

Computer monitoring: benefits and pitfalls facing management

Sonny S. Ariss*

College of Business Administration, The University of Toledo, 2801 West Bancroft Street, Toledo, OH 43606, USA

Received 23 October 2000; accepted 24 May 2001

Abstract

The Information Age has enabled businesses to improve their efficiency through the use of advanced technology. The increase in the use of computers in the workplace has led to the ease of electronic monitoring of employees. Many feel that monitoring is important for the survival of their business. However, some employees regard this action as negatively impacting their work habits and privacy. This article examines the benefits and pitfalls of computer monitoring and recommends specific steps that need to be taken to monitor employees safely and ethically. © 2002 Elsevier Science B.V. All rights reserved.

Keywords: Computer monitoring; Employee's privacy; Ethical issues; Privacy policy; Employee's rights; Corporate security

1. Introduction

The Information Age has had a dramatic impact on our society—and this has been felt both positively and negatively. In recent years, we have seen a huge increase in the use of computers in the workplace, and coincidentally an increase in computerized performance monitoring. According to recent research by the American Management Association, the number of US companies that engage in electronic monitoring rose from 15% in 1997 to 27% in 1999 [24]. Today's electronic systems provide the tools to collect data and monitor the workplace with surreptitious efficiency. It is easy to view e-mail messages that employees send to one another and view what is on their monitors while they are at their computers.

How far should a company go to police employees' use of resources like e-mail and corporate networks? Moon and Kim [16] state the World Wide Web (WWW) is used both for work and pleasure, and have

introduced playfulness as a new factor in determining the WWW acceptance at the workplace. Another article indicates that around 45% of major US firms monitor employees communications and computer use [14] and also that about 53% of US companies have a written Internet usage policy. Approximately 25% have also acquired and use software that restricts access to sites that are deemed unsuitable for employees [1]. However, many employees view monitoring negatively, and believe it adversely affects the quality of their work [18]. The goal of this paper is to examine arguments for and against computerized monitoring in the workplace, particularly with respect to employee e-mail. Although the current state of US law allows employers almost totally free reign in electronic monitoring, an employer should weigh both sides of the question before reaching a decision.

2. New technology makes monitoring as simple as pushing a button

Employees are seldom aware of the many ways that technology can be used to monitor them. Voice-mail

* Tel.: +1-419-530-4060/4612; fax: +1-419-530-7744.
E-mail address: sariss@utnet.utoledo.edu (S.S. Ariss).

and e-mail attract the most attention. In fact, many workers are unaware their e-mail can be monitored and examined by their managers. Even when they understand clearly that others can access it, they will assume that, by deleting a message, there is no longer any chance that anyone can see it. They often do not understand that deleted messages can be retrieved, or that their messages can be used against them or cost them their jobs [7]. In fact, any action performed on a company computer may subject to monitoring even if it is not transmitted over a network nor stored in a file [15].

According to the American Civil Liberties Union (ACLU), 8 million Americans were being electronically monitored by their employers in 1991. That number was 30 million by 1999 [2]. The popularity of monitoring is growing due to enhanced technology which makes monitoring easier than ever. Eavesdropping on phone calls (illegal in the USA since the 1930s) used to involve hiring someone to install a “bug” on a telephone; now it is as simple as pushing a button. Software exists that can scan every e-mail transmitted through a company’s system, searching for keywords determined by the employer. A program called Silent Watch can randomly send the display on an employee’s monitor to a supervisor’s e-mail box—text, graphics, etc. The latest surveillance software on the market can monitor and record every keystroke an employee makes from a computer terminal: every deletion, revision, and touch of the keyboard. The implications of this new technology are startling: if an employee writes an e-mail or a memo, then thinks better of it and deletes the words, it may already be too late. The typing may have been stored on the computer’s hard drive or e-mailed to a system administrator for review [15]. While employees may try to argue that their “draft” thoughts are their own, US courts have consistently held that communications written on company-owned machines are not private.

