Privacy, the Workplace and the Internet

Seumas Miller
John Weckert

ABSTRACT. This paper examines workplace surveillance and monitoring. It is argued that privacy is a moral right, and while such surveillance and monitoring can be justified in some circumstances, there is a presumption against the infringement of privacy. An account of privacy precedes consideration of various arguments frequently given for the surveillance and monitoring of employees, arguments which look at the benefits, or supposed benefits, to employees as well as to employers. The paper examines the general monitoring of work, and the monitoring of email, listservers and the World Wide Web. It is argued that many of the common justifications given for this surveillance and monitoring do not stand up to close scrutiny.

KEY WORDS: email, internet, monitoring, privacy, surveillance, workplace, World Wide Web

The coming into being of new communication and computer technologies has generated a host of ethical problems, and some of the more pressing concern the moral notion of privacy. Some of these problems arise from new possibilities of data collections, and software for computer monitoring. For example, computers can now combine and integrate data bases provided by polling and other means to enable highly personalised and detailed voter profiles. Another cluster of problems revolves around the threat to privacy posed by the new possibilities of monitoring and surveillance. For example, telephone tapping, interception of electronic mail messages, minute cameras and virtually undetectable listening and recording devices give unprecedented access to private conversations and other private communications and interactions. Possibly the greatest threat to privacy is posed by the possibility of combining these new technologies and specifically combining the use of monitoring and surveillance devices with certain computer software and computer networks, including the Internet.

Concerns about the use of computer technology to monitor the performance and activity of employees in the workplace are not new (see Garson, 1988; and Zuboff, 1988), and are widely discussed from a variety of perspectives, frequently in computer ethics texts. Johnson (1995), and Forester and Morrison (1991) raise questions regarding the monitoring of work, while Langford (1995) and Severson (1997) both discuss the monitoring of employees email. The works just cited mention arguments both from the point of view of employers and employees. Parker et al. take a different approach (1990). Their discussion is based on a survey taken of attitudes towards monitoring both employees email and computer usage. Similar surveys have also been reported recently by Loch et al. (1998) and Hawk (1994). There are also a number of sociological examinations, including those by Perrolle (1996) and Rule (1996). An argument from the employees' point of view, highlighting employees' problems and concerns is given by Nussbaum (1989). A number of other important discussions are considered later in this paper.

These discussions are useful, but their purposes are different from the current one in this paper. Applied ethics is interdisciplinary by nature, so questions must be examined from a variety of perspectives. Some of the works just cited highlight the problems or perceived problems, some report on what people actually believe, and some give a sociological analysis. The concern in this paper is to examine the question of employee

Journal of Business Ethics **28**: 255–265, 2000.

monitoring from a philosophical point of view. Hence the emphasis is on analysis and argument, not on original empirical research.

Provision of an adequate philosophical account of the notion of privacy is a necessary precursor to setting the proper limits of intrusion by the various new technologies. Such an account of privacy would assist in defining the limits to be placed on unacceptably intrusive applications of new technologies. Moreover it would do so in such a way as to be sensitive to the forms of public space created by these technologies and not unreasonably impede those new possibilities of communication and information acquisition which are in fact desirable. As always it is important to balance the rights of individuals against the needs of the community. On the one hand there is a fundamental moral obligation to respect the individual's right to privacy, on the other hand there are the legitimate requirements of, for example, employers to monitor the performances of their employees, and law enforcement agencies to monitor the communications and financial transactions of organised crime. Moreover the working out of these ethical problems is relativised to a particular institutional and technological context. The question as to whether email, for example, ought to be assimilated to ordinary mail depends in part on the nature of the technology in question and the institutional framework in which it is deployed. Perhaps email messages sent on a company owned computer network ought to be regarded as public communications within the organisation however personal their content. These email messages, unlike ordinary mail, are always stored somewhere in the backup system owned by the company and are therefore accessible to the dedicated company cybersleuth (Magney, 1996). In this paper the discussion will be restricted to the notion of privacy with reference to computer monitoring in the workplace. First, an outline of the general notion of privacy.

