



PERGAMON

Computers in Human Behavior 16 (2000) 423–440

www.elsevier.com/locate/comphumbeh

Computers in
Human Behavior

Electronic monitoring in their own words: an exploratory study of employees' experiences with new types of surveillance

J.M. Stanton ^{a,*}, E.M. Weiss ^b

^a*Department of Psychology, Bowling Green State University, Bowling Green, OH 43403-0228, USA*

^b*Department of Psychology, Georgia Institute of Technology, Atlanta, GA 30332, USA*

Abstract

Electronic monitoring of employees has recently begun to take new forms such as email and web site monitoring. In an exploratory study of these new types of monitoring, 53 employed individuals responded to an anonymous, on-line, open-ended query about their related experiences. Content analysis of the resulting textual data explored two issues: the extent to which electronic monitoring shaped employees' behavior and the reasoning processes by which employees decided whether or not the monitoring was a negative experience. Results of the content analysis suggested that behavior was influenced by the capabilities of monitoring in combination with managerial expectations. Employees' attitudes about monitoring appeared to be dependent, in part, on the uses to which monitoring information was put. Finally, an unexpected focus on sexual content on the Internet revealed that employees had assimilated managerial concerns about organizational reputation. © 2000 Elsevier Science Ltd. All rights reserved.

Keywords: Human–computer interaction; Internet; Email; Job attitudes

1. Introduction

In 1990, Marx et al. painted a nightmarish picture of an omniscient organization with human resource (HR) systems infiltrating every aspect of employees' work lives. Thankfully, their vision has not become reality, although Orthmann (1998) reported that over 66% of companies surveyed by the American Management Association used employee monitoring or surveillance. Although prior research has focused specifically on electronic *performance* monitoring (e.g. Aiello & Kolb, 1995;

* Corresponding author. Tel.: +1-419-372-2301; fax: +1-419-372-6013.

E-mail address: stanton@bgnnet.bgsu.edu (J.M. Stanton).

Stanton & Barnes-Farrell, 1996), this issue is less in the public eye at the moment than organizational ‘eavesdropping’ on email and World Wide Web usage (e.g. Greene, 1998).

Researchers have not ascertained whether these newer types of electronic monitoring differ from those studied in prior research. Stanton’s (2000a) review indicated that much of the research on electronic monitoring during the 1980s and 1990s focused on measuring the performance of easily quantifiable clerical work and thus also focused on clerical workers. In contrast, more recent techniques facilitate monitoring of a broader range of work-related activities, some of which may not directly translate to performance. For example, organizations may monitor web site visitation to avoid legal liability or potential public embarrassment caused by employee visits to illegal or unpopular sites. It is unknown whether the extent or nature of these behaviors correlates with job performance. Stanton (2000a) suggested that existing electronic performance monitoring research might not inform these newer scenarios.

Thus, one issue that new research should explore is the impact of monitoring and surveillance technologies that do not focus on performance, *per se*. A few examples of such techniques illustrate the range of technologies used to collect non-performance information about employees. Organizations use camera surveillance to thwart theft and vandalism. Active badges facilitate tracking the movements of workers within organizational facilities. In some organizations, managers can access employee email, software program usage, and network uses (e.g. Internet web site visitation and file downloading). Security and legal personnel use these data to reduce liability exposure, monitor the release of sensitive information, and stem losses of company assets. In one notable case, a high-ranking professor at Emory University was forced to resign a tenured post because videotaped evidence allegedly showed him vandalizing a building (Rankin, 1999). The case exemplifies both the ‘non-performance’ aspect of new types of monitoring, and that a new class of workers is affected by the use of electronic monitoring and surveillance devices.

Monitoring and surveillance may affect employees in two broad domains. First, these techniques may affect employees’ feelings about work and the workplace: attitudes, emotions, beliefs, norms, etc. Second, monitoring may modify on-the-job employee behavior including productive, citizenship, and unproductive behavior. Aiello and Kolb (1995), Nebeker and Tatum (1993), Stanton and Barnes-Farrell (1996), and other researchers have documented a variety of effects, not all positive, of monitoring on productive behavior. Citizenship behavior, also called prosocial or extra-role behavior, apparently declines under conditions of intensive performance monitoring (Niehoff & Moorman, 1993). In other words, the more that managers monitor productive behaviors, the less that employees perform activities, such as helping others, that facilitate the overall performance of the organization. Finally, transcripts of hearings in the US House of Representatives (1989) on the activities of monitored telephone operators indicated that monitoring can also affect unproductive behaviors. In those transcripts, telephone operators admitted intentionally hanging up on customers who might have adversely influenced their monitored average call handling time.

One theoretical perspective that ties these effects together is known as social information processing (SIP; Salancik & Pfeffer, 1978; Zalesny & Ford, 1990). In general terms SIP predicts that normative social cues that workers receive from a variety of sources in the workplace will influence their attitudes and behaviors. Brewer (1995) and Larson and Callahan (1990) used the SIP perspective to predict the effects of monitoring on work behavior. Essentially their findings indicated that managers' monitoring activities shaped employees' behavior by drawing attention to what was valued and rewarded in the organization. By implication, social cues from monitoring can also draw employees' attention away from those activities that are shunned or proscribed. Thus, the first question that we intended to explore in the present research is how new types of monitoring technology, including those that do not monitor performance per se, affect employees reported on-the-job behaviors.

