

Surveillance in the workplace

Prof. Simon Rogerson

Dr. N Ben Fairweather

**Originally published as ETHicol in the IMIS Journal Volume 8
No 3 (June 1998)**

In this edition we consider some of the issues associated with electronic surveillance in the workplace. While there is no doubt that employers have a legitimate interest in a certain amount of monitoring of their employees, to ascertain employee efficiency and effectiveness, there is also no doubt that employees are not slaves and as such should not be required to reveal their whole selves to their employer. To allow intimate information to remain private, both traditional workers and teleworkers should not normally have personal communications under surveillance by their employer, and the employer should not routinely monitor the length of time employees spends away from their work during the working period.

Over the last few years, software packages have made electronic performance monitoring possible. This significantly expands the scope of management to collect and process data on their workers. Monitoring will be more intense when workers use, for example, e-mail, video conferencing and dedicated on-line systems to carry out their work.

The practice of monitoring workers' communications is widespread. Richard Spinello suggests that it is carried out in a covert fashion by a growing number of firms such as Pillsbury, UPS, and Intel Corporation. According to The New York Times others, for example, Kmart Corporation have adopted a policy that allows the company to review all e-mail messages, and every employee is informed of this policy at orientation meetings.

Fear that communication is being monitored may make employees less likely to use company resources for personal business. However, in a society where many employees work full-time and many live alone there may be no choice but to conduct some personal business from workplace. This need is especially strong for those working conventional hours as these are likely to be the only opening hours of many of the offices that they need to deal with in their private lives. In such circumstances, it is unreasonable for an employer to expect that no use at all is made of company time and resources for private business that remains private. However, when use for private business is significantly detrimental to the performance of the job that the employer has paid for, or uses a valuable quantity of resources, it is reasonable for an employer to take action, which might include monitoring.

Whilst employers might argue that electronic monitoring acts as an effective deterrent against fraud, industrial espionage and other illegal activities this does not give them a universal right to monitor their employees. Most of us would not consider it acceptable if all of our post were read, which is why there are laws against such interception of post. Just because there is the possibility that someone might abuse e-mail does not mean that everyone's e-mail should be monitored. The civil liberties of innocent people should not be suppressed because a few rogue employees might abuse those liberties. If a company has legitimate suspicions that someone is using its e-mail system for illegal reasons, it should investigate and take any necessary action. A breach of privacy would surely be justified under such circumstances as long as there are appropriate procedural safeguards. When there are no such suspicions, the possibility of such abuse of the systems should not outweigh the reasonable expectation of employees to be trusted by their employer.

On 25 June 1997, the European Court of Human Rights ruled that workers have a "reasonable expectation" of privacy in making and receiving telephone calls at work. It is reasonable to assume that this applies equally to e-mails and other communications at work. Some organisations contend that because they own the computer resources on which e-mail messages are transmitted, they should have an unconditional right to control and monitor the contents of those messages. The European Court of Human Rights was quite clear that ownership does not permit surveillance, in rejecting the UK Government's case that taps of telephones were not in breach of human rights where telephones were government property.

Monitoring is particularly likely with e-mail because unlike other forms of communication e-mail provides an easy means of saving and inspecting messages for many years. With other forms of communication, the setting up of recording and monitoring may be relatively complex and time consuming. With e-mail messages already in ASCII code, using a computer to search large numbers of e-mails for mentions of particular words is as easy as searching in a document being word-processed.

One worry with all types of surveillance and monitoring is that they give power over those monitored to those who carry out the monitoring. This may be greater than the power it is appropriate for them to have, especially when they come to know intimate information about those monitored. This can cause a variety of problems, including breaches of internal security and giving knowledge that amounts to organisational power to those who do not deserve it.

The fear that intimate or organisational information may fall into the wrong hands may lead those who are subject to surveillance or monitoring to be constantly apprehensive and inhibited in actions and communication that may be monitored. In such circumstances employees may feel they are under surveillance of a kind they resent more than traditional workplace monitoring. Where technological methods have been introduced for such detailed monitoring or surveillance, they have in some cases been associated with very low employee morale.

Peer-to-peer communication always exists within any work situation. Business and personal matters become interspersed as workers inadvertently discuss aspects of their personal lives as they conduct business. Such interactions have the potential to make even the most boring jobs bearable. Furthermore, such informal communication can provide the breeding ground for ideas about how work processes could be improved and waste reduced.

If such peer-to-peer communication is facilitated through video conferencing, e-mail or telephone calls at the employer's expense, there may be a strong potential for surveillance of such peer-to-peer communication. Managers may have a fear of such communication, as it enables workers to share stories detrimental to the image of the manager, or co-ordinate complaints. Equally, such time spent not at the primary work task could be seen by managers as wasted time. Such concerns may lead managers to pay particular attention to peer-to-peer communications. Such action might stifle team building and valuable information exchange, and ultimately might lead to a reticent workforce.

Most would agree that some workplace monitoring is a legitimate and essential management activity. However, there is a suspicion that close technological monitoring takes place more because it is technologically easy than because there is any great need for it. It is then that monitoring crosses the line into unethical business practice.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<srog@dmu.ac.uk>
Home Page: (<http://www.ccsr.cse.dmu.ac.uk>)