The notion of privacy has proven to be a difficult one to adequately explicate. One account which has been influential is that by Parent:

> Privacy is the condition of not having undocumented personal knowledge about one possessed by others. . . . [P]ersonal knowledge . . . consists of facts about a person which most individuals in a given society at a given time do not want widely known about themselves (Parent, 1992, p. 92).

A problem with this definition is that personal knowledge and, therefore, privacy, is completely relativised to what people in a particular society, at a particular time, are prepared to disclose about themselves. Accordingly, if in some society everyone is prepared to disclose everything about themselves to everyone else, then they are still, on this account, in a condition of privacy. But they are surely not in a condition of privacy. Rather, they have chosen to abandon such a condition.

Presenting an alternative account is not easy, however, there are a number of general points that can be made (Miller, 1997; Benn, 1988; Warren and Brandeis, 1890). First, the notion of privacy has both a descriptive and a normative dimension. On the one hand privacy consists of not being interfered with, or having some power to exclude, and on the other privacy is held to be a moral right, or at least an important good. Most accounts of privacy acknowledge this much. For example, Warren and Brandeis gave an early and famous definition in terms of the right to be let alone. Naturally the normative and the descriptive dimensions interconnect. What ought to be must be something that realistically could be. The normative dimension of privacy is not a fanciful thing. The proposition must be rejected that the extent and nature of the enjoyment of rights to individual privacy is something to be determined by the most powerful forces of the day, be they market or bureaucratic forces. But it is equally important to avoid utopian sentimentality; it is mere self-indulgence to pine after what cannot possibly be.

Second, privacy is a desirable condition, power or moral right that a person has in relation to other persons and with respect to the possession of information by other persons about him/herself or the observation/perceiving of him/herself by other persons. The kind of "interference" in question is cognitive or perceptual (including perhaps tactile) interference.

Third, the range of matters regarded as private embraces much of what could be referred to as a person's inner self. A demand – as opposed to a request – by one person to know all about another person's thoughts, beliefs, emotions, and bodily sensations and states would be regarded as unacceptable. Naturally there are conditions under which knowledge concerning another person's inner self are appropriate. A doctor, counsellor, psychoanalyst or psychiatrist may need to know about a patient's bodily sensations and states, in so far as this was necessary for successful treatment and in so far as the patient had consented to be treated. Nevertheless such information while no longer unavailable to the doctor or other care worker, would still be unavailable to others, and for the care worker to disclose this information would constitute a breach of confidentiality, except perhaps to another who may be required to assist in the treatment.

Fourth, a person's intimate personal relations with other people are regarded as private. So while a lover might be entitled to know his/her lover's feelings toward him/her, others would not be so entitled. Indeed there would typically be an expectation that such information would not be disclosed by a lover to all and sundry.

Fifth, certain facts pertaining to objects I own, or monies I earn, are held to be private, at least in most Western societies, simply in virtue of my ownership of them. Ownership appears to confer the right not to disclose information concerning the thing owned. Or at least there is a presumption in favour of non-disclosure; a presumption that can be overridden by, for example, the public interest in tax gathering.

Sixth, certain facts pertaining to a person's various public roles and practices, including one's voting decisions are regarded as private. These kinds of facts are apparently regarded as private in part by virtue of the potential, should they be disclosed, of undermining the capacity of the person to function in these public roles or to compete fairly in these practices. If others know how I vote, my right to freely support a particular candidate might be undermined. If business competitors have access to my business plans they will gain an unfair advantage over me. If a would-be employer knows my sexual preferences he or she may unfairly discriminate against me.

Seventh, and more generally, a measure of privacy is necessary simply in order for a person to pursue his or her projects, whatever those projects might be. For one thing reflection is necessary for planning, and reflection requires privacy. For another, knowledge of someone else's plans can enable those plans to be thwarted. Autonomy requires a measure of privacy.

Equipped with this working account of privacy, including a basic taxonomy of the kinds of information regarded as private, let us now consider a number of ethical issues posed by computer monitoring and surveillance in the workplace.

Employers clearly have some rights in seeing that their employees are working satisfactorily. It is not only in the employer's interests that the required tasks are performed efficiently and well. It is also in the interests of other employees and in the interests of the general public. Employees do not want to have to work harder to support lazy or incompetent colleagues. Consumers do not want to buy sub-standard or overpriced products. But it does not follow from this that employees have no right to privacy when at work. Unfortunately, although some may say fortunately, the widespread use of computers has made workplace surveillance very easy.

