employers and employees (Petronio, 2002). Employers may invade or redefine employees’ privacy boundaries to gain more information. Through policies and training practices, employers seek to socialize employees into the organization’s privacy boundaries (Petronio, 2002).

To investigate boundary ownership, we focused on how employers use socialization messages to “claim” information about employees’ physical movements and actions, work products, and communication. Specifically, we explored when and how employees learned they would be monitored and the justifications they recalled their employers providing for the electronic surveillance. Identifying the socialization messages employees remember receiving is important because such messages help establish the decision criteria (e.g., organizational culture, contextual constraints) on which privacy rules and rule compliance is based.

From Sewell and Barker’s (2006) work, we anticipated the organizational justifications would fall into two discursive formations: surveillance as coercive control and surveillance as caring. To explore how employers attempt to create privacy boundaries through their initial socialization messages, one research question and one hypothesis guided our investigation:

**Research Question 1:** When and how do employees learn they will be monitored?

**Hypothesis 1:** Statements related to surveillance as coercive control and surveillance as caring are embedded within the justifications respondents report receiving when they were hired.

Employees bring expectations and understandings from the broader society into the workplace that have implications for their reactions to workplace surveillance (Mason et al., 2002). North Americans generally support employee surveillance (Sewell & Barker, 2006). In the past several decades, the fragile and tenuous (D’Urso, 2006) idea of an individual’s right to privacy became ingrained in the U.S. value system (Gumpert & Drucker, 1998) and is held by many “to be a moral right, or at least an important good” (Miller & Weckert, 2000, p. 256). Given the contrasting national discourses, we sought to identify how employees respond communicatively and attitudinally to electronic surveillance. Investigating the themes embedded within remembered coworker discussions of surveillance and how respondents report feeling about being monitored allows us to begin to understand how and why employees respond as they do, both communicatively and attitudinally, to electronic surveillance. We asked the following:
Research Question 2: What do employees report that their coworkers say about electronic surveillance at work?

Research Question 3: How do employees feel about electronic surveillance at work?

Given the potential role of socialization in setting privacy boundaries, we wondered if respondents would express different reactions toward workplace surveillance depending on whether they learned about the surveillance when hired. If their socialization was effective, we expected to see the same explanations for surveillance appearing in their self-referencing statements and in their descriptions of how the need for and realities of surveillance were explained to them when they were hired. We asked the following:

Research Question 4: Do employees differ in their reactions to electronic surveillance depending on whether they were initially informed that surveillance was taking place in their workplace?

Boundary turbulence. Boundary turbulence refers to disruption or clashes in boundary management. Petronio (2002) argues, “For boundary maintenance to work, everyone must agree on the rules. When one person has a different idea about the way rules are formed and used, the management system may be disrupted and lead to turbulence” (p. 49). These clashes occur when individuals view boundaries as fuzzy or ambiguous; ignore, misunderstand, intentionally violate, or misuse privacy rules; use different criteria to develop rules; perceive different levels of risk concerning revealing and concealing; create linkages that violate ownership expectations; or apply rules from one boundary to another (Petronio, 2002, 2004). Boundary turbulence is a critical concept that needs further exploration (Petronio, 2004). In the present study, we explored issues related to boundary turbulence by first identifying the privacy boundaries our respondents articulated:

Research Question 5: What are the privacy boundaries employees articulate when discussing electronic surveillance?

Employees may respond to electronic surveillance in a variety of ways. For example, they can accept the surveillance implementation and have their privacy incrementally eroded or object and risk being called “a troublemaker” (Sewell & Barker, 2006, p. 8). Other employees seek “‘blind spots’ in a network of control—areas where they can escape the gaze of
manager, thus providing them with space to maneuver” (p. 6). Some express resentment, leave the organization (Holmes, 2003), resist through negotiation (Stanton & Stam, 2003), or engage in reverse surveillance (Sewell & Barker, 2006). Some research suggests few employees resist workplace surveillance, little agreement exists about what constitutes resistance, and many so-called acts of resistance do not actually sufficiently disrupt work productivity (Mason et al., 2002). Given the U.S. cultural attitudes toward surveillance and the arguments provided by Mason et al. (2002), we hypothesize the following:

**Hypothesis 2:** Employees will report few instances of coworker resistance to electronic surveillance.

**Method**

**In-Depth Interviews**

As part of a class assignment and following a detailed interviewing tutorial, 81 undergraduate students enrolled in upper-division organizational communication classes, and 8 students enrolled in a graduate organizational communication class conducted one-on-one, face-to-face, in-depth interviews with 154 respondents regarding workplace surveillance. Undergraduate interviewers selected interviewees in public places, such as cafés, bookstores, and shopping centers. Graduate students interviewed members of top management using snowball sampling to identify potential interviewees. Students interviewed between 1 and 3 interviewees. Most interviews took place in the San Francisco Bay Area with interviewees employed at a variety of organizations. All interviews were taped and then transcribed.

