IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4146

Monitoring Internet Use In the Workplace: Caution Is Advised

Mark T. Dishaw
University of Wisconsin Oshkosh, College of Business Administration, Oshkosh, Wisconsin
Tel: (920) 424-7196, Fax: (920) 424-7413, dishaw@uwosh.edu

ABSTRACT

This paper examines the use of IT systems such as Proxy Servers, and "Carnivore-Like" technologies to create electronic panopticons for the purpose of monitoring an employee behavior, Internet Use, in the workplace. An electronic panopticon is a device or system that allows for the continuous monitoring of an individual's behavior. This type of system when badly implemented can cause serious invasions of employee privacy in the workplace. Such privacy invasions are unwelcome and are frequently resisted. Managers should avoid using this control technique except when absolutely necessary due to the possibility of unintended negative effects.

INTRODUCTION

The right to privacy, recognized in part by the fourth amendment to the United States Constitution, and reinforced by numerous judicial decisions (Tuerkheimer, 1993), remains one of the most cherished individual rights. Louis Brandeis' classic definition of privacy, "the right to be left alone," refers to the rights of an individual in relationship to the government. However, privacy in the workplace is a much more tenuous concept as employees have little formal or legal protection against invasions of privacy by their employers while they are at work. Employers are free, under most circumstances, to monitor the work habits, work papers, telephone calls, WWW site visits, and e-mail messages of their employees.

While the right of an employer to supervise employees admits the possibility that the privacy of an employee might be invaded, in most cases a manager is ill-advised to monitor or supervise to the extent that a privacy invasion occurs. Such invasions are unwelcome and are often resisted with maladaptive behaviors that ultimately may cost the organization much more than is gained through close supervision.

This paper examines a type of management control system that has been incorporated into corporate information systems and networks. This type of system, a *Panopticon*, can be implemented by closely monitoring Internet usage through the use of Proxy server logging or sniffing using "Carnivore-like" technologies. It is argued that the implementation of a Panopticon may have unintended consequences for the organization and may ultimately cost the organization more than can be saved through monitoring.

THE ORIGINS OF THE PANOPTICON

The word *Panopticon*, deriving from the Greek roots *pan* and *optikos*, means, literally, "all seeing." In short, a Panoptic device, or system, is one in which the observer may, if desired, observe every act of the observed.

The origin of the Panopticon is found in the work of the late 18th Century English philosopher Jeremy Bentham (Zuboff, 1988). Bentham's Panopticon was an architectural and mechanical design for a prison. This design allowed the prison staff to constantly monitor the activities of each inmate. No inmate could undertake an act that would be unobserved. At the same time, the inmates could not determine if anyone was actually watching them at a particular moment. Interestingly enough, the design also included a method for the director to monitor the staff who were themselves monitoring the inmates. At the time Bentham recognized that this design could potentially be useful in situations other than penology.

PANOPTIC VISION

Network monitoring and management technologies can record the Internet WWW sites that an employee visits, and may be configured to intercept and record all of the packets exchanged during a web session. While it is possible and often easy to achieve Panoptic **vision** with monitoring technologies; however, vision alone is not sufficient to create power.

The principle of Panoptic vision and power derives from three factors. First, the supervisor must be able to observe the subject at any time. Second, this observation must be done without the subject's knowledge. Third, transgressions must be observed and acted upon by the supervisor.

The second factor, ultimately, is the key. The subject must not be able to determine when the observation is taking place. That the supervisor watches *sometimes* is sufficient to produce the effect. As far as the subject is concerned, the supervisor is *always* watching. This assumes that the consequences of being detected doing something undesirable are significant.

In a traditional Panopticon, a single supervisor cannot actually watch all of the subjects simultaneously. However, with a modern, information technology based Panopticon one supervisor can watch all the subjects all the time. Whether reporting is done in real time, or is deferred, is largely irrelevant. What is required, however, is that the supervisor must read the reports and take action periodically. Failure to act destroys the effectiveness of the system.

The ability of a Panoptic system to actually produce the Panoptic power effect is based on the fear of detection and on consequent correction or punishment by the supervisor. The subject is thus given the incentive to act in the prescribed manner. The goal of the system is to induce upon the subject "a state of conscious and permanent visibility that assures the automatic functioning of power" (Foucault, 1979). However, other less desirable "side effects" are produced as well.