Does this monitoring and surveillance matter? It is often defended by employers, who argue that it is in the interests of all. Employees who are not performing well are weeded out. Those doing their job well can be rewarded on objective criteria. In addition, and probably most importantly, it leads to more efficient and profitable businesses. But there are other important things in life besides efficiency and profitability. In particular, there is the right to privacy. As was indicated above, privacy considerations take a number of forms. All of these are conceivably relevant to employees in their place of work.

The existence of the right to privacy, and related rights such as confidentiality and autonomy, is sufficient to undermine extreme views such as the view that employees ought to be under surveillance every minute of the

working day, or that should they be in a situation where every minute of the working day they suspect that they might be under surveillance, or that there should there be surveillance of a nature or extent in respect of which the employees are ignorant. These extreme situations involve unjustified invasions of privacy. Employers have certain rights in respect of their employees, but there is no general and absolute right to monitor and control employees. This is obvious from the fact that employers are restricted in a whole range of ways by the rights of employees. Employers cannot imprison or rob their employees, and flogging, in order to improve productivity, is not generally condoned. The reason, obviously, why employers cannot imprison or rob (or flog), is that these activities are violations of a human's rights, and the fact that someone is your employee does not confer the right to violate those rights. Even in cases where explicit contracts have been agreed to, there are limits to which either party can go in order to ensure that the other party adheres to that contract.

So much is obvious. What is less obvious is the extent to which an employer can justifiably infringe an employee's right to privacy. It has already been argued that there is a right to privacy, and, other things being equal, employees have this right. The violation of the employee's right to privacy of concern in this paper, is that posed by the electronic surveillance and monitoring of an employee's activities made easy by current computer technology, particularly networking. Keystrokes can be monitored for speed and accuracy, and the work on your screen may be brought up on the screen of another without your knowledge. Common software for accessing the Internet logs all activity, so that a record is kept of all visits to all sites, and email, listservers and so on can monitored. A supervisor can fairly easily find who did what on the Internet. Notwithstanding these technical possibilities of infringing privacy, protection of privacy is high on the list of principles supported by many professional computing association codes of ethics (Barroso, 1997). A good example is found in the Association for Computing Machinery (ACM) code:

> Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals . . .
>
> This imperative implies that only the *necessary amount of personal information* [emphasis added] be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance (1992).

(This code, it should be noted, is the code of a professional computing body, and hence is aimed at computer professionals who often have access to private information stored electronically, in their daily work of creating, managing and maintaining computer systems and networks. There is no implication that *only* computer professionals have responsibilities with respect to individual privacy.)

The quotation above makes it appear that employee monitoring by computer technology is frowned upon by the ACM, and that computer professionals should have no part of it, either in developing necessary software or involvement in the monitoring itself. It could be argued, however, that this surveillance of employees falls within the class of a "necessary amount of personal information"; necessary to the well-functioning of a business. In order to assess the justifiability of computer monitoring, first some arguments for it will be considered, followed by a consideration of a number of criticisms.

Employees, as well as having at least a prima facie right to privacy, are also accountable to their employers because their employers have a right to a reasonable extent and quality of work output for the wages and salaries that they pay, and it is in the employees' interests (as well as the inter-

ests of employers) that their employers make a profit. Given potential conflict between these rights, perhaps an employees' right to privacy, *qua* employee, can, in a range of circumstances, be overridden. Three related types of justification are given, in terms of employers, customers, and employees. The most obvious is that with better monitored employees, profitability is greater, although this is sometimes couched in terms of better quality customer service. For example, "quality of service telemarketing monitoring" is the way that the Telemarketing Association portrays employee monitoring (*Direct Marketing*, 1993). The Computer Business and Equipment Manufacturers' Association puts it like this:

> the measurement of work by computer is a legitimate management tool that should be used wisely. Used appropriately, monitoring and related techniques, such as incentive pay or promotion based on productivity, can increase both an organizations effectiveness and the employee's ability to advance (Lund, 1992, p. 54).