The interview guide included six primary questions: “Tell me about the ways your organization uses technology to monitor employees at work,” “How did you learn about the monitoring?” “How did your organization explain why it needs to monitor employees at work?” “What do your coworkers say about the organization’s monitoring of employees?” “What have you heard others say about what they are doing to avoid being monitored?” and “How do you feel about being monitored?” In addition, interviewers asked secondary questions when necessary to encourage interviewees to elaborate. The interview guide also included questions about the demographics associated with the interviewee’s place of work (e.g., type of organization and size) as well as about the respondent (e.g., ethnic background and salary).
**Interview participants.** Of the 154 people interviewed, 89 were managers and 58 were nonmanagers. The managers worked in high-technology (34%), financial or insurance (11%), retail (9%), transportation (7%), health (6%), telecommunication (3%), manufacturing (4%), education (3%), government (2%), or miscellaneous (21%) companies. Most companies employed fewer than 100 employees (25%) or between 101 and 500 employees (25%), with 20% employing more than 5,000 employees (range = 6 to 80,000). More than half (54%) were European American and 21% were Asian American. Most had worked for their current employer 2 years or less (32%), followed by more than 10 years (29%), between 3 and 5 years (27%), and between 6 and 10 years (12%). Most (30%) were between 31 and 40 years of age or less than 30 years old (26%).

The nonmanagers worked in high-technology (28%), financial or insurance (10%), retail (10%), transportation (2%), health (9%), telecommunication (3%), manufacturing (5%), education (3%), government (9%), or miscellaneous (21%) companies. More than half (56%) worked for a multinational organization. Most companies employed either 100 or fewer employees (28%) or more than 5,000 employees (26%) (range = 8 to 300,000). Most were European American (47%), Asian American (14%), or Latino (14%). Many (42%) earned $50,000 or less and 38% earned between $50,000 and $100,000. Most had worked for their current employer 2 years or less (50%), followed by between 3 and 5 years (20%) (range = 1 month to 50 years). Most interviewees were younger than 25 years old (30%) or between 25 and 30 years old (24%).

**Interview coding.** Using the grounded theory approach, two of the authors read half of the transcripts each to identify themes emerging from the data, designed a coding sheet (see appendix), and calculated Scott’s pi based on 15 (10%) randomly selected interviews. Intercoder reliabilities ranged from pi = 0.73 to pi = 1.0. The coding unit was a unit of text that expressed a complete thought. After the two coders discussed any disagreements in the 15 coded interviews, each coded 78 transcripts. Given the data’s dichotomous nature, frequency statistics, chi-square test results, and Phi coefficients are reported. When subcategories were summed, t-test and Pearson’s r results are reported.

**Results**

Our first research question was “When and how do employees learn they will be monitored?” Seventy-four percent (n = 113) indicated their
company told employees they were being monitored. Those who were not formally told \((n = 41)\) learned by observing surveillance or the consequences of surveillance \((32\%)\) or by seeing the surveillance equipment \((39\%)\), or they just assumed they were being monitored \((28\%)\). Of the 202 coded statements referencing how they were told, some learned through formal documentation \((51\%)\), dyadic communication \((28\%)\), or a group setting \((18\%)\), or they were personally responsible for implementing the surveillance \((2\%)\). Those who learned through formal documentation received a handbook or other written policy \((39\%)\), signed a document acknowledging the surveillance policy \((31\%)\), received a mass e-mail \((20\%)\), or saw signage announcing the policy \((10\%)\). Those who learned through dyadic communication were told by their supervisor or manager \((47\%)\); told personally by a human resource person, an information technology (IT) person, their coworkers, or by top administration \((28\%)\); or heard a story or rumor \((21\%)\).

Our first hypothesis was “Statements related to surveillance as coercive control and surveillance as caring are embedded within the justifications respondents report receiving when they were hired.” Table 1 lists the frequency with which respondents attributed each statement to the company or coworkers or when self-referencing. Although seven different categories emerged in 584 statements, 49% of the statements mentioned either coercive control or caring. Responses of surveillance as coercive control included 181 statements that surveillance protects the company from employee dishonesty and noncompliance and increases productivity by promoting efficiency. The most common subargument involving coercive control was that surveillance is necessary to reduce employee dishonesty and noncompliance \((58\%)\). Responses of surveillance as a form of caring included 118 comments about how employees benefited. The most common subarguments relating to surveillance as caring were that it increases employee safety and security \((29\%)\) and creates a more positive workplace \((26\%)\). An additional 170 comments dealt with how surveillance benefits the company. Table 2 provides a summary of the substatements related to surveillance as coercive control and as caring as well as how it benefits the company.