Monitoring may also affect employees' feelings about work and the workplace. Stanton (2000a) proposed a framework in which perceptions of fairness, satisfaction with monitoring, and monitoring invasiveness were interrelated attitudinal outcomes of monitoring. Fairness was defined as the degree to which workers evaluated monitoring practices affecting them as reasonable and appropriate. Niehoff and Moorman (1993) found that workers considered frequent monitoring a positive influence on fairness of supervisory evaluations. Satisfaction with monitoring was defined as a generalized positive or negative evaluation of monitoring practices. Chalykoff and Kochan (1989) found that five factors, including rating criteria and feedback from monitoring, predicted satisfaction with monitoring. Note that both monitoring satisfaction and monitoring fairness are linked in the research to evaluation of work performance (i.e. productive activities). Invasiveness was defined as the extent to which employees perceive monitoring practices as an invasion of privacy (US Congress, Office of Technology Assessment, 1987). Stone, Eddy and Stone-Romero (1997) reported a study in which participants rank ordered the perceived invasiveness of different monitoring techniques. We were not able to discover other research that examined this construct.

The research reviewed above indicates a need to understand attitudinal reactions to electronic monitoring of non-performance behaviors. Any or all of these factors — satisfaction, fairness, or invasiveness — could be salient reactions to email monitoring, active badges, or web site monitoring, but researchers have not explored this. Thus, the second question addressed by the current research is how employees characterize their non-behavioral responses to electronic monitoring. We tried to ascertain which attitudes, beliefs, or perceptions were influenced by experiences with electronic monitoring.

The present study took a qualitative, exploratory, and generative approach to these questions, using analyses of what employees said about electronic monitoring in their own words. In contrast to statistical analysis of representative sample data, the present study used content analyses of respondents' written answers to an open-ended survey question. The general goal of these analyses was to examine the ideas and beliefs of managers and employees about the impacts of electronic monitoring and to generate new perspectives on the uses and effects of such technologies.

2. Materials and methods

We asked a variety of employed individuals from several organizations to respond in writing to an inquiry about electronic monitoring and used a grounded theory approach to code and analyze the resultant texts. Scholars such as Glaser (1992), Harré (1981) and Strauss (Strauss & Corbin, 1990) have recommended these strategies when existing theory provides insufficiently detailed predictions to use a hypothetico-deductive approach to the analysis. We combined human creation and assignment of thematic codes with frequency analysis of code assignments to identify major thematic content. We triangulated on the themes using a two-part analytical strategy: examination of the most frequently used codes and assessment of important combinations of codes. At each point in the analysis, we illustrate the thematic material using verbatims from participant's written responses.

2.1. Survey instrument

A three-question survey (Appendix A) about uses of personnel data was developed based on a longer semi-structured protocol used by Stanton and Weiss (1999). The interview from that study was based on an extensive literature search that included examinations of scientific works, legal cases, and human resources trade literature. A bibliography of sources used in development of the full-length interview appears in Appendix B. From those sources, we identified a variety of important issues (e.g. email monitoring, background checking, and medical screening) that appeared repeatedly and that appeared to be of concern to both organizations and employees. Not all of the current issues were technology-driven, and we were inclusive in our efforts. Using semi-structured interview development strategies described by Smith (1995), we then constructed an initial interview protocol consisting of separate sections pertaining to job applicant data, employee performance data, and personnel records access and storage. The interview queried factual information about the organization's existing policies as well as reactions to hypothetical scenarios that depicted policies different from those used in respondents' organizations.

For the present study, we extracted material from the semi-structured interview protocol that was particularly relevant to employee data collection, technology, and the monitoring of work behavior. That material was the basis of the three queries we fielded in our open-ended, Internet-based questionnaire. The survey included a demographic section that reported respondents' age, hours worked per week, job tenure, union membership status, location while completing the survey, and job description. We did not inquire about the participants' ethnicity, as this can be a sensitive issue and did not appear relevant to the research question at hand: we had no prior basis on which to expect responses to be influenced by ethnicity.

The question which was the focus of the present study read as follows:

Next, please discuss any technology your company uses to track your work performance. Some companies use computer monitoring, email

monitoring, phone monitoring, security cameras, and/or geographic tracking (for example, of company trucks used by employees). Your company may use technology to track your work in other ways as well. How are these technologies useful or helpful to you? How are they annoying, undignified, or disturbing? Or perhaps you don't even notice these techniques in use?

This question was intentionally worded with both positive and negative components in order to elicit a balanced appraisal rather than one focused only on problems or dissatisfaction. Note also that the query discusses performance and non-performance exemplars, and that the words satisfaction, fairness, and invasiveness were not included. With this phrasing we hoped to elicit a broad consideration of electronic monitoring technologies and to avoid cueing respondents with words representing the specific attitudes of interest.

2.2. Participants

Participants were directed to the web site by researchers, using email sent by researchers, email forwarded by others who had completed the survey, or by a link found on the first author's web site. Stanton (1998) found that data collected from a sample of participants via the Internet-produced results produced covariance structures similar to those obtained from a sample that completed the same questionnaire in the traditional paper-and-pencil form. Stanton used these results to frame an argument that issues such as multiple response by single individuals were not a critical issue in an Internet survey used for research purposes. If anything, the current research instrument required even greater effort on the part of each respondent than that used in Stanton (1998), so we felt a degree of confidence that multiple response was not a critical issue. Further, the exploratory and qualitative nature relaxed the typical demands for representative sampling required in inferential research. Since we used no inferential statistics in the present study we had no assumptions to fulfill in regard to normality or related statistical concerns. In her discussion of grounded theory research techniques, Charmaz (1995) describes a meaningful rationale for non-representative sampling when the primary goals of the research are not inferential.