Here the emphasis is not just on the employer, it is particularly on the benefit to the employee.

An interesting approach to computer monitoring is presented by DeTienne. She argues that this monitoring can be, not only quite benign, but useful to employees:

> Not only will these computers keep closer tabs on employees, but based on this added information, the computer will be able to help employees do their jobs more effectively. . . .
>
> Information gathered via computer monitoring will increasingly be used to coach employees. Currently, many organisations use the information gathered as a basis for criticism. Companies will begin to realize that it is more motivating for employees to be coached rather than reproached (1993).

So the claim is that computer monitoring of employees has multiple benefits, at least potentially. It improves the quality of goods and services, and so is good for customers; it makes businesses more efficient, so profits rise, which benefits employers; and it helps employees get higher pay and promotion, and assists them in doing their jobs better. Given all these benefits, why is it questioned? There are two types of reasons, one type based on the unacceptable consequences to the organisation of monitoring and surveillance. Such consequences include ill health, stress and lowering of morale. The other type of reason concerns the harm to employees, including as a harm, infringement of employees' rights to privacy. Other harms relate to employees' well-being. There is evidence that computer monitored employees suffer health, stress and morale problems to a higher degree than other employees (Bewayo, 1996; Aiello and Kolb, 1996). If it does indeed generate these sorts of problems, then these problems must be weighed against the benefits. It might be countered that if the problems are too great, then monitoring will not make organisations more efficient, and so the practice will stop. Alternatively, the organisations who practice it will not be able to attract good employees, and so will be forced to discontinue it. One weakness of this counter is that workers are not always free to pick and choose their employers, particularly in times and places of high unemployment. Many will almost certainly prefer to work under conditions which they do not like, than to not work at all. Another flaw in the argument is that it is not necessarily true that practices which are detrimental to health and morale will lead to less efficiency, at least not in the short term. For example, forcing workers to work for long hours without rest over extended periods could increase productivity in the short term, but lead to longer term health problems. Raising the levels of stress through continual monitoring could have the same effect. If the work requires a relatively low level of skill, and if there is unemployment, workers are easily replaceable. Treating workers in this fashion may not be good for a businesses' long term viability or profitability, but many businesses are not around for long. If the motive is short term profitability, long term effects are irrelevant. More importantly, treating workers in this fashion may be good for the profitability, long and short term, of that particular business. The problem may be the long term ill effects on the business sector in general, or on the specific industry sector in question.

The moral objection to computer monitoring

is based on the principle that a right cannot be infringed without very good reason. It would be rare that greater efficiency or profitability would constitute such a good reason. There clearly are times when a person's privacy rights can be overridden. An unconscious and unconsenting hospital patient, for example, may need constant monitoring, but that is for the patient's own good. A prison inmate might also need constant monitoring, but that might be for the protection of the community. Monitoring of employees however, does not, in most circumstances, secure these fundamental rights to life and protection.

A defender of computer monitoring might argue that the moral problem only arises if employees have no input into the establishing of the monitoring system, or if they are not fully aware of its scope and implications. If these conditions are satisfied, there is no moral problem, because the employee has, in effect, consented to the system's use, by accepting employment under those conditions.

While this has some initial attraction, on closer examination it is not so plausible. One reason is the same as that discussed in connection with health and morale. When unemployment is high, or if the person badly needs a job, there is not much force in consent. It is rather a case of economic coercion. A second problem is that even if people do consent to some sort of treatment, it does not follow that it is moral to treat them in that manner. Slavery cannot be justified on the grounds that some slaves may not have minded their condition too much if they knew nothing better, and if they had always been taught that slavery was the natural order of things. Likewise, violation of privacy cannot be condoned simply because some employees are willing to accept it.

