The Ethics Of Cyberveillance In A Global Context

John F. Veiga, (Email: Jack.Veiga@business.uconn.edu), University of Connecticut, Storrs
Jeffery Thompson, Miami University, Ohio
Richard Dino, University of Connecticut, Storrs
Irene Hau Siu Chow, Chinese University of Hong Kong, Hong Kong
Eleanor O'Higgins, University College, Ireland
Ali bin Khalifa Al Khalifa, University of Bahrain, Bahrain

Abstract

Whether one calls it "cyberveillance," "cybermonitoring," "cybersnooping," or "cyberspying," one thing is clear, the computer activities of employees are increasingly being monitored by their companies. Some reports suggest that up to 17% of the Fortune 1,000 companies now utilize some form of computer monitoring software and the predictions are that this figure will jump to 80% very soon. Such software allows an employer to monitor virtually every message sent, website visited and key stroked. Given the global reach of many of these large firms, there are at least two major concerns that need to be addressed. First, what are the ethical implications of this practice? Given that 12% of all firms report that they do not notify their employees of their monitoring activities, are employees being treated fairly? And second, in what ways are local customs, mores and values in various parts of the world being violated or ignored?

Like it or not, we are awash in what various popular writers have termed "cyberveillance," "cybermonitoring," "cybersnooping," or "cyberspying." Simply put, employees' use of the Internet and email today are increasingly being monitored by their companies. What seems to be missing in this rush to monitor are the ethical implications of doing so, which are significantly exacerbated in multinational firms. In order to understand how such actions are likely to be seen from a variety of multinational perspectives, we first developed a case involving a multinational company contemplating cybermonitoring and then we queried a group of international scholars, asking them to first approach managers in their region for reactions to the case, and then to provide a summary and synthesis of as to how such actions would be received in their respective parts of the world. Finally, we conclude by presenting a reasoned analysis regarding the general ethical questions involved.

Before you read this analysis, we invite you to first read the case below and think about your own reactions. This is a hypothetical case involving composite information from the popular press involving a multinational bank. The bank is trying to decide if it should purchase and utilize monitoring software.

The Case of Cyberveillance at Global Banking Ltd.

Global Banking Ltd. is a 100-year-old American Company that specializes in retail banking and financial services. Global has several major locations around the world and is organized primarily by geographic region. In the most recent fiscal year, Global reported assets in excess of $50 billion (U.S.). Global is a well-managed, relatively fast-paced, bank with a culture that inspires employee loyalty and trust. Global credits their success to their utilization of the best people and technology in the world.

The bank is considering the installation of software on its global Intranet that will monitor every employee's computer activity, both on-line and off-line. Monitoring would be done on every message sent, every website visited, every file formatted and every key stroked, even if the employee never stored the data.

Before proceeding further with this new software installation, Global's CEO, B.J. Murphy decided it would be worthwhile to get some initial reactions from managers in the various geographic regions as to the appropriateness of installing this software. Accordingly, Murphy sent the following memo:

To: All Geographic Division Managers
From: B.J. Murphy
Re: Monitoring Software

Recently, I saw a survey by the American Management Association that reported increasing corporate use of sanctions against violators of their rules on computer use. Twenty-eight percent of the companies in the survey said they have dismissed employees for misuse or personal use of telecommunications equipment. Indeed, 17% of the Fortune 1,000 companies now have monitoring software. Last week when I spoke to a colleague at Xerox, she told me Xerox had fired 40 employees for what it deemed inappropriate use of the Internet.

While I am not an alarmist, nor do I believe that we have a serious problem at this time, I have spoken with representatives of several firms that make monitoring software a practice. They assure me that it is quite easy to maintain. However, before I proceed, I wanted to get your reactions to installing this software. For example,

- *How do you think employees in your culture will feel about being monitored?*
- *Should we tell employees we are doing this and, if so, what policy statement ideas do you have for presenting this to all employees?*
- *What about our corporate culture? Does this kind of surveillance damage our strong reputation for loyalty and trust?*
- *Would you recommend proceeding? And if so, how should we implement?*

I would appreciate hearing your reactions to these issues at our next subsequent meeting. Please come prepared to discuss these issues and, in particular, "local" issues as they relate to your culture. While I am mindful that all of us have not worked together in the past given our geographic locations, I am quite confident, given each of your special talents, that you can develop recommendations that will benefit our shareholders, and our employees. I look forward to your recommendations.