Research Question 2 was “What do employees report that their coworkers say about electronic surveillance at work?” About a quarter \((24\%)\) said their coworkers do not react to being monitored \((e.g.,\) no one talks about it, they are not aware they are monitored, they are not affected by it, they are ambivalent\). Overall, 35% of the statements attributed to coworkers were similar to those attributed to the organization. As illustrated in Table 1, of the shared statements \((attributed\ to\ the\ organization\ or\ to\ coworkers\ or\)}
appearing in self-referencing statements), proportionally more coworker comments focused on surveillance as caring (34%) and on the company’s right to monitor employees (9%). Fewer coworker comments dealt with surveillance as coercive control (21%), although a much larger majority of those arguments dealt with surveillance as controlling employee dishonesty and noncompliance (71%). As noted in Tables 1 and 2, few coworker statements dealt with how surveillance benefits the organization (15%).

In addition to the shared comments, some statements were only attributed to coworkers or appeared in self-referencing statements. As shown in Table 3, 65% of all comments attributed to coworkers indicated surveillance is either acceptable (55%) or problematic (44%), which is different from those that appeared in self-referencing comments (65% discussed surveillance as acceptable and 28% as problematic). Coworker statements suggesting surveillance is acceptable included that it is just part of life in the organization (28%), it is generally OK (19%), it is necessary (17%), and it is done only for cause (11%). Coworker statements that surveillance is problematic included that it is an invasion of privacy (22%) or forces coworkers to modify their behaviors (22%).

Research Question 3 was “How do employees feel about electronic surveillance at work?” Interviewees reported that surveillance is beneficial or necessary (68%), gave a mixed reaction (17%), appeared ambivalent (10%), or said it is bad (6%). There was a significant difference by managerial status ($\chi^2 = 10.07, p < .05$). More managers (74%) than nonmanagers (56%) indicated surveillance is beneficial, and more nonmanagers (13%) than managers (1%) said it is bad.9
Of the 292 self-referencing statements coded, 57% were the same arguments as attributed to the organization (see Table 1), and the proportional magnitude of the three major reasons (i.e., coercive control, caring for employees, and benefit company) were similar to those attributed to the organization, although some of the subarguments differed in relative frequency (see Table 2). Of the self-referencing statements, 28% stated that surveillance is acceptable, 12% indicated it is problematic, and 3% indicated surveillance should be balanced (see Table 3). The two most frequent statements suggesting surveillance is acceptable were that surveillance is being done only for cause (22%) and that the surveillance is not excessive.
Of the statements on whether surveillance is problematic, the most frequent either express a general dislike for surveillance (26%) or indicate it is an invasion of privacy (17%).

Several interesting differences emerged in the reasons attributed to coworkers and those made in self-referencing comments. General statements that surveillance is acceptable and that it is just part of life were more likely to be attributed to coworkers, whereas statements indicating that the surveillance is not excessive, is done only for cause, and should be balanced appeared in the interviewees’ self-referencing statements. In terms of surveillance as being a problem, the need to modify behavior was attributed to coworkers, whereas increased stress as a result of being monitored appeared in self-referencing statements.

### Table 3
**Frequency of Statements That Surveillance Is Acceptable, Surveillance Is Problematic, Surveillance Should Be Balanced**

<table>
<thead>
<tr>
<th>Theme</th>
<th>Coworker</th>
<th></th>
<th>Respondent</th>
<th></th>
<th>Total</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
<td>%</td>
<td>n</td>
</tr>
<tr>
<td>Surveillance is acceptable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Should work at work</td>
<td>12</td>
<td>19</td>
<td>4</td>
<td>5</td>
<td>16</td>
<td>11</td>
</tr>
<tr>
<td>Applied fairly</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>Necessary</td>
<td>11</td>
<td>17</td>
<td>15</td>
<td>18</td>
<td>26</td>
<td>18</td>
</tr>
<tr>
<td>Part of life</td>
<td>18</td>
<td>28</td>
<td>7</td>
<td>9</td>
<td>25</td>
<td>17</td>
</tr>
<tr>
<td>Not secret</td>
<td>5</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>13</td>
<td>9</td>
</tr>
<tr>
<td>Used passively</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Does not invade privacy</td>
<td>3</td>
<td>5</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>Not excessive</td>
<td>2</td>
<td>3</td>
<td>16</td>
<td>20</td>
<td>18</td>
<td>12</td>
</tr>
<tr>
<td>Done only for cause</td>
<td>7</td>
<td>11</td>
<td>18</td>
<td>22</td>
<td>25</td>
<td>17</td>
</tr>
<tr>
<td>Subtotal</td>
<td>64</td>
<td>44</td>
<td>82</td>
<td>56</td>
<td>146</td>
<td>100</td>
</tr>
<tr>
<td>Surveillance is problematic</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Linked to fewer rewards</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Invasion of privacy</td>
<td>11</td>
<td>22</td>
<td>6</td>
<td>17</td>
<td>17</td>
<td>20</td>
</tr>
<tr>
<td>Must modify behavior</td>
<td>11</td>
<td>22</td>
<td>4</td>
<td>11</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>Want more trust and freedom</td>
<td>8</td>
<td>16</td>
<td>7</td>
<td>20</td>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>Power inequity</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Increased stress</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>14</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Unclear policy or reasons</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Benefits company exclusively</td>
<td>0</td>
<td>—</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Dislike surveillance</td>
<td>11</td>
<td>22</td>
<td>9</td>
<td>26</td>
<td>20</td>
<td>23</td>
</tr>
<tr>
<td>Subtotal</td>
<td>51</td>
<td>59</td>
<td>35</td>
<td>41</td>
<td>86</td>
<td>100</td>
</tr>
<tr>
<td>Surveillance should be balanced</td>
<td>1</td>
<td>9</td>
<td>10</td>
<td>91</td>
<td>11</td>
<td>100</td>
</tr>
</tbody>
</table>
Research Question 4 was “Do employees differ in their views about electronic surveillance depending on whether they were initially informed that surveillance was taking place in their workplace?” There were no significant differences in terms of employee attitudes toward being monitored (i.e., positive, negative, mixed, and ambiguous) ($\chi^2 = 1.44, p = .70$), the numbers of privacy boundaries mentioned that the company should not cross ($t = -1.89, p = .20$), and the number of coercive control ($t = 1.09, p = .28$) and caring ($t = 1.24, p = .22$) reasons embedded in employee comments regarding how they feel about being monitored.