CONTROL SYSTEMS

Control is a fundamental activity engaged in by managers, and can be thought of as the process of producing a desired state or result. Control can take on many forms such as policies, procedures, budgets, etc. In the most general of terms, control can be thought of as "good," in the sense that more control can yield more desirable results. This is well supported in the empirical control literature; however, it carries with it a very significant set of assumptions.

For a control mechanism to be effective in a given situation, it must be appropriate in both kind and degree. Improperly designed or applied control mechanisms will normally produce less than desirable results. The assumption that "more is better" may apply only over a very narrow range. Unfortunately, as evidenced by extensive system failures and the numerous management "horror stories" in the popular and business press, it appears that many managers remember the "more is better" adage without remembering the qualifying assumptions.

A common method of classifying control systems or mechanisms in an organizational setting divides controls into two categories (Ouchi

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference.

& Maguire, 1975): Outcome Controls and Behavioral Controls. Any control mechanism will carry with it advantages and disadvantages. The role of management in carrying out its control responsibilities is to institute a mix and balance controls that yield the highest net benefit to the organization. It may be necessary to adopt controls that are loose or tight, behavioral or outcome oriented, or a combination, based on the circumstances at hand. The monitoring of Internet use in the workplace is a prime example of an area where managers must understand, as fully as possible, the consequences of their control activities. Below, we briefly review the nature of Outcome and Behavioral controls.

Outcome Controls

Outcome controls emphasize the end result instead of the process of achieving the result. Common types of outcome controls include quotas, budgets, profit plans, deadline. It is possible to think of outcome based control systems as approximating a market-based arrangement between management and employee. The employee is compensated or rewarded based upon output (Anderson & Oliver, 1987).

Outcome controls are usually specified when it is difficult to prescribe the actions necessary to produce a desired result. In such an event, it is usually effective to specify the desired result to the responsible party, and allow that individual or group to proceed. This is often the case when the objective can be achieved through several legitimate paths of action. Outcome controls are an integral part of management by objectives (MBO), which is used even for lower level managers and individual contributors such as programmers, accountants, and engineers. It is quite common to see behavioral controls combined with outcome controls, especially at the lower levels of management.

The disadvantages of outcome-based controls are well known (Anderson & Oliver, 1987). The chief disadvantage is the possibility that counter-productive or damaging behaviors will be the result. These include, but are not limited to, the transmission of personal e-mail or visits to WWW sites that are irrelevant to job performance (surfing) or are simply inappropriate as to content.

Behavioral Controls

Behavioral controls focus not on the result, but on the means or actions taken to achieve that result. This control philosophy aims to achieve desired results by imposing restrictions on a subject's behaviors or actions. Panopticons typically are used to implement behavioral controls.

There are a number of reasons for choosing behavioral control mechanisms. If the steps needed to successfully complete a task are known, then behavioral control may be employed to ensure that the task is completed efficiently. Any process that has written instructions or procedures uses behavioral control.

This type of control is frequently employed when it is necessary to coordinate tasks performed by a number of workers. Health, safety, legal, or public policy issues also may necessitate using behavioral control.

Behavioral controls provide a number of advantages. First, it is possible to specify the exact steps needed to complete a task. Second, it is possible to prevent acts that may inadvertently damage the organization. Third, it is possible to treat employees more equitably by imposing uniform standards and rewards based only on the actions for which a person is responsible and not on events outside that person's control (Anderson & Oliver, 1987).

There are a number of problems associated with behavioral controls. One of the most significant is the need to ensure that the behaviors being controlled are going to yield the desired result. Even more significantly, behavioral controls introduce the possibility of unintended results or "side effects." Since by their nature, behavioral controls restrict an employee's freedom, resentment may occur. Another problem is the need for management to be consistent in the reward structure. If managers are told that employee development and team building are valued behaviors, but managers who produce the best financial results are promoted, it is clear which behavior is actually valued (Merchant, 1985).

Since behavior controls do limit freedom and monitoring behavior usually is, by its nature, intrusive, other potentially serious problems arise. These include invading employee privacy, and using control for disciplinary purposes. Controlling an employee's work life in areas not related or peripherally related to performance essentially constitutes an invasion of privacy, and will produce employee resentment, induce stress, and generate adversarial relationships between the workforce and management. The result is usually a decrease in net organizational productivity, an increase in turnover, and unfavorable financial results. The failure of managers to recognize the potential negative effects of control systems has resulted in a number of classic management failure cases (Merchant, 1985).

The motivation for imposing tight behavioral control can arise from the need to precisely control sensitive processes, and to achieve other "mission critical" objectives. However, a manager may impose more control in the widely held belief that "more is better" and organizational management culture may reinforce the belief system of an individual manager or a group of managers. It is important to realize that the right amount of control is only that which will generate a desired result. Results and side effects must be considered carefully before instituting a control system.

