

Workplace Surveillance, Privacy and Distributive Justice

CEPE 2000

Lucas D. Introna

University of Lancaster, UK

Email: Lintrona@lse.ac.uk

Abstract: Modern technologies are providing unprecedented opportunities for surveillance. In the workplace surveillance technology is being built into the very infrastructure of work. Can the employee legitimately resist this increasingly pervasive net of surveillance? The employers argue that workplace surveillance is essential for security, safety, and productivity in increasingly competitive markets. They argue that they have a right to ensure that they 'get what they pay for', furthermore, that the workplace is a place of 'work' which by its very definition excludes the 'personal' dimension at the core of all privacy claims. Legal developments, especially in the USA, seem to favour such an interpretation. The individual's call for workplace privacy seems illegitimate in a context where the 'personal' is almost excluded by default. In this paper I want to argue that the private/public distinction is not useful in the context of workplace surveillance since it always seems possible to argue that the workplace is always and only 'public'—thereby leaving the employee without resources to defend their claim. Such a position belies the fact that the fundamental claim of workplace privacy is not a claim for some personal space as such but rather a claim for the protection against the inherently political interests in the 'gaze' of the employer. Furthermore, that it is probably impossible, in practice, to separate the public from the private in the flow of everyday work. Thus, it seems that one needs to develop another approach to think through the issues at stake. I will argue that the distribution of privacy rights and transparency (surveillance) rights is rather a matter of organisational justice. I will suggest that we may use theories of justice—in particular the work of Rawls—to develop a framework of distributive justice for distributing privacy and transparency between the collective and the individual in a way that is fair. I will contend that such an approach will provide the employee with resources to defend their legitimate claim to workplace privacy.

Introduction

Surveillance has become a central issue in our late modern society. The surveillance of public spaces by closed circuit television, the surveillance of consumers through consumer surveys and point of sale technology and workplace surveillance, to name but a few. As surveillance increases more and more questions are being raised about its legitimacy. In this paper I want to focus on one of the more problematic areas of surveillance namely workplace surveillance. There is no doubt that the extensive use of information technology in all organisational processes has created enormous potential for cheap, implicit and diffused surveillance. Surveillance that is even more 'close' and continuous than any human supervisor could be. The extent of current surveillance practices are reflected in the following indicators:

- Forty-five percent of major U.S. firms record and review employee communications and activities on the job, including their phone calls, e-mail, and computer files. Additional forms of monitoring and surveillance,

such as review of phone logs or videotaping for security purposes, bring the overall figure on electronic oversight to 67.3% (American Management Association 1999).

- Piller (1993) reported in a *MacWorld* survey of 301 business that 22% of the business have searched employee computer files, voice mail, e-mail, or other networking communications. The percentage jumped to 30% for business with a 1000 or more employees.
- The International Labour Office (1993) estimate that some 20 million Americans may be subject to electronic monitoring on the job, *not including telephone monitoring*.
- In 1990 it was reported that up to one million jobs in Britain are subject to security checks (Lyon 1994, p.131).

It would be reasonable to say that these formal surveys do not reflect the actual practice. It would be reasonable to

assume that organisations would not tend to publicise the degree to which they engage in systematic monitoring. Since surveillance often function as a resource for the execution of power, and power is most effective when it hides itself. One can imagine that the vast majority of organisations engage in anything from isolated incidents of specific monitoring to large scale systematic monitoring.

The purpose of this paper is not to bemoan surveillance as such. I believe it is rather more important to understand the context and logic of surveillance in the workplace. In this paper I will argue that the real issue of workplace surveillance is justice as fairness. I will argue that it is the inherent political possibilities of surveillance that concerns employees. That they simply do not trust the interested gaze of management, and they have very good reason for such mistrust. Finally I will discuss the possibility of using Rawls' theory of justice to establish a framework for distributing the rights of privacy and transparency between the individual (employee) and the institution (the employer).