However, if interviewees were informed that they would be monitored when they were hired, similar statements appeared when they described how their organization justified the surveillance and when they described how they felt about being monitored. For example, if interviewees said that they were told when hired that electronic surveillance was important to control dishonest employees, they also mentioned that electronic surveillance controlled dishonest employees when describing how they felt (their self-referencing statements). This occurred in 13 cases, compared to none when employees were not initially told about the surveillance. In terms of surveillance as coercive control, self-referencing statements correlated with organizational justifications for “protects against dishonest employees” ($\Phi = .311, p < .05$) and “enhances productivity” ($\Phi = .265, p < .01$). In terms of surveillance as caring, three different organization and self-referencing statements correlated: “helps employees grow” ($\Phi = .380, p < .001$); “rewards good employees” ($\Phi = .312, p < .01$), and “increases employee safety and security” ($r = .325, p < .001$). In terms of benefits for the company, five different types of organization and self-referencing statements were significantly correlated: “protects intellectual property” ($r = .236, p < .01$), “prevents theft generally and by customers” ($r = .322, p < .001$), “protects company’s good name” ($\Phi = .492, p < .001$), “provides virus protection” ($\Phi = .393, p < .001$), and “increases company safety and security” ($r = .386, p < .001$). In terms of customer service, two organization and self-referencing statements were correlated: “provides quality customer service” ($\Phi = .312, p < .01$) and “increases customer safety and security” ($r = .325, p < .001$). Finally, there was a significant correlation between organization and self-referencing general expressions related to enhanced safety and security that did not specify company, employee, or customer ($\Phi = .305, p < .01$).

Research Question 5 was “What privacy boundaries do employees identify?” Fifty (33%) respondents made 90 comments indicating a line or boundary their company should not cross. The most frequent theme dealt
with inappropriate company attitudes and behaviors (34%), including making employees feel spied upon, monitoring employees without their knowledge, being intrusive, and severely limiting what employees can do with technology. The second-most frequent theme (24%) was that the company should not monitor personal matters (e.g., anything not done at work, personal e-mails, and phone calls). A third theme dealt with the reasons for surveillance (e.g., should not monitor for discrimination-based reasons; 13%). A fourth theme dealt with inappropriate technologies (e.g., genetic testing to screen new hires, intrusive metal detectors; 11%). A fifth theme focused on places that should not be monitored (e.g., restrooms, break rooms, and work cubicles; 8%).

Regarding our hypothesis that there would be few instances of employee resistance to electronic surveillance, 33 respondents (21%) mentioned ways employees evade being monitored. Of the 39 strategies provided, the most frequent were to (a) use encrypted Web sites, go through firewalls, or use the system itself (e.g., use provided dial-up instead of T1 line; 20%); and (b) use personal equipment at work (e.g., cell phones or e-mail; 20%). The second-most frequent strategies were to (a) avoid being seen (e.g., telling each other to stay out of camera’s view or be careful, wait until work is finished and there are no customers around, and turn off volume of instant messaging; 18%) and (b) realize that the company records personal e-mail and monitor words and topics accordingly (18%). A few statements dealt with sabotaging the system or stealing something (e.g., sign out equipment for work and then take it home, steal passwords; 13%) or discussed how employees work together to evade being monitored (e.g., clocking each other in, making friends with the IT guy so he will warn them, opening the door with a badge and leaving it open; 10%).

Discussion

An organization’s use of electronic surveillance technologies raises a fundamental tension between an employer’s desire for information to reduce uncertainty and an individual’s interest in privacy (Stanton & Stam, 2003). Existing within this fundamental tension are issues related to privacy boundary ownership and boundary turbulence. According to Petronio, Ellemers, Giles, and Gallois (1998), the boundary metaphor for privacy connotes permeability and flexibility as well as impenetrability and immovability. In some organizations, employees do have input into the design or implementation of the surveillance system (Alge, 2001; Stanton & Stam,
2003). Yet our research suggests that generally organizations set privacy boundaries. One manager in a high tech service and sales organization said,

No one likes anyone looking over their shoulder. But because we are so open about it, I think they realize what the boundaries are, and because of that they are comfortable within that. They know when they are crossing a boundary and stepping over the line, and it probably won’t be a secret. So they know their limitations, and they stay within them.