What can be made of the argument that employee monitoring can be to the benefit of the employees themselves. Their privacy is violated, but it is in a good cause. Three benefits to the employee have been suggested. One is that it can, if used properly, help them to improve their work practices. This might be true, but it would at best only justify short term monitoring, and only with the employee's consent. Perhaps the techniques and satisfaction of clumsy lovers could be improved by information gained from spying on their activities, but that hardly seems to justify spying. A second benefit is said to be that employees can be assessed on purely objective criteria, say number and accuracy of keystrokes. While objectivity is good, assessment of an employee's worth will usually have a substantial subjective element as well. A highly responsible or experienced person who types slowly may well improve the productivity of others. So at best this is a weak justification for infringement of privacy. Finally, it is argued that this monitoring will help get rid of "dead wood", workers who are not doing their fair share of the work. This will not only be good for the employer, but also for the other employees. However, while none of us want to support lazy and incompetent colleagues, it is not clear that this will not have countervailing effects, namely, on the hardworking and competent workers also thus monitored. There could, of course, be limited and targeted monitoring where there was good reason to believe that particular employees were not meeting reasonable standards. This would seem to be a far more reasonable policy. However this is clearly not *general* monitoring and surveillance of the kind being discussed here. Supporting such colleagues is not good, but violation of privacy would, to many, seem even worse. (For discussion of these three points see De Tienne, 1993; Lund, 1992; and Fenner and Lerch, 1993.)

A stronger argument for employing surveillance is the control of crime in the workplace, especially theft and financial fraud. Law enforcement agencies can have rights which override those of individuals in certain circumstances when it is in the public interest. Theft and fraud in the workplace are still theft and fraud, so some surveillance can be justified in order to apprehend culprits.

Another form of monitoring, perhaps less worrying, but often discussed, is that of monitoring employees' email. While this might be thought to be akin to opening private mail or listening in to private conversations, the argument is that because the system on which the email operates is owned by the employers, they have a right to read any messages (see Loch

et al. 1992 for a discussion of a survey on this issue). But do they? The fact that two people are conversing in my house does not give me an automatic right to listen to what they are saying. But what if the two people are my employees? Does this make a difference? One argument that it does not, might go as follows: All I am paying for is my employees' labour. What they say to customers might be my business, but what they say to each other is not if it does not obviously and directly harm the business. Perhaps the cases are not analogous, because in the email case they are using my equipment, while in the other they are not. But what they say is still none of my business even if the consequences of what they say might be. The fact that they are continually having conversations might be overloading the equipment or hindering the work of others or themselves. Accordingly, banning or limiting private conversations might be justified. But this would not justify *monitoring* conversations. Perhaps this still misses the point. How will I know if the email is being used for private discussions unless I monitor it? I will not know unless I am told. But if no problems are being caused by overuse and so on, then there is no need to worry. If no harm is being caused by personal email, either to the computing equipment or to productivity, then monitoring what is said can have no purpose, except perhaps to satisfy curiosity. This is hardly a justification for violating a right. If there are problems such as the overloading of the system or inadequate work levels, then some steps may need to be taken, but even here actually reading messages would rarely be necessary. There could be a limit put on the length or number of messages, or the productivity of employees in question could be investigated. Employing people does not confer the right to monitor their private conversations, whether those conversations be in person or via email.

It might still be argued that what one employee says to a second employee might be my business as employer, if their conversation is work related. But even this cannot in general be correct. Consider the following three situations. First, if the two employees are, say, doctors in a private hospital, then their work related conversation might need to be protected by confidentiality. Second, what an employee is saying to a 'customer' might be protected by confidentiality, for example in the case of a lawyer working for a large corporation. In these circumstance a professional employee, that is, one who is a member of what is commonly thought of as a profession, for example, a medical doctor, lawyer or accountant, will need to be treated differently from a non-professional. Third, even non-professional employees need a measure of autonomy – conferred by privacy in the sense of non-interference and non-intrusion – in respect of one another and the public, if they are to take responsibility for their jobs and their performance in those jobs. Taking responsibility in this sense involves "being left alone" to do, or fail to do, the tasks at hand. Far from having the effect of ensuring that people do not make mistakes, intrusive and ongoing monitoring and surveillance might have the effect of causing employees to underperform because they are never allowed to take responsibility for outcomes, and therefore become lazy or engage in corrupt practices. Consider in this connection a salesman trying to convince a customer to buy a house, or a mechanic trying to figure out what is wrong with a car, or a supervisor trying to instruct a new clerk. The conception of employees that those who favour monitoring or surveillance tend to have in mind seem to be those doing menial, repetitive jobs that do not require any autonomy or individual initiative or judgment in order to be performed.