3. The legality of electronic monitoring

The adoption of information technology in the workplace has increased the interest in the right of privacy issues in the 1960s and 1970s [10]. Mainly due to increased surveillance potential of computer

systems, laws governing the collection, record keeping and sharing of personal information were demanded. While federal law prohibits employers from listening in on an employee’s private telephone conversations, there is no protection when it comes to electronic communications on computers [9]. The courts have ruled that the US Electronic Communications Privacy Act of 1986, which prohibits unauthorized interception and disclosure of the contents of any electronic communication, does not apply to a company’s internal e-mail system because of an exception for business purposes in intercepting messages [22]. Under current US law, a corporate provider of private communication networks is allowed to intercept employee messages as long as he/she has a business reason for doing so. Legally acceptable business reasons range from protecting intellectual property to checking employee performance, to enforcing company policies. Thus, any reason given by an employer that is at all related to business has been acceptable as a “business reason”. Moreover, current law also protects companies against liability if employers give public notice of their screening policies. An employer’s monitoring actions are not prohibited under wiretap laws if at least one of the participants has given their prior consent or approval.

Some employees, finding that their privacy is not protected by statute, have sued their employers for invasion of privacy. While in the mind of an employee, this may seem to be an invasion of privacy, legal cases have proven otherwise. It is not unless an employee can prove that he/she had a reasonable expectation of privacy. In one 1996 case, *Smith V. Pillsbury*, the employee plaintiff claimed that Pillsbury had assured its employees that e-mail was private, but the judge ruled that no reasonable employee would expect to have privacy from his employer [21]. Moreover, any invasion of privacy must be intentional and highly offensive, not the result of random sampling or accidental discovery [12]. The burden is on the plaintiff to prove that his employer intentionally committed an act that would be highly offensive to a reasonable person. This is almost too severe to be overcome. Therefore, the current state of the law virtually assures employers *carte blanche* with regard to communications sent via company systems. Electronic monitoring is a relatively new issue and is worth studying.

4. The computer monitoring debate

Even though computer monitoring is legal, there is much disagreement among employees, employers, and experts as to whether it is ethical [19]. While there is no doubt that monitoring can benefit an employer, it raises concerns about employee privacy and micro-managing. Some employees feel degraded, stressed, and dehumanized by being closely monitored. But some employers feel it is their right to monitor their employees in any way they wish, since those employees are using company-owned equipment on company paid time.

5. Common arguments in favor of computer monitoring

Electronic monitoring within an organization may be perceived by an employer as a necessity as well as a right [8]. In an era where technology can be misused to harm the organization, it is appropriate that technology should be used to prevent harm. Within guidelines of privacy and professionalism, electronic monitoring can play an important role in protecting an organization from employee abuse. There are many reasons for employers to use modern technology to keep tabs on employees, among them to: prevent misuse of company resources; monitor employee performance; ensure that company security is not breached and guard against legal liability for employee statements or actions.

5.1. Preventing misuse of company resources

Many employers realize that some personal activities take place on company time, and most do not discipline their employees for making an occasional personal phone call. However, at some point, personal calls and e-mails begin to detract from time for which the employer is paying. Unauthorized use of the Internet can steal not only minutes and hours but bandwidth that rightfully should be spent on work. For example, at Poplar Grove Airport in northern Illinois, a programmer was hired to build web sites and work on special projects at a salary of about US\$ 50,000. But for weeks, the man disappeared into his office and produced almost nothing. After installing Silent Watch, the CEO discovered that the programmer

was visiting pornographic web sites and sending and receiving sexually explicit e-mails. The CEO burst into the man's office with a file full of printouts and fired him on the spot. "We don't pay you for that", he said. However, the CEO admitted, "We were relieved our business wasn't being compromised". Without the electronic monitoring software, many more weeks might have been stolen while the management tried to discover why no work was being done.

5.2. Ensuring that company security is not breached

In a recent Computerworld survey [4], the most common reason given for monitoring e-mail was to protect intellectual property. The possibility of leaking trade secrets and business strategies is a major concern, especially now that information is so easily stored and transmitted. Electronic monitoring can discourage breaches of security if employees are aware that their communications are not private. Monitoring can also identify who committed a breach, and pin down exactly what information was given, thereby allowing an employer to deal with certain types of problems swiftly and effectively.