The European Perspective

While there is some diversity in culture among European countries, certain general observations about the European context can be made. Broadly speaking, varying adherence to a social democratic model exists in all EU countries. The stakeholder model is very much in favor in Europe, in contrast to the shareholder model that prevails in the U.S. This means that the power of management—as agents of the owners of the business—relative to workers is nowhere near as great as one would expect to find in the U.S. Since employees are important stakeholders in the European enterprise, it is not surprising, then, that we find directives that guarantee working conditions, minimum wages and general workers' rights.

It is interesting that the country that most resists these directives is the UK, perhaps the EU country that is closest to the U.S. in culture and management practices. These differences are illustrated in a study comparing British and French practices in the development and content of mission statements (Brabet & Klemm, 1994). The

French involved most employees in the process, along with outside constituencies, such as clients. British companies' mission statements were developed by senior management, with occasional middle management participation. British statements were more specific with shorter-term measurable objectives, while French statements had broader long-range aspirations encompassing social and community values.

It is within this context—i.e., employees as important stakeholders—that issues related to surveillance and the individual's right to privacy collide. The right to privacy has been enshrined in an EU data protection directive that upholds several principles. First, the collection of data about an individual and its specific purposes should be disclosed to the individual, the individual should have the right to opt out, and in the case of especially sensitive data, should only be included in the data collection if there is a choice to opt in. Second, the individual should have access to the data and a means of correcting it, as appropriate. Third, the holder of the data should ensure its security and protect against transfer of the data without the consent of the individual concerned. Fourth, the data should be used only for the specific purpose stated. And fifth, the individual should have judicial recourse in the event of legal abuse by the holder of the data. Interestingly, in the UK, a law was enacted in October, 2000, allowing broad surveillance of staff without their consent, although with their knowledge. This law will probably be tested against a Human Rights Act passed in the UK earlier in 2000. Thus far, there is a general perception that employers have won out against trade unions and civil liberties groups (Eaglesham, 2000).

Given this context, one would expect resistance and a negative attitude to the notion of surveillance in Europe. However, to test this assertion more fully, the Global Banking case was presented to individuals in France, Ireland, Italy and Spain to gauge reactions. In France, Ireland and Spain, subjects answered each of the four questions posed in the case in detailed writing, and their responses are reported below. In Italy, the case was discussed in a group and the general consensus of the group is reported. In France the respondents were 49 final year business undergraduates. In Ireland (N=33), Italy (N=24), and Spain (N=15), the respondents were postgraduate business executives. Here's what we found:

1. How do you think employees in your culture will feel about being monitored?				
Response	**France**	**Ireland**	**Spain**	**Total**
Positive	0 (0%)	3 (9%)	0 (0%)	3 (3%)
Necessary evil	9 (18%)	6 (18%)	2 (13%)	17 (18%)
Negative	40 (82%)	24 (73%)	13 (87%)	77 (79%)

2. Should we tell employees we are doing this? **All respondents answered *affirmatively.***

3. What about our corporate culture? Does this kind of surveillance damage our reputation for loyalty and trust?				
Response	**France**	**Ireland**	**Spain**	**Total**
Yes	40 (82%)	22 (67%)	12 (80%)	74 (77%)
Neutral/Mixed	4 (8%)	4 (12%)	2 (13%)	10 (10%)
No	5 (10%)	7 (21%)	1 (7%)	13 (13%)

4. Would you recommend proceeding?				
Response	**France**	**Ireland**	**Spain**	**Total**
Yes	2 (4%)	5 (15%)	4 (27%)	11 (11%)
Conditional	11 (22%)	10 (30%)	5 (33%)	26 (27%)
No	36 (74%)	18 (55%)	6 (40%)	60 (62%)

The consensus of the Italian group was similar to the findings of the other groups—a negative reaction to the whole idea and that it constituted a breach of trust and should not proceed. And, if management chose to proceed, employees should be told. Thus, there is considerable negative reaction all around. To invoke a system such as the one proposed is seen as counterproductive to real control through commitment, and demoralizing. Some

responses indicated a feeling of being insulted, of being treated like a child. An overwhelming majority thought the solution proposed was too drastic. However, few alternatives were suggested, other than that loyalty and commitment are better than external monitoring. Most respondents were of the opinion that limited personal use of company email and the Internet is acceptable, and those who stay within such limits should not be subjected to what they regarded as harassment. The phrase "big brother" was used in several instances. An invasion of privacy was also given as a reason to avoid the kind of monitoring system proposed in the Global Banking case. Indeed, several respondents queried the legality of the whole operation.