Resisting workplace surveillance

In the second half of the twentieth century, two major trends seem to create the background for our contemporary discussion of workplace surveillance. The first of these are the increasing challenge by the employees of their conditions of work, especially the normalising practices of discipline. The social revolution of Marxism and later of liberal democracy trickled into the production floor. Initially as labour became increasingly unionised the debate about surveillance became articulated as a conflict between labour and capital in the Marxist idiom. Later workers demanded rights in the workplace they were already accorded elsewhere. Modern management increasingly needed to justify its surveillance practices. A second trend that intensified the debate was the rapid development of surveillance technology that created unprecedented possibilities for comprehensive surveillance. With the new technology, surveillance became less overt and more diffused. In fact, it became built into the very machinery and processes of production (workflow systems, keystroke monitoring, telephone accounting, etc.). This increasingly 'silent' and diffused potential of surveillance technology also started to concern policy makers, unions, social activists and the like. However, in spite of their best efforts, and considerable progress in the establishment of liberal democracy in Western society, the balance of power is still firmly in the hands of the employer. The United States Congress' Office of Technology Assessment report (U.S. Congress 1987) into employee monitoring concludes that "*employers have considerable latitude in making use of new monitoring technologies; they have generally been considered merely extensions of traditional management prerogatives*" (p.6). Even today there exist very little enacted legislation in Western democracies that articulate the fair use of workplace monitoring¹ (U.S. Congress 1987, Appendix A). I would argue that that one of the

reasons for this is lack of adequate protection may be the inappropriate way in which the workplace monitoring debate has developed (I will address this in detail in the next section).

In the United States the right of the employer to conduct workplace surveillance as a means to protect the employer's interest to organise work, select technology, set production standards, and manage the use of facilities and other resources, is recognised by the law. This means that there is no legal obligation on employees to ensure that "monitoring be 'fair', that jobs be well designed or that employees be consulted about work standards, except insofar as these points are addressed in union contracts..." (U.S. Congress 1987, p.2). As less than 20% of office work in the US is unionised, it seems that decisions about work monitoring are made solely at the discretion of employers.

Recent legal developments seem to confirm this asymmetry of power. For example, in the area of e-mail monitoring the right to use surveillance of communications technology supplied for business purposes have been confirmed in the Electronic Communications Privacy Act of 1986 ("ECPA"). Essentially the ECPA expanded pre-existing prohibitions on the unauthorised interception of wire and oral communications to encompass other forms of electronic communications. However, the ECPA does not guarantee a right to e-mail privacy in the workplace because of three very important exceptions. I will just focus on two here. The first is the *business extension* or ordinary course of business exception. This exception allows the employer to monitor any communications that use communications technology supplied to the employee in the ordinary course of business for use in conducting the ordinary course of business. This means that the telephone or the e-mail account supplied to an employee to conduct their work can legally be monitored as long as the monitoring can be justified having a valid business purpose (Dichter and Burkhardt 1996, p.14). The second is the *consent exception*. This exception allows monitoring in those cases where prior consent has been obtained. It is important to note that implied consent is also recognised by the law. Employers who notify employees that their telephone conversations or e-mail is likely to be monitored will have the implied consent of their employees (Santarelli 1997). It also seems as if common law does not provide any correction in the balance of power. In common law the decision of permissibility hinges on the notion of a "reasonable expectation of privacy". This may mean, for example, that if an employee is provided with a space to store personal belongings, or a particular phone line for personal calls, it would be reasonable for them to expect it not to be monitored. Johnson (1995) and others have remarked that this expectation of privacy can easily be removed by an explicit policy that all communication using company equipment can and will be subjected to monitoring.