That said, we nonetheless tried to obtain responses from a wide variety of respondents holding a number of different types of jobs. We attempted to include companies from several different industries including for-profit, non-profit, and educational institutions. We directed our requests for participation toward contacts in approximately 25 different organizations including a university, legal firms, manufacturing firms, service firms, and a governmental organization. Initial organizational contacts comprised a convenience sample selected from among acquaintances of the researchers. The overall response rate suggested that, on average, two individuals responded from each organization. There were 53 respondents in total, but four of these provided no textual material in response to the question of interest in this study. Of the remaining 49 respondents, 20 were male, 28 were female, and one

did not report gender. The ages of respondents ranged from 20 to 59 years ($M=40$ years, $S.D.=11.47$). Respondents had spent between 1 month and 32 years at their jobs ($M=7.88$ years, $S.D.=8.37$), and worked between 10 and 85 hours per week ($M=41.82$ hours, $S.D.=13.16$). Three were union members, 46 were non-union members.

2.3. Procedure

Participants completed the survey over the Internet using a web browser. Information was entered into textual fields and the resulting data were forwarded anonymously via email to the first author. The data were exported from the email client into a word processor file. The total amount of text generated by respondents was equivalent to 31 typed pages.

2.4. Textual coding procedure

The strategy for coding was guided generally by Strauss and Corbin (1990) and particularly by Charmaz (1995). The files containing the textual data were imported into a qualitative data coding and analysis program developed by Centers for Disease Control and Prevention researchers to process semi-structured qualitative data (Carey, Wenzel, Reilly, Sheridan & Steinberg, 1998). We utilized the team-based code book development procedures recommended by MacQueen, McLellan, Kay and Milstein (1998). The coding team consisted of the two authors of this paper. The coding team used thematic material from respondents' texts as the basis of codes. In essence, we tried to capture the meaning of each idea within responses while also detecting commonality in ideas across responses. Upon completion of the code book, both members of the team assigned codes to all responses. We used the procedures described in Carey, Morgan and Oxtoby (1996) to improve inter-coder agreement. In contrast to the examples described by those researchers, however, we were able to obtain 100% agreement on all responses because of the relatively small number of codes that we employed. Descriptions of the complete set of codes we used appear in Appendix C.

3. Results

3.1. Demographic group comparisons

There were 26 respondents who were monitored and 23 who were not. Notably, the monitored and non-monitored groups were not significantly different from each other on any of the demographic variables recorded. Monitored and non-monitored individuals did not differ on the basis of age, hours worked, or job tenure. Table 1 contains means and t -values. The groups were balanced in terms of gender with about 2:3 ratio between males and females, $\chi^2(1)=0.96$.

Table 1
Means and *t*-values for monitored/unmonitored groups

	Monitored	Unmonitored	<i>t</i> -Value
Age	<i>M</i> = 40.3 years	<i>M</i> = 39.6 years	<i>t</i> (47) = 0.18, n.s.
Hours worked	<i>M</i> = 44.9 hours/week	<i>M</i> = 38.3 hours/week	<i>t</i> (47) = 1.80, n.s.
Job tenure	<i>M</i> = 6.4 years	<i>M</i> = 9.5 years	<i>t</i> (47) = 1.29, n.s.

3.2. Response code analysis

There were 29 unique content codes and 109 total uses of these codes in the 49 usable responses to the survey question (see Appendix C for code titles). Of these 29 codes, 14 codes were assigned to more than one respondent. To avoid reporting truly idiosyncratic material, we focused on these 14 codes in the analyses below. A list of the 14 content codes and their endorsement rates appears in Table 2. The following analysis highlights the five most frequently used codes by reporting and discussing a representative verbatim for each one.

As described above in the demographic section, 26 out of 49 respondents reported having no monitoring technology in use in their workplace. Responses reporting this were straightforward, simply stating that, to their knowledge, the respondents were not subject to any technological monitoring. An example of a response in this category was: “No technology is used to track my work performance.” (Respondent 6)

The other 23 respondents reported being monitored via some combination of computer monitoring, phone, electronic time clock, security camera, position monitoring, and/or production monitoring. Many respondents were monitored by techniques falling into more than one category. Seventeen of the monitored individuals reported being monitored through their computers (eight exclusively so). The computer monitoring category encompassed a wide range of monitoring techniques

Table 2
Codes used more than once and endorsement rates

Description of code	Total usage
There is no monitoring technology in place	23.00
Employee's computer use is monitored	17.00
Monitoring is not annoying, undignified, or disturbing	10.00
Monitoring provides security	9.00
The employee tracks his/her time at work with a time recording system	7.00
Telephone use is monitored	5.00
Employee is annoyed by technology or company policy	4.00
Employee tailors behavior because of technology	4.00
Monitoring is done in person by a supervisor	3.00
Production is tracked with monitoring	3.00
Respondent disturbed by technological monitoring	3.00
Organizational/personal concern with sex	3.00
Employee's physical position is monitored	2.00
Monitoring is intrusive	2.00

including monitoring of email account usage, Internet usage, web sites visited, software usage, and time the computer was actually in use or idle. A typical response in this category was: “I know that email sent via the company server is not confidential and could potentially be monitored. I also know that the Web sites you visit and how much time you spend at them are known to the MIS people.” (Respondent 15)