It can be seen that a small number of respondents saw the proposed cyberveillance as undesirable, but a necessary evil, understandable in the circumstances. In some cases, respondents saw the monitoring practice as more acceptable in larger multinational companies. Several people also considered the practice as quintessentially American, not in the European tradition, and hoped it would not spread to Europe.

A minority of respondents acquiesced with the Global Banking monitoring proposal only under certain conditions. These were suggestions such as invoking the system only temporarily, consulting with everyone concerned, and generally using a "light touch." With respect to the overwhelming view that employees should be informed, this is in line with the EU privacy directive.

The Asian Perspective

Hong Kong provides an interesting case to study the privacy-ethical issue, especially in the context of a modern and westernized economy with a Chinese culture. Hong Kong is rated by the Heritage Foundation as the world's freest economy. Following the British tradition, Hong Kong people enjoy freedom and privacy protection. Unlike their counterparts in China and Taiwan, Hong Kong Chinese are very individualistic in the workplace. In addition, the workforce of Hong Kong is generally well educated. For sure, they are neither used to, nor willing to be monitored under any circumstances or by any method. The surveillance system definitely will hurt the morale and loyalty of our people. The trusting relationship that takes a long time to build may become very fragile under surveillance.

The Chinese society has historically been dominated by respect for hierarchy and obedience to authority. Subordinates will not openly challenge their superiors. In this traditional high power distance culture, subordinates will not strongly oppose the installation of a monitoring system. They will reluctantly accept and obey the new policy. In Hong Kong, while people are highly adaptable to change, they too will accept the new system but will need time to adjust to it. However, the installation of the monitoring software will be seen as a sign that employees lack self-regulation. Hence, unless the inappropriate use of computer resources is very serious, the installation of monitoring software is not recommended. Instead, in this context, the organization would be well advised to rely on employee self-restraint and self-control.

If monitoring software is determined to be essential, then it must be introduced in a very thoughtful way. Most importantly, managers need to fully explain the reasons for installing the system and justify the policy. The policy statement should explicitly point out that the intention is not to invade employee privacy, but to make more efficient use of the company's resources. Employees need to be assured that they are protected by privacy ordinance. The message should be transmitted top down. And, because employees in Hong Kong tend to be very vocal about their rights and interests, opinions should be obtained in advance through some type of open forum. It is important to cultivate a sense of fairness, equality, and open-mindedness in order to maintain good relationships and to show top management's sincere respect for employees' rights. Finally, it is important that the penalty for violating the rules be clearly stated to help reduce the uneasy feelings of insecurity and worry about being fired. In sum, it is possible to initiate cybermonitoring, albeit with care and patience.

The North American Perspective

In the U.S., the capability of cybermonitoring is in many respects no different than the general class of monitoring capabilities engendered by prior advances in technology, such as the use of strategically placed video

surveillance cameras or the thorough analysis of call-log lists generated by communications systems. While there has been, historically and culturally, a general understanding and agreement by employees in North America that company assets are to be used exclusively for company purposes, there is also an expectation on their part of a fundamental guarantee to an individual's right to privacy (Handy, 2001). And clearly, cybermonitoring is precariously balanced on the fence between these two fundamental beliefs.

In the U.S., technology itself, as well as the complexities of the home/workplace environments, our continuously rising expectations of employee productivity and the evolution to more non-traditional working patterns (work/lifestyle balance) have helped to blur a once clear boundary between work time and home time. In turn, the workplace has invaded our homes and our homes have invaded the workplace. North American employees have come to expect that the employer's job is not to complicate this situation but to simplify it by doing whatever can be done to help them do their jobs to the best of their capabilities, ensuring the ultimate benefit to shareholders as the company attains its corporate goals. Put simply, employees should work toward the common good of the company with the expectation that the company has their best interests at heart.