The discussion so far in relation to the Internet, has concerned only email, but of course Internet access involves much more than just email. Some employees have, on their employer's computing equipment, almost unlimited access to material, particularly through the World Wide Web (WWW). Is it an unjustified invasion of privacy for employers to monitor their employees activity on the WWW, to check on the sites visited? Given costs, particularly in processing time, associated with activity on the WWW, some restrictions seem quite justifiable. It would be difficult to condemn an employer who prohibited access except for work-related tasks. Given general knowledge of this prohibition, the

periodic checks of the sites accessed by employees is not unreasonable. More interesting problems arise in situations where employees require very free access in order to do their jobs properly, for example, many people involved in education. Universities, typically, allow their staff completely unfettered Internet access. Does the university then have a right to know how its employees are using this access? In general it would seem not. From a privacy perspective, there is no problem with restricting access to certain sites by the use of software. Monitoring sites visited, however, is not such an acceptable way of restricting access. Monitoring someone's use of the Internet in this way is a bit like monitoring library use, and it is instructive to look at how the library profession views the privacy issue.

Librarians have long been concerned about maintaining the privacy of library users' reading habits. The American Library Association puts its concern this way:

> The ethical responsibilities of librarians . . . protect the privacy of library users. Confidentiality extends to "information sought or received, and materials consulted, borrowed, acquired," and includes database search records, reference interviews, circulation records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services (*ALA Policy Manual*, 1996).

Why have librarians traditionally been so concerned about privacy? The reading habits of library users are the business of nobody except the user, but that in itself is not too important. My preference for unsugared, black tea rather than the sweet, white variety is also the business of nobody but me and the person making it for me, but worrying about the privacy of this information seems a bit extravagant. While much information about users which is stored in library databases might not be much more important than my preference in tea, in general, reading habits do reveal a little more about a person. It can been argued that what someone reads is very close to what he or she thinks, and therefore the ability to discover what is read is, in effect, the ability to find out what is thought.

It is not difficult to imagine situations where governments, advertising agencies or other groups could make use of this information for purposes which were not beneficial to the individual. For example, according to Million and Fisher, in the United States the Moral Majority attempted to obtain the names of school districts and individuals who had borrowed a film on sexual maturity from the Washington State Library (1986). Sometimes of course it might be beneficial to the community, for example when law enforcement agencies need information for criminal investigations. Borrowers, however, can be harmed if their records are not kept private. The burden of proof should be on those who want records made public, or at least available. The privacy of the individual can be overridden, but only to protect more important individual rights, or for the sake of very significant public goods (for further discussion see Weckert and Adeney, 1997).

Given that university librarians are part of the library profession, according to their own code of ethics, they are bound to keep library records private, including the borrowing records of university staff. From a professional librarian's point of view then, it would be an invasion of privacy for the university to check on an employee's borrowing record, even though the library is university owned and operated. It is difficult to see where the relevant difference lies is between the library and the Internet in this instance. Both are sources of information.

One complicating factor which rears its head in the context of email and Internet monitoring is vicarious libality, that is, the liability an employer might have for the actions of his or her employees. *Black's Law Dictionary* defines it thus:

> The imposition of liability on one person for the actionable conduct of another, based solely on a relationship between the two persons. Indirect or imputed legal responsibility for acts of another; for example, the liability of an employer for the acts of an employee . . . (1990).

Given this, it seems irresponsible of an employer not to monitor the email of employees or their use of the Internet in general. If this does not

happen, the employer could be liable for breaches of the law with respect to, for example, defamation, copyright infringement and obscene material (Cutler, 1998). It does not follow from this however, that an employer has the right to monitor employee activity on the Internet which the employee could reasonably expect to be private. It does though, strengthen an employer's right to insist that his or her computing equipment is not to be used for anything apart from legitimate work related purposes. This policy must, of course, be made clear. It also might call into question the appropriateness of maintaining vicarious liability in some of these contexts. At any rate, the general point to be made here is that where an employer allows private email and other Internet activity, his vicarious liability does not necessarily legitimise monitoring of that activity.