Ten respondents who were electronically monitored explicitly reported that they had not found negative effects from the monitoring. “My agency does track my use of computers and phones to make sure such use is job related (does allow for some personal use that is reasonable). I do not have a problem with this.” (Respondent 54)

Nine respondents reported having monitoring for security reasons in their workplace. A typical response was: “Security cameras/key cards have also been used to verify who was entering the building after hours or to observe potential thefts after hours.” (Respondent 43)

Six respondents reported having to record their time at work in some way. This included time sheets or time clocks. Note that unless a respondent explicitly mentioned an electronic timekeeping methodology these responses were not coded as electronic monitoring. One respondent who was *not* subject to electronic timekeeping said:

There is a pretty detailed method of time-sheet entry... specific job codes for each hour that you work in order to properly bill each client. Technical employees must be 100% billable and are tracked and get in trouble if they don't consistently meet their utilization goal. (Respondent 11)

In summary, the most frequently used response codes indicated that many respondents were not subject to any type of electronic monitoring. Of those who were subject to monitoring, only a minority found the monitoring negative in some way. Further, respondents cited the job-relatedness of monitoring and improved security as reasons for electronic monitoring.

3.3. Frequency analysis of co-occurring codes

3.3.1. Changing behavior in response to monitoring

Knowledge of a computer monitoring system's capabilities and understanding the tolerance level of organizational managers appeared to relate to individuals' behavior. Four respondents who were monitored by computer reported that they would modify or had modified their behavior with regard to time spent in email programs, sites visited on the web, etc., and especially the amount of personal activity undertaken on monitored company equipment:

However, I do know that if someone wanted to they could read my email, and monitor computer work. None of this bothers me, because these are work-related resources. If I have someone that personal, I would not associate with anything at work. (Respondent 19)

I know that e-mail sent via the company server is not confidential and could potentially be monitored. I also know that the Web sites you visit and how much time you spend at them are known to the MIS people. However, I don't know if they are being monitored with the intention of tracking your work habits or for other reasons. It's a little disconcerting that your private e-mails or your Web research that you do off hours could be tracked if someone really wanted to. However, most people know that that is the case and have adapted their habits accordingly (e.g., don't send confidential information via e-mail, or decide not to care if someone reads their e-mail). (Respondent 15)

If necessary, some work could be tracked by the computer systems administrator or by someone (a supervisor) with administrator rights. I don't worry about this because I'm always gainfully employed — even filling out this survey is a work process that is useful information in my occupation, human resources. (Respondent 46)

3.3.2. Reasoning and attitudes about monitoring

Monitored individuals exhibited an interesting mix of attitudes toward the monitoring. As was noted previously, 10 of the monitored individuals reported that the monitoring did not bother them at all. In three cases where a respondent was disturbed by the monitoring, he or she was unsure of what the information was being used for or how important the management viewed it to be. Here is a verbatim that expresses this combination of ideas:

I know that e-mail sent via the company server is not confidential and could potentially be monitored. I also know that the Web sites you visit and how much time you spend at them are known to the MIS people. However, I don't know if they are being monitored with the intention of tracking your work habits or for other reasons. It's a little disconcerting that your private e-mails or your Web research that you do off hours could be tracked if someone really wanted to. (Respondent 15)

Likewise, one individual who was subject to the monitoring of his physical position, and who believed that the information was important to his employer, also reported being disturbed by the monitoring:

...we all have id badges to get into the building and into certain areas. The technological capability is there to track employees throughout the building. ... DO I worry about this ability? Yes. What bothers me is that at any time I may be called upon to explain my actions. Like most people, I don't go through the day paying close attention to where I am or even why I'm there. For example, I may stop to see an employee in another part of the building for some reason and may stay for 30 seconds or 30 minutes. My fear is that some point down the road, say six weeks later, I get called into a meeting to address the question,

“what were you doing in that part of the building for 30 minutes?” Most likely I wouldn’t have any recollection why I was there. To compound the problem, like many employers my employer has a “guilty until proven innocent” approach to administrative problems. (Respondent 42)

In contrast, one respondent who reported not being annoyed by the monitoring noted a belief that nothing was being done with the information. Consequently, that respondent appeared to feel less concern over the potential impact of her computer use on her job position. Note how this verbatim also captures a legitimizing organizational rationale for monitoring that the respondent believes to be legitimate.