5.3. Guarding against legal liability resulting from employee communications

Legally, the owner of an electronic system is responsible for all communications sent from or on that system, even though they are not business-related. For instance, in 1996, Prodigy was sued for libel because of one member's post, which accused an investment firm of fraud [11]. A recent survey of 500 corporate security directors revealed that 98.6% had seen not only computer-related crime within their organizations but problems related to sexual harassment, pornography, copyright infringement, and software piracy for which the company could be held liable. One company recently received a letter from the FBI, revealing that one of its employees was downloading child pornography in the office [23]. According to Elizabeth Du Fresne, chair of the employment and labor practice division of a Miami law firm, the Internet is the first place attorneys go for evidence in a sexual harassment or obscenity suit, because it is so easy to prove offensive behavior. "They (employees and managers) all know that they

can't hang up a Penthouse calendar in the workplace. They all know that they can't make a racist or sexist joke in the workplace, . . . but . . . I don't understand why they think they can send racial and sexist jokes via e-mail or download pornography at work".

Apparently, there are many employees who do not understand the consequences of downloading or circulating offensive material. Even CEOs have placed their companies in trouble by inappropriate use of e-mail and the Internet, as shown by the following examples [23].

- One CEO of an international company settled out of court when it was found that all his hits on the Internet were porn sites and that he had 81 dirty jokes in his personal folders, classified by category.
- In a case where there was never even a lawsuit, a CEO paid US\$ 1.5 million to a female employee after he downloaded pornography, showed it to her, and asked her to perform the activities depicted.
- Chevron Corp. was sued because of e-mail circulated within the company that listed 25 reasons why beer is better than a woman, it settled out of court, for US\$ 2.2 million.
- It cost a West Coast company US\$ 250,000 to settle an age discrimination lawsuit after an e-mail search showed that the company CEO had written an e-mail instructing human resources to "get rid of" a female employee.
- Microsoft Corp. settled a sexual harassment suit for US\$ 2.2 million involving pornographic messages sent within the company via e-mail.

Employers have a legal obligation to prevent harassment, discrimination, and other abuses of e-mail and the Internet. By monitoring e-mail and Internet usage, employers may be able to protect themselves from costly lawsuits resulting from messages with illegal or inappropriate content.

5.4. *Keeping performance up to par*

With increasing use of e-mail, many employers are randomly scanning outgoing messages to monitor employee performance during negotiations with customers, to ensure good sales tactics, or to determine progress in meeting deadlines. Many data entry clerks, customer service representatives, and telemarketers are monitored routinely to ensure that their performance meets pre-determined standards. An organization's

interest in employee performance is obvious, particularly in job categories where accuracy is paramount or direct contact with customers can make or break relations with a customer and hence the business. When random monitoring is used, the organization can benefit from better employee performance and minimal loss of productivity [3]. Hays [9] states, "Employees need to stay productive. And the only way to determine that is by monitoring their computer time". Used properly, electronic monitoring can be a way to alert management to potential performance problems before they become disasters.

6. Potential pitfalls of monitoring

Despite the many positive uses of electronic monitoring, its misuse can have undesirable consequences on employee morale, economic loss, and the potential for unethical behavior. Employers must use caution and exercise good judgment to minimize or avoid common pitfalls.

6.1. *Negative effect on employee morale*

Numerous studies have documented the negative effects of electronic monitoring on employee morale and productivity. Employees who are monitored complain that surveillance results in paced work, lack of involvement, reduced social support from peers and supervisors, and fear of job loss. One study reported that 75% of the employees surveyed believed that their work quality had suffered due to electronic monitoring. Some have linked anxiety, depression, and nervous disorders to the stress induced by workplace monitoring [5]. Those who are monitored may be "constantly apprehensive and inhibited" due to the constant presence of an "unseen audience". Some employees have even compared electronic monitoring to "working as a slave and being whipped, not in our bodies but in our minds" [5]. One data processor felt her work life was intolerable because her screen periodically flashed, "You're not working as fast as the person next to you" [17].