One explanation for employee compliance with the privacy boundaries organizations set is that those boundaries often are established initially through new employee socialization (Petronio, 2002). Therefore, in the current study we sought to explore the socialization messages respondents remember receiving. Consistent with Whitty’s (2001) study of Australian employees’ experiences with workplace surveillance, we found that 75% of our interviewees were told when hired that they would be monitored. We asked interviewees to reflect back to when they were first hired and answer the question “How did your organization explain why it needs to monitor employees at work?” We found multiple correlations between the justifications for surveillance respondents attributed to their organization and within their self-referencing statements. If interviewees said that they were told by their organization that electronic surveillance was important to control dishonest employees, they also mentioned that surveillance helped control dishonest employees when asked how they felt about electronic surveillance. This important finding suggests that either (a) socialization is effective at setting the privacy boundaries or (b) employees project how they feel about surveillance onto how they said their organization justified the surveillance. Either way, some consensus appears in how the surveillance is perceived. Certainly, our ability to understand the directional nature of the relationship is constrained by our data. However, given socialization’s role in setting privacy boundaries (Petronio, 2002), we assume the socialization had the desired effect.

The main justifications for surveillance attributed to organizations focused on how electronic surveillance benefits the organization or reflected Sewell and Barker’s (2006) two discursive formations, surveillance as coercive control and surveillance as caring. These justifications are consistent with previous research (e.g., Holmes, 2003; Thompson, 2003) and appeared in what interviewees indicated their coworkers said and in their own self-referencing statements. This key finding suggests that discursive formations at the societal level reverberate through company socialization messages
and coworker conversations and are illustrated in the attitudes our interviewees shared. The majority of the statements (60%) depicted surveillance either as coercive control or as benefiting the company, although 20% of the statements emphasized caring. In a comment illustrating surveillance as coercive control, one interviewee said,

We are only doing it on special occasions if there is a problem because we don’t want one bad apple to destroy the whole barrel. . . . [Employees know] someone could check on them. . . . I think it’s a good thing. It’s a deterrent and it keeps us all honest. It keeps the organization clean.

A manager in a semiconductor manufacturing organization provided a comment that illustrates surveillance as caring: “Some employees may look at it as invading their privacy a little bit, but we need to monitor employees to make sure that we are not overworking employees. . . . So, the employee benefits.” If employees perceive some benefit, they may be more likely to open their privacy boundaries (Stanton & Stam, 2003). They discussed ways managers might promote these benefits, such as career growth, professional development, and bonuses, to gain greater access to employee information. In our study, interviewees reported learning about similar benefits when they were hired (see Table 2) and mentioned the same gains in their self-referencing statements, providing us with some insight into the “personal calculus” (Stanton & Stam, 2003) people access when deciding to open or close their privacy boundaries.

Sewell and Barker (2006) argue that the picture is incomplete if scholars discuss electronic surveillance only as either coercive control or caring. Our interviewees’ comments also suggest that the dichotomy between the two perspectives is artificial. In U.S. workplaces, employees hear, discuss, and perceive electronic surveillance as both coercive and caring, which may help explain the limited boundary turbulence and resistance we identified. How electronic surveillance is framed can influence employee privacy management. Privacy issues may appear less salient and resistance less likely when employees believe electronic surveillance demonstrates a form of caring rather than an excessive form of coercive control that primarily benefits employers. When surveillance is framed as coercive control, privacy can become a line in the sand around which boundary turbulence exists and resistance occurs. Our results indicate that in most organizations, both discursive formations coexist (i.e., caring, coercive control) which may help explain the limited boundary turbulence and resistance we identified.
Because employees actively participate in assigning meanings to new surveillance processes (Stanton & Stam, 2003), we wanted to investigate what interviewees said their coworkers discussed as a way to understand how employees respond communicatively to electronic surveillance. Interestingly, interviewees attributed statements that surveillance is problematic more often to coworkers than to themselves. Employees engage in impression management (Rosenfeld, Giacalone, & Riordan, 1995), and so perhaps those interviewees who found surveillance to be problematic attributed such concerns to their coworkers. Many employees want to be seen as good employees (Sewell & Barker, 2006) who do not challenge their company’s surveillance activities.