I recently discovered that there is a report about how long each employee in the organization is using the Internet. However, I do not think anything is being done with that information. I feel it is appropriate for companies to know that. They pay the bills and it may point towards misuse. (Respondent 50)

Among employees monitored primarily for security reasons, where their actual work performance was presumably not monitored (and thus would have no bearing on their perceived job performance), eight out of nine did not report feeling annoyed or disturbed by the monitoring. This verbatim reports another legitimizing rationale for monitoring: “... [they use] computer monitoring, security cameras, security codes for access after hours. ... These technologies generally protect my security while I am working. I generally do not find them annoying, undignified or disturbing.” (Respondent 18)

3.3.3. *Concerns about sexual content on the Web*

The background literature outlined in the introduction did not anticipate one additional significant combination of content codes that appeared. Three individuals working in environments that included computer monitoring expressed a clear concern for issues relating to the display of sexually explicit materials on company-owned computers. While it is likely that company policies prohibit or discourage heavy visits to any Internet sites that are not job related, employees seemed to be concerned exclusively with sites containing explicit sexual material. Other types of prohibited sites (e.g. gambling) were not mentioned:

We have an automated program which tracks Internet usage and reports access to sexually explicit sites. All employees know that accessing sexually explicit sites from office pcs will not be tolerated. Should one get such a site accidentally, we are to exit immediately. Some employees have been tracked for extensive hits on such sites, and have been disciplined for that misconduct. (Respondent 37)

Pertaining to e-mail and Internet usage, our network administrator has the capability to read incoming and outgoing mail as well as monitor Internet

usage (e.g., time on the system, sites visited, etc.)... like many employers my employer has a “guilty until proven innocent” approach to administrative problems. An example, charges were brought against an employee by another employee that the first employee was downloading pornography. The first employee’s computer was searched and, sure enough, one picture of a nude woman was found. The employee’s defense: I didn’t put it there, my computer is in a common area without password protections, thus anyone (another employee, cleaning staff, etc.) could have used the computer. The CEO’s response: if he didn’t do it make him find the person that did. Guilty until proven innocent. (Respondent 42)

In the latter response above, note how the uses to which monitoring information is put influenced the attitude of the respondent. The CEO’s “guilty until proven innocent” stance concerning the electronic evidence was apparently an irritant to this respondent.

4. Discussion

In the past, employee monitoring focused primarily on the quantity, and to a lesser extent, the quality of an employee’s on-the-job task performance behavior (Attewell, 1987). New technological developments such as active badges and monitoring software have made monitoring employees’ off-task behaviors simpler and more cost-effective for the organization. Simultaneously, the widespread availability of Internet access has apparently facilitated a plethora of new types of unproductive or even counterproductive behaviors. The distributed nature of work conducted on networked computers has also made it easier for employees to hide off-task behavior from their supervisors. Thus, the general goal of the present research was to examine the ideas and beliefs of managers and employees about the impacts of new types of electronic monitoring and to generate new perspectives on the uses and effects of such technologies. We accomplished this goal using content coding of textual data. Several interesting findings emerged from these analyses.

First, we confirmed that new varieties of monitoring technology (e-mail monitoring, Internet monitoring, etc.) have the potential to shape the way people behave in the workplace. Several respondents explicitly reported that they would change or had changed their behavior at work as a direct response to new monitoring technologies. The behaviors that people reported changing were primarily “unproductive” behaviors, such as using business e-mail accounts for personal messages, surfing the Internet for things other than company projects, or playing computer games during the work day. By commenting on these issues, respondents demonstrated knowledge of what the organization was capable of monitoring, and of organizational norms — what management believed to be appropriate and inappropriate behaviors. These findings fit neatly within the framework and predictions of social information processing theory (Zalesny & Ford, 1990), in that these

workers have apparently received social cues from the nature and capabilities of monitoring and surveillance systems and have translated these cues into norms for organizational behavior. This finding highlights the importance of explicit and well-communicated organizational policies, however, since informal or implicit social information can sometimes lead to the formation of inappropriate norms. Research on monitoring from an organizational justice perspective (e.g. Stanton, 2000b) has also documented the importance of organizational policy justifications for monitoring techniques.

In our second area of inquiry, we explored the reasoning behind reactions to monitoring: why some people believed monitoring to be intrusive or invasive and some did not. Popular culture and previous research efforts have led to a widespread belief that employees find technological monitoring to be invasive and troublesome, causing symptoms from mental distress to physical illness (e.g. Aiello & Kolb, 1995; Smith, Carayon, Sanders, Lim & LeGrande, 1992). Surprisingly, only a minority of the respondents in our study who were subject to monitoring found the monitoring to be negative in some way. The sampling strategy and sample size of the present study were not in any sense a probability sample of workers, and thus it is impossible to generalize the proportions obtained in this study to a larger population. Nonetheless, our results suggest that at least *some* monitored employees do not feel that the technological monitoring in their workplace is disturbing, annoying, undignified, or intrusive. Some respondents actually reported appreciating the monitoring, saying that it proved to their bosses that they were doing their work, or, in the case of surveillance cameras, that it provided them with a sense of security. Hence, for some employees, technological monitoring may actually represent a benefit. A large-scale survey across multiple professions is needed to ascertain the proportions of employees that feel positively or negatively about technological monitoring, and about whether there are differences in feelings among different demographic groups. Our literature review uncovered just one survey that requested employees' reactions to electronic monitoring (MSF, 1999) and that was limited to trade union members in Great Britain.