Even in less extreme cases, employees are likely to see monitoring as an unwelcome intrusion into their privacy, as well as a mark of distrust. Therefore, they may feel they are denied the self-respect that comes

with being trusted to do their jobs correctly on their own. Loss of self-respect leads to decreased performance and low morale.

6.2. Economic loss

Employers may find that the decision to monitor via computer leads to economic loss. Apart from the issue of decreased productivity, when employees may simply leave work early or take time off to devote to personal or family matters. Moreover, supervisors and managers will inevitably spend more of their time reviewing employee communication. There could also be legal costs if a suit is brought, even if it appears likely that no specific law has been violated [13]. Employers must consider the hidden costs of monitoring, beyond those of licensing the software.

6.3. Encouraging negative management styles

Managers who have a negative, “Theory X”, style of managing may use electronic monitoring to micro-manage the company. Managers with a Theory X style assume that workers generally dislike work and must be forced to do their jobs. This problem is compounded by the simplicity of monitoring. An employee may not be able to tell when monitoring is occurring. For example, “Investigator” can be sent as an e-mail attachment disguised as an “upgrade”. This displays an onscreen informing the user that this PC will be monitored, but that the notice can be disabled by a systems manager. The ethical concerns raised by deliberately humiliating employees are obvious; however, most managers and supervisors believe that warning employees about monitoring defeats the purpose of monitoring. The motive for monitoring communication is generally considered to be important in determining whether or not it is ethical. Although there are valid business reasons for monitoring, most employees do not wish to give up their privacy to an employer’s idle curiosity, or desire to control their personal lives [20].

7. Conclusion and recommendations to practicing managers

Excessive “snoopervision” may be regarded as unethical and economically destructive. But effective

supervision is a business necessity. The decision to monitor or not involves a delicate balance between the employer’s legitimate interests and the employee’s legitimate concerns [6]. The debate must be resolved on an individual basis, according to an employer’s best-judgment after considering all the factors. However, if the decision is made to use electronic monitoring, then ethical, legal, and employee relations problems can be mitigated.

7.1. Recommendations for monitoring

- Identify the business purpose for the monitoring and confine it to what is necessary to accomplish that purpose. Monitoring will only be used as necessary and will not be intrusive on the employees’ computer work.
- Require every employee to sign a statement that authorizes your organization to monitor e-mail and computer usage. This statement makes it clear that employees should have no expectations of privacy in their electronic communications.
- Develop and provide employees a written policy on employee use of communication systems, outlining exactly what types of communication are prohibited.
- Inform all employees how and when they will or might be monitored and what standards will be used to evaluate their performance.
- Inform employees that employee passwords for company systems do not guarantee privacy and may be overridden. Require employees to notify an administrator of their passwords to further decrease their expectation of privacy.
- Consider the costs of excessive monitoring, such as low morale, high turnover, and potential lawsuits, when formulating and enforcing policies.

References

- [1] Business Week, Footnotes: Data: Management Recruiters International, August 1999, p. 6.
- [2] J. Cook, Big brother goes to work, *Office Systems* 16 (8), 1999, pp. 43–45.
- [3] D. Dianne, Got security problems? It’s all in the attitude, *Computing Canada* (1996) 2–5.
- [4] D. Dominique, More managers monitor e-mail, *Computerworld* 33 (42), 1999, pp. 97.