Although privacy boundary negotiation may be feasible in many interpersonal contexts, employees often lack the power or motivation to actively participate in the boundary negotiation process, thereby limiting the degree of boundary turbulence. An electronics store employee said, “I’ve had a couple of coworkers who . . . were rebellious against it, but they can’t really do much about it. They’re working under company policy and once you’re under company rules and regulations, you lose all your rights.” Employees often exchange privacy control for a job (Petronio, 2002). Even though we asked questions where interviewees might mention privacy concerns (e.g., “What do your coworkers say about the organization’s monitoring of employees?” and “How do you feel about being monitored?”), only 17 statements directly mentioned privacy invasion (see Table 3). Mason et al. (2002) argue that many employees accept monitoring as legitimate or do not see it as a privacy threat. Indeed, 85% of our interviewees’ self-referencing statements either paralleled the justifications they attributed to their organization or indicated surveillance is acceptable.

Various authors argue that employees clearly distinguish between illegitimate trespass into their personal privacy and legitimate monitoring of occupational performance (e.g., Findlay & McKinlay, 2003; Mason et al., 2002). Given this, what privacy boundaries, if any, do employees seek to establish? Generally, the boundaries our interviewees expressed involved inappropriate company attitudes and behaviors, monitoring personal messages, using inappropriate technologies, monitoring in certain locations, and monitoring to build a case against certain employees. A high-tech firm nonmanager expressed the following concern:

As we go forward, we start to gather all types of information about people because saving information is cheap. The problem is that when I want to catch someone or not hire someone, I can go back and then gather all this
information and create a case against anybody I want. That is very, very dangerous.

Stanton and Stam (2003) examined the implementation of new technologies and the surveillance capabilities associated with the technologies. The employees in their study were involved from the beginning in the implementation process, and their reactions to surveillance were encouraged. In contrast, our respondents worked in a wide range of organizations and reported on surveillance already in place. We found little employee resistance to being monitored and very little boundary turbulence. Employees face institutional norms reinforcing surveillance practices, have few ownership expectations regarding private information at work, and appear to experience little motivation (a criterion important for rule development according to CPM theory)—and potentially great risk—to attempt change. An insurance company manager said, “Employees usually do not come forward and complain about or question the company’s rule. If they did, they could lose their job.”

Implications

Theoretical Implications

To date, few communication theories have been applied to electronic workplace surveillance (see D’Urso’s [2006] structural–perceptual model and Stanton & Stam’s [2003] information boundary theory for two notable exceptions), even though communication issues permeate electronic surveillance. Although Petronio (2000) discussed employee surveillance and privacy issues in her CPM theory, this study is among the first to apply the theory to employee communication about workplace surveillance. It expands Stanton and Stam’s (2003) research by focusing on additional critical aspects of CPM theory (i.e., boundary ownership and boundary turbulence) to help us better understand how electronic surveillance boundaries are framed for and by employees across organizations.

Although the tension between organizational interests and employee privacy rights have been discussed in previous research, our results are significant because they illuminate the extent to which employees allow organizations to set and own privacy boundaries. We identified a broad range of the justifications organizations appear to use to establish boundary ownership during employee socialization, justifications repeated in the interviewees’
own self-referencing statements. In addition, in their self-referencing statements, interviewees often embraced arguments regarding the need for electronic surveillance that exist at the societal level, something akin to Petronio’s (2000) discussion of how patients who adopt the ideology of physician as protector give up control of boundary ownership. Working together, socialization plus the giving up of control creates a condition that legitimizes organizational surveillance over employee claims regarding the right to privacy.

CPM theory was initially developed to better understand communication and privacy in interpersonal relationships, and the situation appears to be very different for employee communication and privacy. Applying the suppositions of CPM theory, our interviewees reported no employee input into the development of privacy rules and limited expectations for even having private information, although they did articulate some privacy boundaries. Organization members do perceive risks associated with public knowledge of their private information and use evasion and modify their behaviors to minimize these risks.

Mumby (2005) provides an overview and critique of the workplace resistance research, and various authors claim that resistance does occur, albeit subtly (e.g., Button, Mason, & Sharrock, 2003; Collinson, 2003). We conducted anonymous interviews with employees from a range of organizations to minimize intraorganizational pressures on interviewees’ responses. We must conclude that widespread boundary turbulence and resistance regarding electronic surveillance do not exist, a finding that supports Mason et al.’s (2002) arguments.

Practical Implications

Given that our respondents generally supported electronic workplace surveillance and given the lack of strong state or federal privacy laws (Willis, 2003), employers might easily justify increased employee surveillance. However, employees are not powerless and can engage in acts of resistance, leave the organization, post damaging information online (Gossett & Kilker, 2006), and tell prospective employees an organization is a bad place to work if they perceive electronic surveillance to be an excessive or increasing form of coercive control. High levels of surveillance can damage trust, leading to a less efficient workforce (Miller & Weckert, 2000) and other costly consequences for organizations (see the 2003 special issue of Organization Science that discussed the role of trust in organizations).
Surveillance also can damage intraorganizational communication as managers communicate less with surveilled employees (Botan, 1996), and surveilled employees may feel they lack opportunities to communicate freely with others and act autonomously (Hoffman, Hartman, & Rowe, 2003). Hampered communication may lower productivity, limit the development of important informal organizational networks, and prevent employees from exchanging key job-related information.