It is possible, using information system technologies, to monitor the actions and activities of individual employees at the translation level, and even the keystroke level. When the system is designed to record and allow a supervisor to review every action of an employee, a Panopticon has been created.

Panoptic systems allow for the ultimate control of employee behavior; they are behavioral control "gone nuclear." The potential for disastrous results are exponentially increased. Every act, every transaction, is recorded, complete with time and date stamps. Management is able to detect even minor missteps or departures from policy. The constant surveillance that normally produces conformity also will generate fear and risk aversion. These are not desirable traits to foster in employees.

CREATING A PANOPTICON: PANOPTIC VISION PLUS ACTION

While information technology can be used to create Panoptic vision, another component must be added to create a true electronic Panopticon. For Bentham's Panopticon to function as intended, there had to be a keeper to watch and discipline the errant subjects. This is also necessary to create an electronic Panopticon.

It is also possible to create a Panopticon without actually monitoring low level work behavior. In this type of Panopticon, managers may undertake the monitoring of the attitudes and beliefs of employees through the monitoring of electronic communications. Management's desire to have only loyal employees, and the general notion of loyalty to the organization in the name of success and cohesion is understandable. It is also, in all likelihood, impossible to completely attain. A disturbing example, somewhat reminiscent of the Panopticon described in Orwell's *1984* (Strub, 1989), of using information technology to engage in the widespread, systematic, surveillance of employees is described in *In the Age of The Smart Machine* by Shoshana Zuboff (1988).

Zuboff describes in vivid detail how in a company she calls DrugCorp (the name of the company is disguised), management undertook to detect and suppress "undesirable" attitudes and activities. DrugCorp had an electronic mail and bulletin board system, which was used by professionals, clerical staff, and managers. Communication of all types was on the system, including routine memos and announcements, sharing ideas, special interest bulletin boards, and personal messages. The communication flow was natural and uninhibited, and included negative comments about situations within the organization. The system was a considerable benefit for DrugCorp. This began to

change when one manager discovered a bulletin board on the system that contained material he considered to be offensive and a complete waste of corporate resources. After this manager took action, other managers used system management facilities to monitor messages on the system. At one point, management detected an "Equal Rights" electronic conference on the system. Management perceived this as a threat and users were called in to explain. Ultimately DrugCorp's system lost its effectiveness as users learned that management could and did regularly monitor content, and call potential dissidents to task (Zuboff, 1988). In this case, management clearly attempted to control not only behavior, but also attitude and thoughts.

This type of monitoring is trivial to accomplish. Anytime a person sends an e-mail message or visits a Web site using a company network, that message or request is subject to interception and analysis using readily available systems administration tools.

While it is unclear how widespread are e-mail and Web access monitoring practices, it is quite clear that the threat of monitoring is perceived as very real by users of these technologies. There are a number of stories in the MIS community that recount individual incidents where employees have been disciplined or terminated. While many of these stories are difficult, if not impossible, to verify, the persistence of these stories is evidence that they are believed many users.

IMPACTS ON INDIVIDUAL MORALE & PRODUCTIVITY

Managers who institute extensive Panoptic monitoring systems may expend considerable funds in the implementation process. While such systems are justified in the eyes of management by increases in productivity, there are a number of hidden costs. There is considerable evidence that monitoring is correlated with stress (Aiello & Kolb, 1995; Kolb & Aiello, 1996) and work related illness. It has also been suggested that monitoring is associated with absenteeism and employee turnover (Nussbaum & duRivage, 1986). Other research has associated electronic monitoring with lower task performance (Stanton & Barnes-Farrell, 1996).

Recent research has also shown that monitoring in customer service operations can actually lead to a loss of customers. Employees, in their quest to meet production volume standards, inadvertently damage relationships with customers. Employees are disinclined to take extra time with the customer on the phone, or they may not handle problems that are reported by customers, hoping that someone else will. Problems take time, and too many problems cause missed quotas. Difficult problems may be deferred for days until a situation is reached by the worker where it will not adversely impact the day's quotas (Grant, Christopher, & Irving, 1988).

THE DISCIPLINARY ORGANIZATION

We have seen that Panoptic technologies can be used to create Panoptic power, the ability to continuously monitor and supervise an individual's behavior. Indiscriminate, widespread, use of Panoptic power, including the monitoring of Internet utilization, may give rise to the phenomenon of a Disciplinary Organization, where power and thereby control, arises from the primarily from the continuous surveillance of the members, and the consequent ability to correct or discipline errant members. Under such conditions of continuous surveillance the relationship between manager and subordinate becomes adversarial, rather than cooperative.