- [5] B. Fairweather, Surveillance in employment: the case of teleworking, *Journal of Business Ethics* 22 (1), 1999, pp. 39–49.
- [6] G. Flynn, Balance on the fine line of employee privacy, *Personnel Journal* 74 (3), 1995, pp. 90–92.
- [7] S. Greengard, Policy matters, *Personnel Journal* 75 (5), 1996, pp. 78.
- [8] S. Greengard, Privacy—entitlement or illusion? *Personnel Journal* 75 (5), 1996, pp. 74–88.
- [9] S. Hays, To snoop or not to snoop? *Workforce* 78 (10), 1999, pp. 136–137.
- [10] S. Henderson, C. Snyder, Personal information privacy: implications for MIS managers *Information Management* 36, 1999, pp. 213–220.
- [11] R. Herschel, P. Andrews, Ethical implications of technological advances on business communication, *The Journal of Business Communication* 34 (2), 1997, pp. 160–170.
- [12] T. Hodson, F. Englander, V. Englander, Ethical, legal, and economic aspects of employer monitoring of employee electronic e-mail, *Journal of Business Ethics* 19 (1), 1999, pp. 99–108.
- [13] B.T. Johnson, Technological surveillance in the workplace, available at <http://www.twlaw.com/techsurv.html>, 1995.
- [14] J. Menezes, More employers spy on workers, *Computing Canada* 25 (23), 1999, pp. 11–13.
- [15] M. McCarthy, Keystroke cops, *The Wall Street Journal*, <http://www.msnbc.com/news/378768.asp>, March 2000.
- [16] J. Moon, Y. Kim, Extending the TAM for a World Wide Web context, *Information Management* 4 (38), (2000) 217–230.
- [17] K. Nussbaum, Workers under surveillance, *Computerworld* 26 (1), 1992, pp. 21.
- [18] E. Oz, R. Glass, R. Behling, Electronic workplace monitoring: what employees think, *Omega: The International Journal of Management Science* 27, 1998, pp. 167–177.
- [19] M.A. Pierce, J.W. Henry, Computer ethics: the role of personal, informal and formal codes, *Journal of Business Ethics* 15 (4), 1996, pp. 425.
- [20] R. Ramsey, The “snoopervision” debate: employer interests versus employee privacy, *Supervision* 60 (8), 1999, pp. 3–5.
- [21] R. Rosenberg, The workplace on the verge of the 21st century, *Journal of Business Ethics* 22, 1999, pp. 3–14.
- [22] J. Sipior, The ethical and legal quandary of e-mail privacy, *Association for Computing Machinery: Communications of the ACM* 38 (12), 1995, pp. 48.
- [23] M. Verespej, Internet surfing, *Industry Week* 249 (3), 2000, pp. 58–64.
- [24] K. William, Corporate e-mail monitoring on the rise, *Strategic Finance* 81 (7), 2000, pp. 19.



Sonny S. Ariss is the Interim Dean of the College of Business Administration at The University of Toledo. He holds a BBA in management, an MBA in finance, both from The University of Toledo and a PhD in Strategic Management from the Ohio State University. Prior to being named Interim Dean, Dr. Ariss was the Director of the Small Business and Entrepreneurship Institute, the Chairman of the Management Department, the Director of Undergraduate

Programs, and the Associate Dean for Undergraduate Studies.

He is the recipient of The University of Toledo Outstanding Teaching Award, the DeJute Memorial Teaching Award, the University College Outstanding Teaching Award and the International Alumnus Award. He is a two-time recipient of the Small Business Administration Best Small Business Case of the Year Award.

As a Professor of International Business, Entrepreneurship, and Strategy in the College of Business Administration, his current research centers in the areas of strategic planning, information technology, entrepreneurship and small business management. His articles have been presented at many national and regional conferences, and have appeared in the *Academy of Management Review*, *Nueva Empresa*, *Public Personnel Management*, *Advances in International Comparative Management*, *Managing Strategic Action*, *Empowerment in Organizations*, *Management of Change and Innovation*, *SAM Advanced Management Journal*, *International Journal of Production Economics*, *International Journal of Technology Management*, and the *Journal of Contemporary Business Issues*. In addition, Dr. Ariss has served as a reviewer on review panels and editorial boards of several books and journals in the field of management.

Dr. Ariss is a recognized authority on strategic planning and business management and has consulted for several small and large Fortune 500 companies in their strategic planning and organization development efforts.

Dr. Ariss is a member of Beta Gamma Sigma (Business Honor Society), Sigma Iota Epsilon (Honorary Management Fraternity), the National Academy of Management, the Strategic Management Society, and the Decision Sciences Institute.