There was unanimity among American managers queried that any policy that Global develops regarding cybermonitoring must be consistent with, and linked to both the organization's culture and the "American way," and reflective of the loyal and trusting relationship that has been built with their employees. Employees will understand and expect that linkage, as well as respect it. Any policy that is inconsistent with that linkage will send the wrong signal and undoubtedly have a negative impact on worker productivity, employee retention, corporate culture, and the achievement of the company's goals. Global does not want to send a message of mistrust, nor does it want to dilute its employees' commitment to the organization. Global wants to avoid creating an employee backlash that would most certainly come in the U.S.

The policy that is implemented must be designed to enable employee productivity and set the example for other firms who are struggling with similar challenges—that is Global must take the high ground. Contrary to the newly developing cyber-policies of many companies in the U.S, the template should be simple and easily understood, and it should stay that way even after Global attorneys review it and make their additions. Global must come down on the right side of this issue. In a sense, it could be a twin-win—by creating a policy that upholds the beliefs that employees can be trusted to do the right thing, and at the same time endorses cybermonitoring to the extent that it makes employees, who misuse company assets, think twice. Clearly, such thinking underlies a particular cultural phenomenon in the U.S—as a rule, North American workers tend to be highly individualistic, and hence loathe slackers and free-riders, believing all workers must carry their own weight. This belief is so ingrained and personalized, that to some extent they are willing to sacrifice some of their own privacy to prevent such behavior from occurring. While this attitude may also be good news for the company, management should never assume that employees are doing this primarily for the good of the company. Indeed, if nothing else, North Americans are driven by a sense of fairness and equity that transcends the firm.

Fairness means that employees will be trusted to do their jobs and appreciated for their contributions, that they will never be monitored without prior knowledge, and that they will always be notified when monitoring is to begin or end. On the other hand, equity means that monitoring will primarily be done to combat poor workplace performance, for example, low employee productivity, or alternatively, for suspicion of activities that are either illegal or can be construed as detrimental to fellow employees or the company.

The Middle Eastern Perspective

Every society has notions of what one should believe and how one should behave in order to avoid suspicion and unpopularity. Some at these societal conventions are given explicit formulation in legal codes, others are more intuitively judgmental, helped by a vast body of ethical and practical judgements described as "common sense". This dictates what we should wear, which financial values we should adopt, who we should respect, what etiquette we should follow and the style of domestic life we should lead.

The Middle East as a region presents a national grouping of relatively tightly knit countries with one cultural heritage, common moral and religious standards and general, uniform modes of living. The Middle East also provides a unique and strategic area of management practice, given the family structure and the relationship between family members, the degree of acceptance of authority in society, economic conditions and overall standards of living. Hence, any managerial decision should not change employees' social values, culture, family structure, and individual pride.

Western managers must understand various aspects of Arab culture to improve their management strategies in this environment. In the Middle East, personal status depends on family position and social contacts. A Middle Easterner is usually content with the status quo and is always ready to state an opinion. The predominant religion of the countries in the region is Islam. Islamic values and traditions influence behavioral attitudes toward the conduct of business and attendant management practices. As a result, for business managers in the Arab world it is of paramount importance to learn and understand central Islamic values and influences, most importantly an emphasis on high ethical standards, the principles of egalitarianism, and the Moslem's belief in God's control over personal events in his life. Moslems approach their religion as a total system containing its own political-legal, economic-technological, and socio-cultural aspects.

For western managers to work in this environment, they must first come to realize that their cultural values are likely to differ significantly from Middle Eastern values. Global's proposed monitoring scheme is likely to face stiff resistance in the Middle East, since there is a reluctance to impose discipline and a reluctance to accept discipline there. Employees would react unfavorably to being monitored and possibly disciplined.

However, this lack of willingness to accept discipline can be overcome. Initially, Global should monitor everyone but only discipline the extreme cases and then only after a set of procedures are established, such as verbal and written warnings. The news of the penalties on the extreme cases will likely reduce the number of instances of misuses. If this is done carefully, over a reasonable period, it should lead to improving overall discipline and confrontation will be avoided.