A classic example of a disciplinary organization was ITT under the tenure of Harold Geneen as its CEO (Hopper & Macintosh, 1993). This organization created a system that sought to control management behavior. Managers were compelled as part of an elaborate planning process to produce a commitment to achieve certain financial results. The corporate staff undertook to monitor the behavior and progress of division managers through an elaborate system involving information systems, a series of interlocking reporting relationships, and a monthly reporting process where the CEO himself "examined", personally, each of the division managers in public meetings. The stress of working in such a highly visible environment compelled compliance and created maladaptive behaviors in some cases. While the ITT case is not an example of a true panopticon in the sense that it could monitor personal behavior, it had the same effect in that it compelled compliance with set of behaviors by making every managerial act subject to review and correction by a higher authority.

CONCLUSION

This paper demonstrated how modern, electronic Panopticons function to provide management with the most amount of control possible over the work and task environment. It also showed that such control measures, if implemented in a Draconian fashion can actually harm, possibly irreparably, the organization.

In spite of the potential negative side effects of electronic Panopticons, many organizations will continue to implement systems that deliberately or inadvertently create Panoptic vision. Informed management's should take steps to implement and manage these systems to avoid or at least mitigate, the problems.

The question of whether Panoptic vision leads inexorably to Panoptic power is very difficult to answer. Recall that for Panoptic vision to produce Panoptic power, an additional ingredient, management action, is required. Without action based on the system in question, Panoptic power cannot arise. However, even if used infrequently, the system will give rise to Panoptic power. The jinni will have escaped from the bottle.

Will managers confronted with an opportunity to use such a system actually go ahead, or will they "just say no"? I suspect that the temptation will prove too great. Control is seductive. In spite of continued warnings of the potential dangers, the pressures of modern competition will be too great, and eventually the temptation to impose strict controls using such systems will prevail.

True Panoptic systems should be implemented as a "last resort." Management must first consider other alternatives. Only once these are ruled out should Panoptic systems be considered. The key to the use of any Panoptic system technology is to avoid the appearance of control for control's sake, and to avoid controlling trivial matters. In this manner, an individual will be afforded privacy, but control will be maintained. Enforcement would be through social forces rather than by direct supervision (Ouchi & Maguire, 1975). Individual monitoring should be done of individual employees only during their initial training period. Once an employee passes through the probationary period, individual monitoring should be discontinued unless there is specific evidence of a problem.

It is ironic that the technologies that have the power to fundamentally change the workplace and provide more flexibility for both worker and manager can be used to create Panopticons. Ultimately, the Panopticon deliberately deprives the worker, like the prisoner, of freedom, privacy, and finally, dignity. Managers who sow the wind may reap the whirlwind.

REFERENCES

Aiello, J. R. & Kolb, K. J. (1995) Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress, Journal of Applied Psychology, (June): 339-354

Anderson, E. & Oliver, R. L. (1987) Perspectives on behavior-based vs. outcome-based sales force control systems, Journal of Marketing, (October): 76-88

Foucault, M. (1979). Discipline and punish: The birth of the prison, New York: Vintage Books

Grant, R. A., Higgins, C. A. & Irving, R. H. (1988) Computerized Performance Monitors: Are They Costing You Customers?, Sloan Management Review, (Spring): 39 - 45

Hopper, T. & Macintosh, N. (1993). Management accounting as disciplinary practice: The case of ITT under Harold Geneen, Management Accounting Research, (4): 181-216

Merchant, K. A. (1985). Control in Business Organizations, Boston: Pitman Publishing Co.,

Nussbaum, K., & duRivage, V. (1986) Computer monitoring: Mismanagement by remote control, Business and Society Review, (Winter): 16 - 20

Ouchi, W. G. & Maguire, M. A. (1975) Organizational Control: Two Functions, Administrative Science Quarterly, (December): 559 - 569

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, (December): 738-745

Strub, H. (1989). The theory of panoptical control: Bentham's panopticon and Orwell's *1984*, The Journal of the History of the Behavioral Sciences, (January): 40 - 59

Tuerkheimer, F. M., (1993). The underpinnings of privacy protection, Communications of the ACM, (August): 69-73

Zuboff, S. (1988). In the Age of the Smart Machine, New York: Basic Books