From this brief discussion it is clear that it would be fairly easy for employers to monitor all aspects of work and communications (on equipment made available for ordinary business use) as long as the employer explicitly communicates policy that monitoring can take place, and that the employer can justify it for a valid business purpose. It is hard to image what sort of monitoring—excluding some extreme cases—can not be defended as being for a valid business purpose (productivity, company moral, safety, etc). It is also hard to image what sort of resources an individual employee can use to generate a 'reasonable expectation of privacy' in a context where accepting employment contract also means accepting the policies of the organisation and thereby relinquishing the right to a "reasonable expectation of privacy"—assuming there is an explicit monitoring policy. In the context of the typical asymmetry of power present in such employment situations it is hardly a matter of choice. It is clear, and acknowledged by many, that the current US climate is heavily biased in favour of the employer.² The lack of legislation in other countries would also indicate that it would be reasonable to conclude that workplace monitoring is still largely viewed as a right of employers with the burden of proof on the employee to show that it is invasive, unfair or stressful. It would seem that a legal correction in the imbalance of power is not likely to be forthcoming in the near future.

In spite of this imbalance of power, surveillance has not become a widespread practice, as one would assume (U.S. Congress 1987, p.31). In addition, it seems that where surveillance is operating it is not always challenged to the degree that one would assume (U.S. Congress 1987, p.31). Why is this so? It seems that there is not sufficient evidence to suggest surveillance *of individuals* would lead to *long term* productivity improvements. To use Denning's well known quality dictum (revised accordingly): productivity is not merely a matter of surveillance, but is rather an emerging element of a system designed for productivity as a whole. There is also accumulating evidence that surveillance *of individuals* lead to stress, a loss of sense of dignity, and a general environment of mistrust. In this environment of mistrust employees tend to act out their employer's expectations of them—thereby eradicating any benefit that the surveillance may have had (Marx 1986; U.S. Congress 1987). Furthermore, I believe surveillance is not always challenged because we all at times benefit from its fruits. For example, the use of surveillance data for performance assessment can result in a more equitable treatment of employees. Such data can provide evidence to prevent unfair allocation of blame. It would be possible to think of many ways in which employees may use surveillance for their own benefit—such as "the boss can see on the CCTV that I do actually work many hours overtime", and the like.

Like power surveillance "passes through the hands of the mastered no less than through the hands of the masters"

(Foucault 1977). It does not only bear down upon us as a burden but also produces possibilities and resources for action that can serve multiple interests. Surveillance is no longer an unambiguous tool for control and social certainty, nor is it merely a weight that weighs down on the employee—rather its logic and its effects has become increasingly difficult to see clearly and distinctly. Surveillance, with modernity, has lost its shine.

In the next section, I want to consider the relationship between surveillance and autonomy and indicate its link with justice. This will provide the background for the next section where I will develop a framework for distributing the rights of privacy and transparency between the individual and the collective.

Privacy as a matter of justice

Privacy is by no means an uncontroversial issue. Some, like Posner (1978), tends to see the need for privacy as a way of hiding or covering up what ought to be exposed for scrutiny. He argues that exposure through surveillance would provide a more solid basis for social interaction because the participants will be able to discern all the facts of the matter for themselves. Privacy, for him, creates opportunities for hiding information that could render many social interactions "fraudulent". To interact with someone without providing that person with all information would be to socially defraud that person, or so he argues. This is a very compelling argument, which has made Posner's paper one of the canons in the privacy literature. As such, it provides a good starting point for our discussion.

At the root of Posner's argument—and the argument for surveillance in general—is the fundamental flaw of the modernity's belief in surveillance as a neutral gaze, as a sound basis for certainty—for knowing that we know. Surveillance can only fulfil its role as guarantor of certainty if it is complete and comprehensive—in short, omnipresent—and if it can be done from a vantagepoint where all things are of equal or no value—which is impossible. If these conditions can be fulfilled then Posner's argument will be valid. However, once surveillance loses its omnipresent and value free status—which it never had in the first place—it no longer deals with facts but rather with values and interests. Science becomes politics—as it has been from the beginning (Latour 1987; Latour and Woolgar 1986 {1979}). Knowing is replaced by choosing. We have to select what to survey, and most importantly, we have to select how to value what we find in our surveillance.