The potential use of information collected was a concern of employees. Employee reactions to monitoring appeared to depend on whether and how the organization planned to use information gathered from monitoring. Although this issue has not been researched in the context of monitoring, there is an analog in the drug testing literature. Raciot and Williams (1993) and Stone and Kotch (1989) found that employees preferred a drug testing program that sent those who tested positive to an employee assistance program over a system that discharged those who tested positive for drug use. Likewise, Tepper and Braun (1995) found that workers considered a drug testing system less invasive when consequences of a positive test were less punitive. Those findings may generalize to monitoring since respondents in the present study who believed that the monitoring had no influence on their job situation were not bothered by it (i.e. those who believed that nothing would be done with the data and those who were monitored for security reasons). In contrast, respondents who felt that the monitoring had the potential to affect their job situation reported being disturbed or bothered by the monitoring (i.e.

those who believed that the data collected would lead to disciplinary action or dismissal). These findings underscore the need for additional research to explore the relationship between uses of monitoring information and employee reactions to monitoring.

Some individuals monitored by computer voiced concern with sexually explicit material on the Internet. These reports were spontaneous since the issue of pornographic material was not addressed in the original question. Other prohibited sites, such as gambling sites, were not mentioned. Some individuals who mentioned sexual material may have worked in organizations that demonstrated a broad interest in controlling their behavior. It is possible that this individual focus on sex is a reflection of corporate emphasis on the subject. Companies may put more emphasis on prohibiting these sites over others because of potential damage to the company's reputation should the pattern of web site visits become public.

Although consuming pornography probably has a detrimental effect on individual's productivity, another reason for this focus on controlling visits to sexually explicit Internet sites is the potential for sexual harassment lawsuits. Companies can be held legally liable in harassment lawsuits for knowing that sexually harassing conduct or conditions were present and failing to take prompt remedial action (Burns, 1995). Research shows that males consume substantially more pornography than women (Lopez & George, 1995), and they are almost exclusively the defendants in sexual harassment lawsuits (Maypole & Skaine, 1983). A male employee who consumes Internet pornography in the presence of a coworker could be considered to be harassing that coworker by creating a hostile work environment. This situation is clearly an important concern for organizations. Interestingly, however, although visits to gambling and other recreational sites have equal potential with pornography to reduce productivity and visits to hate speech or bomb recipe sites may have very serious legal ramifications, these types of sites were not mentioned in respondents' verbatims. The absence of these concerns suggests the possibility that organizational norms for unproductive visits to non-pornography sites may not be as well established as those against visits to pornography sites. Further research is needed on whether employees perceive weaker prohibitions against recreational use of non-pornography sites.

The present study provided a detailed view of the perspectives of a small set of respondents. Thus, the major limitation of the study is its generalizability. The comments of respondents in this study should not be considered representative of a larger population. Likewise, these perspectives should not be considered exclusive of other viewpoints. Instead, the responses and analyses in the present study should be considered as demonstrative of some of the possible impacts of new monitoring techniques on employees. At least three enticing threads for future exploration have been uncovered. Social information that appears to come both from the capabilities of monitoring systems and from managers' communications about those systems may inform the development of behavioral norms among employees. These norms in turn shape behavior: employees may avoid personal use of email, surfing to pornography sites, etc. Future research should explicitly measure these norms and assess the strength of their impact on

the behavior of monitored employees. Our second finding was that employees' attitudes about new types of monitoring may be dependent on the uses to which monitoring information is put. Future research should compare work scenarios where the degree of punitive and non-punitive outcomes from monitoring varies. Finally, an exclusive focus on sexual content on the web may be masking other unproductive or counterproductive uses that Internet access facilitates. Future research should measure the types and relative amounts of Internet activities that employees engage in on the job and the perceived organizational norms concerning these activities.

Acknowledgements

The authors would like to acknowledge the assistance of Amanda Julian, Shreya Sarkar-Barney, Derek Steinbrenner, and Heather Odle. The reported research was supported by grant SBR9810137 from the National Science Foundation. The National Science Foundation does not necessarily support or endorse the findings or conclusions of this research

Appendix A. Three-item web-based survey instrument

1. In the box below, please briefly discuss information that your company collected from you when you were applying for a job, or after you accepted the job and were filling out forms for human resources. Some companies ask for social security number, emergency contact, work history, medical history, drug tests, medical tests, skill tests, background checks, and/or credit information. Your company may have asked other questions also. Did you care or worry about providing any of this information, or was it all pretty routine?
2. Next, please discuss any technology your company uses to track your work performance. Some companies use computer monitoring, email monitoring, phone monitoring, security cameras, and/or geographic tracking (for example, of company trucks used by employees). Your company may use technology to track your work in other ways as well. How are these technologies useful or helpful to you? How are they annoying, undignified, or disturbing? Or perhaps you don't even notice these techniques in use?
3. Finally, use the box below to describe something particularly good or bad that has happened to you at work because of the technology that your organization uses. Have you received a bonus or promotion because of technology? Have you been fired or discriminated against because of technology? Has your boss found out something about you (using technology) that you wish he or she hadn't? Any problems with privacy with your web browsing, email, or other aspects of Internet use?

Appendix B. Bibliography of resources reviewed for development of full length interview

9 to 5, Working Women Education Fund. (1990). *Stories of mistrust and manipulation: the electronic monitoring of the American workforce*. Cleveland, OH: Author.

Adler, P. A., Parson, C. K., & Zolke, S. B. (1985, Winter). Employee privacy: legal and research developments and implications for personnel administration. *Sloan Management Review*, 26(2), 13–22.

Agre, P. E. (1997). Introduction. In P. E. Agre, & M. Rotenberg, *Technology and privacy, the new landscape* (pp. 1–28). Cambridge, MA: MIT Press.