Finally, should employers be able to monitor listservers which are on their computer systems? For employers in general, this will probably be a rare situation, but not for universities. Suppose that a university runs courses by distance education, something which is becoming increasingly common. The lecturer and students decide to establish a listserver to facilitate discussion, and to help overcome the isolation often felt by distance education students. Does the university have a right to monitor activity on that listserver without notifying the participants? It might be argued that they do, because the listserver is public in the same sense that a university lecture theatre is, and so any authorised university person has access. The analogy however, is not good. If someone enters a lecture theatre, he or she is there for all to see. There is no question of secrecy. Suppose now that the university monitors lectures, not by having staff attend, but rather by secretly installing cameras and microphones. The analogy here is closer, but the monitoring does not seem so benign. It might be objected that in the listserver case there is nothing secret. The university monitor enrols, so it is not too difficult to discover the monitoring. Just look to see who is enrolled. But that is not the point. If there is to be monitoring, the onus for making it public should not be on those monitored, but on those monitoring.

Drawing an analogy between listservers and lecture theatres is misleading in any case. While it is true that authorised university staff can attend lectures in university owned buildings without violating anyone's right to privacy, nothing follows from this about secret listserver monitoring. Normally university lectures are not private. Anyone can come and listen. The situation changes a little with tutorials, where there is more interaction, and at private discussion between a lecturer and a student. It is not so clear that the university would be justified in authorising someone to monitor tutorials, without the tutors and students knowledge, or to monitor private student-lecturer discussions. The claim that this is justified simply because these activities are taking place on university property is dubious at best. Listservers seem more like tutorials than lectures. There is some privacy. One cannot just look and see what is happening, as is possible with a newsgroup. One must enrol. Secret monitoring of class listservers then, can be seen as a violation of privacy rights, just as secret monitoring of tutorials would be.

Workplace monitoring is a practice which requires much more examination. Employers need an efficient and competent workforce in order to survive in a competitive environment, and customers demand and deserve high quality goods and services. The employees who produce these goods and services have a responsibility to work to the best of their ability for the financial reward that they receive, but they do not forfeit their rights to privacy by virtue of being employees. Although workplace monitoring can be justified in some circumstances, privacy is a moral right, and as such there is a presumption against its infringement. This paper has argued that some of the common justifications given for this monitoring do not withstand close scrutiny.

A number of questions remain to be researched, both empirical and analytical. One of these questions is the relationship between monitoring and trust in the workplace. It would appear that monitoring is a sign or distrust, and perhaps employees who know that they are being monitored, and hence not trusted, will become less trustworthy, in which case they will require more monitoring. Superficially at least, it appears

that monitoring could precipitate a breakdown in trust, which in the longer term would probably lead to a less efficient workforce. But this requires investigation. Another issue is the role of vicarious liability in the violation of individual employee privacy. It seems that the current law (in countries which have it), or its interpretation, encourages, or even necessitates employee monitoring which is morally questionable. Perhaps the law requires modification in the light of contemporary computer technology. Privacy is perhaps the topic most discussed by those concerned about the social and ethical implications of computer technology. It deserves to be.

References

ACM Code of Ethics and Professional Conduct: 1992, Section 1.7. http://www.acm.org/constitution/code.html (Read 25 July, 1998).

Aiello, John R. and Kathryn, J. Kolb: 1996, 'Electronic Performance Monitoring: A Risk Factor for Workplace Monitoring', in S. L. Sauter and L. R. Murphy, (eds.), *Organisational Risk Factors for Job Stress* (American Psychological Association), pp. 163–179.

ALA Policy Manual: 1996, Section Two (Position and Public Policy Statements), 52.4 Confidentiality of Library Records, gopher://ala1.ala.org:70/00/alagophviii/policy.hb (Read 25 July 1998).

Barroso Asenjo, P.: 1997, 'Key Ethical Concepts for the Internet and for Ethical Codes of Computer Professionals', *Australian Computer Journal* **29**, 2–5.

Benn, S. A.: 1988, *Theory of Freedom* (Cambridge University Press, Cambridge).

Bewayo, E.: 1996 , 'Electronic Management: Its Downside Especially in Small Business', in J. Kizza (ed.), *Social and Ethical Effects of the Computer Revolution* (McFarland and Co., Jefferson, NC), pp. 186–199.