Implementing employee surveillance systems, then, should not be done without some reflection. Persson and Hansson (2003) argue for the application of ethical criteria in the decision to implement a surveillance program. First, the surveillance must be necessary to ensure effective employee job performance, protect the organization’s interests, or protect a third party’s (e.g., customers) interests. Second, it must be efficient and the least intrusive approach possible. Finally, the outcome must not cause more problems than those solved. Managers should balance protection for employees’ civil liberties against their fear of what a few rogue employees might do (Fairweather, 1999). Additionally, Hoffman et al. (2003) suggest, “To be respectful of the balance between personal and professional interests, the employer should offer a means by which the employee can control the monitoring in order to create personal boundaries” (p. 306). In an interview, an insurance company manager said,

Employers and top-management managers have to understand that an appropriate balance needs to be achieved between their legitimate interests in monitoring employees and employees’ right to privacy in the workplace. We must take care not to infringe on employees’ privacy rights.

**Strengths, Limitations, and Future Directions**

This study applied a communication theory to focus on a topic of increasing relevance. Our use of CPM theory led us to (a) investigate the socialization messages respondents remembered receiving when they were hired, (b) seek to identify the privacy boundaries they articulated, and (c) focus on any reported resistance as a manifestation of boundary turbulence. We explored the intraorganizational communication existing when surveillance is present.

As with any study, there are limitations. Our convenience sample came primarily from the San Francisco Bay Area. Because our purpose was descriptive rather than predictive, we felt the convenience sample was acceptable.
Many interviewees (nonmanagers = 28%, managers = 34%) worked in IT companies, and others held IT-related jobs within other industries. Their IT background may have caused them to experience less boundary turbulence. Identifying information as to the contextual and political circumstances of each localized case of surveillance was impossible. Asking respondents to reflect back carries with it problems related to respondent memory. Also, one-time interviews elicit espoused behavior and made it difficult to explore the CPM theory processes.

Future longitudinal research investigating local political struggles about the necessity, purpose, and consequences of surveillance are needed and can be captured through ethnographies and case studies, especially when new surveillance systems are implemented. Access to organizational documents or transcripts of new-employee orientation meetings would allow researchers to identify the actual versus reported organizational justifications given for the surveillance policies. Future researchers might investigate the dominant narrative within an organization (i.e., surveillance as coercive control, surveillance as caring) and whether privacy issues and resistance are more salient depending on the dominant narrative. CPM theory discusses how individual characteristics (e.g., self-esteem) influence boundary rule formulation in interpersonal relationships. Researchers might also seek to identify any important individual characteristics that may exist for understanding employee boundary rule formulation.

As we initially noted, additional theory and research related to workplace surveillance are needed because current scholarship often focuses on surveillance as either good or bad (Sewell & Barker, 2006). Our interviewees reported a more nuanced view, and by analyzing their words, we formed a more complete picture of the range of justifications, reactions, and concerns employees associate with electronic surveillance. Clear overlaps exist between some of the justifications for electronic surveillance employees remember hearing when hired and the feelings they shared regarding electronic surveillance. This suggests organizations effectively establish many privacy expectations and boundaries for new employees. Still, in their discourse, the interviewees articulated some boundaries that should not be crossed. Organization members are more likely to attribute evaluations (both positive and negative) of their organization’s electronic surveillance to their coworkers than to take ownership themselves. This study moved CPM theory into the organizational arena, finding that many of the theory’s suppositions may need modification when applied within that context.
Appendix
Emergent Themes

1. Reasons related to surveillance as coercive control:
   a. Necessary to enhance productivity, efficiency, improve performance, control quality
   b. Keeps employees honest; prevents theft of property and equipment by employees; ensures employees follow company guidelines and use company assets only for business

2. Reasons related to surveillance as caring:
   a. Helps employees grow, reach career goals, develop, and learn
   b. Rewards good employees
   c. Helps them do tasks (e.g., balance cash deposits)
   d. Protects employee (from theft of their things, if falsely accused, from harassment, from customer threats)
   e. Ensures fairness from slackers
   f. Helps shape a positive and nonabusive organizational culture or professional environment (e.g., prevent sexual harassment)
   g. Increases employee safety and security

3. Surveillance benefits company:
   a. Protects general assets (e.g., from sabotage)
   b. Protects intellectual property (e.g., trade secrets, new product development, confidential information)
   c. Prevents theft and loss; prevents theft of property and equipment by customers
   d. Protects company’s good name/reputation
   e. Provides virus protection
   f. Enhances financial health, well-being, and growth, reduces costs
   g. Addresses legal issues (e.g., comply with regulations, protect against lawsuits, protect against harassment charges, and resolve disputes)
   h. Helps managers manage (e.g., managers use to make decisions)
   i. Increases safety and security to company

4. Surveillance benefits customers, provides quality customer service, ensures confidentiality of customer information, increases customer safety and security