Anthony, C. S. (1994, March). Electronic monitoring legislation for businesses with call centers is fraught with problems. *Telecommunications*, 28, 22.

Attewell, P. (1987). Big brother and the sweatshop: computer surveillance in the automated office. *Sociological Theory*, 5, 87–99.

Baird, J., Kadue, D. D., & Sulzer, K. D. (1995). *Public employee privacy: a legal and practical guide to issues affecting the workplace*. Chicago: American Bar Association.

DeTienne, K. B. (1993). Big brother or friendly coach? Computer monitoring in the 21st century. *The Futurist*, 27, 33–37.

Ethics Officer Association (1997). *Sources and consequences of workplace pressure: increasing the risk of unethical and illegal business practices*. Belmont, MA: Author.

Flynn, G. (1997, October). How much medical disclosure is too much? *Workforce*, 76(10), 89, 92.

Greene, R. W. (1998, September). Internet addiction: is it just this month's hand-wringer for worry-warts, or a genuine problem? *Computerworld*, 32, 78–79.

Hatch, D. D., & Hall, J. E. (1997, August). Video surveillance presents HR challenges. *Workforce*, 76(8), 67.

Marx, G. T., Moderow, J., Zuboff, S., Howard, B., & Nussbaum, K. (1990, March/April). The case of the omniscient organization. *Harvard Business Review*, 68(2), 12–30.

Picard, M. (1994, February). Working under an electronic thumb. *Training*, 31, 47–51.

Pincus, L. B., & Trotter, C. (1995). The disparity between public and private sector employee privacy protections: a call for legitimate privacy rights for private sector workers. *American Business Law Journal*, 33, 51–89.

Privacy Rights Clearing House (1996a). *A checklist of responsible information-handling practices (English)*. Privacy Rights Clearing House (funded by Sprint).

Privacy Rights Clearing House (1996b). *How private is my medical information? (English)*. Privacy Rights Clearing House (funded by Sprint).

Rule, J., McAdam, D., Stearns, L., & Uglow, D. (1980). *The politics of privacy: planning for personal data systems as powerful technologies*. New York: Elsevier.

Sipior, J. C., & Ward, B. T. (1995). The ethical and legal quandary of email privacy. *Communications of the Association for Computing Machinery*, 38(12), 8–54.

Smith, H. J. (1993, December). Privacy policies and practices: inside the organizational maze. *Communications of the ACM*, 36(12), 105–122.

Society for Human Resource Management (1991). *Privacy in the workplace survey report*. Alexandria, VA: Author.

Thurston, R. J., & Jones, J. R. (1994, May). Health-care reform warrants HRIS updates. *Personnel Journal*, 73(5), 42–46.

US Congress, Office of Technology Assessment (1987). *The electronic supervisor: new technology, new tensions* (OTA-CIT-333). Washington, DC: US Government Printing Office.

Wallace, W. (1995, February). Bills aimed at rights protection. *Business Marketing*, 80, 20.

Appendix C. Brief code descriptions

Employee's computer use is monitored
 Infractions in company policy detected with monitoring are disciplined
 Monitoring is done in person by a supervisor
 There is no monitoring technology in place
 Monitoring activity is accompanied by a warning signal
 Telephone use is monitored
 Employee's physical position is monitored
 Production is tracked with monitoring
 Monitoring provides security
 The employee tracks his/her time at work with a time recording system
 Employee is annoyed by technology or company policy
 Orwellian "Big Brother" concept is mentioned
 Concerns for responsibility for/ownership of the computer
 Respondent disturbed by technological monitoring
 Employee worries about explaining actions to company
 Employee gives up freedom to get security
 Employer has guilty until proven innocent policy
 Technology used to monitor the workplace threatened home privacy
 Information collected is impractical
 Monitoring is intrusive
 Individual is protected by a large number of employees
 Monitoring is not annoying, undignified, or disturbing
 Trust violated by the company
 Employee values quality over quantity
 Employee tailors behavior because of technology
 Honor system is used, no monitoring/restrictions necessary
 Technology or company policies are undignified
 Problems caused a decrease in useful technology
 Web sites are blocked by technology
 Organizational/personal concern with sex.