Black, Henry Campbell: 1990, *Black's Law Dictionary*, 6th edition (West Publishing Co., St. Paul, MN), p. 1566.

Cutler, P. G.: 1998, 'E-mail: Employees and Liability', *Chemistry in Australia* (March, 1), 30–31.

DeTienne, K. B.: 1993, 'Big Brother or Friendly Coach', *Futurist* **27**, 33–37.

Direct Marketing: 1993, 'Telephone Monitoring Heads to Congress', (August 6), **6**. Quoted in M. Levy, 'Electronic Monitoring in the Workplace: Power Through the Panopticon', http://bliss.berkeley.edu/impact/students/mike/mike_ paper.html (Read 25 July 1998).

Fenner, Deborah B. and F. Javier Lerch: 1993, 'The Impact of Computerized Performance Monitoring and Prior Performance Knowledge on Performance Evaluation', *Journal of Applied Social Psychology* **23**, 573–601.

Forester, Tom and Perry Morrison: 1991, *Computer Ethics: CautionaryTales and Ethical Dilemmas in Computing* (MIT Press, Cambridge, MA).

Garson, Barbara: 1988, *The Electronic Sweatshop* (Simon and Schuster, New York).

Hawk, Stephen, R.: 1994, *Journal of Business Ethics* **13**, 949–957.

Johnson, Deborah G.: 1994, *Computer Ethics*, Second edition (Prentice Hall, Upper Saddle River, NJ).

Langford, Duncan: 1995, *Practical Computer Ethics* (McGraw-Hill, Maidenhead, Berkshire).

Loch, Karen D., Sue Conger and Effy Oz: 1998, 'Ownership, Privacy and Monitoring in the Workplace: A Debate on Technology and Ethics', *Journal of Business Ethics* **17**, 653–663.

Lund, J.: 1992, 'Electronic Performance Monitoring: A Review of the Research Issues', *Applied Ergonomics* **23**, 54–58.

Magney, J.: 1996, 'Computing and Ethics: Control and Surveillance Versus Cooperation and Empowerment', in J. Kizza (ed.), *Social and Ethical Effects of the Computer Revolution* (McFarland and Co., Jefferson, NC), pp. 200–209.

Miller, S.: 1997 'Privacy and the Internet', *Australian Computer Journal* **29**, 12–15, for a similar discussion of the notion of privacy.

Million, A. C. and K. N. Fisher: 1986, 'Library Records: A Review of Confidentiality Laws and Policies', *Journal of Academic Librarianship* **11**, 346–349.

Nussbaum, Karen: 1991, 'Computer Monitoring a Threat to the Right to Privacy?', reprinted in Roy Dejoie, George Fowler and David Paradice, *Ethical Issues in Information Systems* (Boyd and Fraser Publishing Company, Boston).

Parent, P. "Privacy": 1992, in E. E. Cohen (ed.), *Philosophical Issues in Journalism* (Oxford University Press, New York), pp. 90–99.

Parker, Donn B., Susan Swope and Bruce N. Baker: 1990, *Ethical Conflicts In Information and Computer Science, Technology, and Business* (QED Information Sciences, Inc., Wellesley, MA).

Perrolle, Judith A.: 1996, 'Privacy and Surveillance in Computer-Supported Cooperative Work', in

David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy* (University of Minnesota Press, Minneapolis), 47–65.

Rule, James, B.: 1996, 'High-Tech Workplace Surveillance: What's Really New?', in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy* (University of Minnesota Press, Minneapolis), pp. 66–76.

Severson, Richard J.: 1997, *The Principles of Information Ethics* (M.E. Sharp, Armonk, NY).

Warren, S. and L. Brandeis: 1890, 'The Right to Privacy', *Harvard Law Review* **4**, 193–220.

Weckert, J. and D. Adeney: 1997, *Computer and Information Ethics* (Greenwood Publishing Group, Westport, Conn.).

Zuboff, Shoshana: 1988, *In the Age of the Smart Machine: The Future of Work and Power* (Basic Books, New York).

ARC Special Research Centre for Applied Philosophy and Public Ethics, Wagga Wagga, Australia.