5. It is company property so the company has the right to monitor

6. Surveillance is standard practice in the industry or the nature of the job

7. Surveillance is acceptable:
   a. You should work at work; you’re their employee; you have no right to privacy
   b. It is applied fairly

(continued)
Appendix (continued)

c. It is necessary
d. It is just part of life; it is part of company
e. It is not done in secret; company policy and reasons are clear
f. It is used passively; the data gathered are not used
g. It does not invade privacy
h. It is not excessive; not invasive; it is not abused
i. Violators deserve to be caught; if you are not doing something wrong, you should not mind

8. Surveillance is problematic:
   a. Surveillance is linked to fewer rewards or to punishment
   b. It is an invasion of privacy; it is a violation of civil liberties
   c. It requires behavior modification; changed behavior in response to monitoring (chilling effect)
   d. Employees should be trusted; surveillance results in lack of freedom
   e. Surveillance results in a loss of employee power; monitors have too much power
   f. Surveillance increases competition and stress
   g. Surveillance policy and reasons aren’t clear
   h. Surveillance is only for company’s benefit; company’s motives are suspect
   i. Generalized worry, concern, or dislike

9. The use of surveillance should be balanced; it should be cost effective; must weigh company’s interests against employees’ rights; must weigh company’s need for surveillance against creating a trusting atmosphere and not alienating the employees

Notes

1. Employee surveillance has been a feature in the modern workplace since the times of scientific management and extending through the shifts toward bureaucratic and then concertive control (D’Urso, 2006).

2. Although we discuss actions taken by “organizations,” it is important to note employees are the organization (Weick, 1979) and that it is employees (e.g., managers, security personnel) who set the surveillance policy and monitor one another.

3. Petronio (2004) discusses the evolutionary development of communication privacy management (CPM), identifying the theory’s roots as being in the self-disclosure literature, especially social penetration theory and Altman’s (1975, 1977) use of a boundary metaphor to illustrate private space and territory. Although initially applied to interpersonal relationships (Petronio, 1991), more recent research has broadened aspects of the theory to discuss a wider range of issues (e.g., Mattson & Brann, 2002; Orrego et al., 2000; Petronio, Flores, & Hecht, 1997; Schultz, 2000).
4. Because of space constraints, the literature on employee socialization is not reviewed here. Readers seeking more of a background in communication-related socialization research might read Barge and Schleuter (2004), Comer (1991), Myers (2005), and Waldeck, Seibold, and Flanagan (2004).

5. Employees in the United States have more moderate expectations of privacy than employees in Great Britain and Germany (Petronio, 2002) and often accept surveillance as a legitimate part of their working lives (Mason, Button, Lankshear, Coates, & Sharrock, 2002). Also, the U.S. legal system emphasizes employers’ property rights more than employees’ privacy rights (Findlay & McKinlay, 2003).

6. The 154 employees made 454 comments dealing with how they were monitored. The most frequent ways involved cameras (56%) and e-mail (56%). Those who mentioned e-mail surveillance most frequently said their company stored or had access to all e-mail (41%), making it available for later monitoring, or scanned the e-mails (17%). Phone surveillance was the third-most frequent form mentioned (40%), with employers listening in on (30%) or recording calls (27%). Other methods included tracking the Web sites employees visited (38%), requiring employees to use badges or key cards to enter or move around the workplace (28%), blocking Internet sites and using firewalls (26%), looking at information on the computer or desktop and monitoring data transmissions (24%), monitoring productivity (17%), and using time and attendance systems (8%). Eighteen percent reported one major form of surveillance; 27% reported two major forms; 21%, three forms; and the remaining 37%, between four and nine forms.

7. For example, the primary question, “How does your organization explain why it needs to monitor employees at work?” included these secondary questions:

   How did you learn about these policies?
   Who told you about these policies?
   What did that person say about these policies?
   What other explanations does the organization give?

8. Because not all survey respondents and interviewees provided responses to demographic questions, categories do not add up to 100%.

9. We tested for other significant differences between managers and nonmanagers and found only one other. Because it might have been a spurious finding based on the large number of t tests run, we did not report it here.

References


Allen et al. / Workplace Surveillance 199


Myria Watkins Allen (PhD, University of Kentucky, 1988) is an associate professor in the Department of Communication at the University of Arkansas, Fayetteville. Her current research interests include privacy issues, information technology workplace issues, and cross- and intercultural workplace communication dynamics.

Kasey L. Walker (PhD, Purdue University, 2003) is a visiting assistant professor in the Department of Communication at the University of Arkansas, Fayetteville. Her research interests include interorganizational collaboration, social networks, and critical theory.

Stephanie J. Coopman (PhD, University of Kentucky, 1989) is a professor in the Department of Communication Studies at San Jose State University. Her research takes an applied approach, focusing on areas such as organizing and online communication, health care teams, and communicating disability.

Joy L. Hart (PhD, University of Kentucky, 1988) is a professor of communication at the University of Louisville. Her research and teaching interests center on organizational and health communication.