References

- Aiello, J. R., & Kolb, K. J. (1995). Electronic performance monitoring and social context: impact on productivity and stress. *Journal of Applied Psychology, 80*, 339–353.
- Attewell, P. (1987). Big brother and the sweatshop: computer surveillance in the automated office. *Sociological Theory, 5*, 87–99.
- Brewer, N. (1995). The effects of monitoring individual and group performance on the distribution of effort across tasks. *Journal of Applied Social Psychology, 25*, 760–777.
- Burns, S. E. (1995). Issues in workplace sexual harassment law and related social science research. *Journal of Social Issues, 51*(1), 193–207.
- Carey, J. W., Morgan, M., & Oxtoby, M. J. (1996). Intercoder agreement in analysis of responses to open-ended interview questions: examples from tuberculosis research. *Cultural Anthropology Methods, 8*, 1–5.
- Carey, J. W., Wenzel, P. H., Reilly, C., Sheridan, J., & Steinberg, J. M. (1998). CDC EZ-Text: software for management and analysis of semistructured qualitative data sets. *Cultural Anthropology Methods, 10*, 14–20.
- Chalykoff, J., & Kochan, T. A. (1989). Computer-aided monitoring: its influence on employee job satisfaction and turnover. *Personnel Psychology, 42*, 807–829.
- Charmaz, K. (1995). Grounded theory. In J. A. Smith, R. Harré, & L. Van Langenhove, *Rethinking methods in psychology* (pp. 27–49). London: Sage.
- Glaser, B. G. (1992). *Emergence vs. forcing: the basics of grounded theory analysis*. Mill Valley, CA: Sociology Press.
- Greene, R. W. (1998, September). Internet addiction: is it just this month's hand-wringer for worry-warts, or a genuine problem? *Computerworld, 32*, 78–79.
- Harré, R. (1981). The positivist-empiricist approach and its alternative. In P. Reason, & J. Rowan, *Human inquiry: a sourcebook of new paradigm research*. Chichester: Wiley.
- Larson, J. R., & Callahan, C. (1990). Performance monitoring: how it affects work productivity. *Journal of Applied Psychology, 75*, 530–538.
- Lopez, P. A., & George, W. H. (1995). Men's enjoyment of explicit erotica: effects of person-specific attitudes and gender-specific norms. *Journal of Sex Research, 32*(4), 275–288.
- MacQueen, K. M., McLellan, E., Kay, K., & Milstein, B. (1998). Codebook development for team-based qualitative analysis. *Cultural Anthropology Methods, 10*, 31–36.
- Marx, G. T., Moderow, J., Zuboff, S., Howard, B., & Nussbaum, K. (1990, March/April). The case of the omniscient organization. *Harvard Business Review, 68*(2), 12–30.
- Maypole, D. E., & Skaine, R. (1983). Sexual harassment in the workplace. *Social Work, 28*(5), 385–390.
- MSF: Manufacturing, Science, Finance (1999). *MSF quarterly survey of workplace opinion*. London: Author.
- Nebeker, D. M., & Tatum, B. C. (1993). The effects of computer monitoring, standards and rewards on work performance, job satisfaction, and stress. *Journal of Applied Social Psychology, 23*, 508–536.
- Niehoff, B. P., & Moorman, R. H. (1993). Justice as a mediator of the relationship between methods of monitoring and organizational citizenship behavior. *Academy of Management Journal, 36*, 527–556.
- Orthmann, R. (1998, December). Workplace computer monitoring rose in 1998. *Employment Testing — Law and Policy Reporter*, p. 182.
- Raciot, B. M., & Williams, K. J. (1993). Perceived invasiveness and fairness of drug-testing procedures for current employees. *Journal of Applied Social Psychology, 23*, 1879–1891.
- Rankin, B. (1999, June 6). Emory chief's actions questioned; twists revealed in ex-prof's suit against school. *The Atlanta Journal and Constitution*.
- Salancik, G. R., & Pfeffer, J. (1978). A social information processing approach to job attitudes and task design. *Administrative Science Quarterly, 23*, 223–253.
- Smith, J. A. (1995). Semi-structured interviewing and qualitative analysis. In J. A. Smith, R. Harré, & L.V. Langenhove, *Rethinking methods in psychology* (pp. 9–26). London: Sage.
- Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y., & LeGrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics, 23*, 17–28.

- Stanton, J. M. (1998). An empirical assessment of data collection using the Internet. *Personnel Psychology*, 51, 709–725.
- Stanton, J. M. (2000a). Reactions to employee performance monitoring: framework, review, and research directions. *Human Performance*, 13, 85–113.
- Stanton, J. M. (2000b). Traditional and electronic monitoring from an organizational justice perspective. *Journal of Business and Psychology*, 15, 129–147.
- Stanton, J. M., & Barnes-Farrell, J. L. (1996). Effects of electronic performance monitoring on personal control, task satisfaction and task performance. *Journal of Applied Psychology*, 81, 738–745.
- Stanton, J. M., & Weiss, E. M. (1999). Technology and personnel data: contrasting the concerns of human resource managers and employees. manuscript under review at *Information Technology and People*.
- Stone, D. L., & Kotch, D. A. (1989). Individuals' attitudes toward organizational drug testing policies and practices. *Journal of Applied Psychology*, 74, 518–521.
- Stone, D. L., Eddy, E. R., & Stone-Romero, E. F. (1997, April). *Perceived invasiveness of employee monitoring systems*. Paper presented at the annual meeting of the Society for Industrial and Organizational Psychology, St. Louis, MO.
- Strauss, A. L., & Corbin, J. A. (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Newbury Park, CA: Sage.
- Tepper, B. J., & Braun, C. K. (1995). Does the experience of organizational justice mitigate the invasions of privacy engendered by drug testing? An empirical investigation. *Basic and Applied Social Psychology*, 16, 211–225.
- US Congress, Office of Technology Assessment. (1987). *The electronic supervisor: new technology new tensions* (OTA-CIT-333). Washington, DC: US Government Printing Office.
- US House of Representatives (1989). *Hearing before the subcommittee on courts, civil liberties, and the administration of justice on H. R. 1950: telephone monitoring by employers* (Serial No. 102). Washington DC: US Government Printing Office.
- Zalesny, M. D., & Ford, J. K. (1990). Extending the social information processing perspective: new links to attitudes, behaviors, and perceptions. *Organizational Behavior and Human Decision Processes*, 47, 205–246.