In general, it is rather difficult to imagine, at least in the foreseeable future, superimposing such advanced management systems on societies who put more emphasis on human relationships and traditional values. Clearly, western management practices should not be transferred blindly to the Middle East. What is needed is an evolutionary process in which change is introduced gradually, over time, as opposed to a revolutionary process where change is forced upon employees without regard for their the culture. Clearly, lessons can be learned from Japanese multinationals that frequently engage in business in the Middle East. They have achieved success in part because they were able to first recognize and thoroughly understand cultural differences. Moreover, the Japanese have shown an ability to exercise patience in educating middle eastern workers which in turn has resulted in transforming managerial practice to fit the Japanese mold. Such lessons suggest that cultural analysis and sensitivity applied with abundant patience, throughout their implementation, are critical to achieving success in the Middle East.

A Concluding Ethical View

Companies that electronically monitor employees navigate treacherous ethical waters. Although Global Banking’s right to dictate the use of its resources (including employee computers) is uncontroversial, its claim of control over employee communications and intellectual activities is ethically problematic. Whenever a company intervenes covertly in the process of interpersonal communication or individual formulation of ideas, privacy is threatened. Note that argument does not extend to monitoring employee use of the Internet. Internet “surfing” typically does not involve an intellectual exchange. Monitoring of Internet use is thus less morally questionable than the monitoring of communications or idea formulation. Companies are generally justified in preventing inappropriate Internet use through monitoring.

Kantian moral philosophy enshrines the dignity of individuals as moral agents, who deserve to be treated as ends in themselves rather than as means to another’s end. As has been argued elsewhere, “monitoring submits to

scrutiny, that which was intended only for the eyes of a trusted other, and thus inhibits the communicator's ability to autonomously choose how and with whom to communicate… [Monitoring], especially when covert, treats people as a means to a corporate end, rather than as ends in themselves that warrant respect and have certain rights to privacy. Such covert monitoring leads to a sacrifice of human dignity (Thompson, DeTienne & Smart, 1995, p. 160).

Ethicists have pointed out that covert monitoring may also sacrifice other important features of the work context that have both moral and practical import. For instance, privacy of communication is an important aspect of trust building among co-workers. When employees suspect they will be monitored, their electronic communications may become formal and impersonal, and less likely to breed the intimacy that underlies effective and trusting relationships at work. Global Banking might undermine its culture of trust and collaboration if it adopts electronic monitoring.

Another likely casualty of monitoring is individual uniqueness. As Bloustein (1964) argued, the person "…whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being…is not an individual" (p. 188).

The leaders of Global Banking should contemplate the impact of their monitoring policy on the willingness of employees to express fresh ideas either via e-mail or in preliminary written drafts on their computer screen. Such ideas are usually raw, incomplete, and perhaps even politically volatile in their nascent form. If Global Banking begins to monitor every computer keystroke, employees may suppress the individuality and uniqueness that is the germ of innovation.

If Global Banking decides, after taking these issues into consideration, that it does need to monitor employees after all, the ethical view must make one essential demand—to inform employees about the policy. As Benn (1984) has argued, "Covert observation—spying—is objectionable because it deliberately deceives a person about his world" (p. 241). Such deception lies at the heart of what Kant meant when he spoke of treating another individual "as a means only." If electronic monitoring is to be performed ethically, public notice of the monitoring is a minimum requirement—in all parts of the world.

References

1. Benn, S. I. 1984. Privacy, freedom and respect for persons. In *Philosophical Dimensions of Privacy: An Anthology*, New York: Cambridge: 223-244.
2. Bloustein, E. J. 1964. Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review,* 39: 962-1007.
3. Brabet, J. & Klemm, M. 1994. Sharing the vision: Company mission statements in Britain and France. *Long Range Planning*, 27: 84-94.
4. Eaglesham, J. 2000. Staff privacy in the spotlight. *Financial Times*, October 9: 18.
5. Handy, C. 2001. Tocqueville revisited: The meaning of American prosperity. *Harvard Business Review*, January: 57-63.
6. Thompson, J. A., DeTienne, K. B. & Smart, K. L. 1995. Privacy, e-mail and information policy: Where ethics meets reality. *IEEE Transactions on Professional Communications*, 38: 158-164.

Notes