Employees do not fear the transparency of surveillance, as such, in the way argued by Posner. It is rather the choices, both explicit and implicit, that the employers will by necessity be making that employees mistrust. They are concerned that these choices may only reflect the interests of the employer. They are rightly concerned that the employer will only have 'part of the picture', and that they may be reduced,

in subsequent judgements, to that 'part of the picture' alone. They are also concerned that employers will apply inappropriate values when judging this 'part of the picture'. More than this, they will also be concerned by the fact that employers may implicitly and unbeknowningly bring into play a whole lot of other 'parts' of pictures that ought not be considered in that *particular context*—for example judging a particular employee candidate for promotion or not because it is also known that the employee is a Muslim. They are concerned because we can not, contrary to the modern mind, separate out what 'pictures' we take into account or not when making judgements, *in the act of judging itself* (Merleau-Ponty 1962). We are entangled and immersed in our values and beliefs to the point that they are merely there, available for use, part of the background that we do not explicitly attend to in making actual judgements (Heidegger 1962 {1937}). It is part of our thrownness (*Befindlichkeit*). It is therefore fruitless to posit that we should or should not apply particular data or particular values in making a particular judgement. We can simply not say to what degree we did or did not allow our judgement to become influenced by certain facts and certain value dispositions, in making a particular judgement. The facts and values are not like fruits in a basket before us from which we can select, by rational choice, to take some and not others. We are immersed, engrossed, and entangled in our world in ways that would not normally make us explicitly attend to the particular facts, values and interests that we draw upon in makings particular judgements. We can of course attempt to make them explicit as bureaucracies and scientific management tried to do. However, Dreyfus (1992; 1986) has shown that skilled actors do not normally draw upon these explicit representations *in action*. Foucault (Foucault 1977) has also showed that these explicit representations are more important as resources for the play of power than resources for 'objective' judgements, which is exactly why employees mistrust them. To conclude: it is the very political possibilities of surveillance, in the data selected, the values applied, the interest served, and the implicit and entangled nature of the judgement process, which makes employees—and persons in general—have a default position of mistrust rather than trust in 'exposing' themselves. It is this untrustworthy nature of judgements—of the products of surveillance—that moved Johnson (Johnson 1989) to define privacy as the right to the "freedom from the judgement of others". It is also this untrustworthy nature of judgements that made the OTA report argue that they view, as the most central issue of workplace monitoring, the issue of fairness. Fairness, as the levelling of the playing field, as serving all interests, not only the few.

Thus, the issue of workplace privacy is not merely a matter of 'bad' employees wanting to hide their unscrupulous behaviour behind a call for privacy—undoubtedly this is the case in some instances—it is rather a legitimate concern for justice in a context in which the employees are, for the most

part, in a relationship of severe power asymmetry. I would therefore argue that the development of the workplace privacy debate will be best served if it is developed along the lines of *fairness and organisational justice* rather than along the lines of a general notion of privacy as a matter of some personal space. The personal dignity and autonomy argument can so easily be seen as personal lifestyle choices that have no place in the public workplace as expressed by Cozzetto and Pedeliski (1999) in their paper on workplace monitoring: "*Autonomy embraces areas of central life choice and lifestyle that are important in terms of individual expression, but irrelevant to an employer and of no public concern.*" I believe many employers and authors in the field find the concept of workplace privacy problematic because they link it to the general debate on privacy that are often cast exclusively in the mould of personal dignity and autonomy. This leads to claims of irrelevance. As one employer expressed it in the Canadian Information and Privacy Commissioner's (IPC) report (1993) on workplace privacy: "*The paper overstates this issue as a problem of pressing concern for employees and employers and the general public...the IPC is making more of an issue out of this, and looking for problems where none need exist*"(p.9).

If we accept the general idea that workplace privacy and surveillance is a matter of justice, how should one go about structuring the debate? In the next section I will discuss the distribution of privacy and transparency as an issue of distributive justice using the work of Rawls (1972).

Privacy, surveillance and distributive justice

For the individual privacy secures autonomy, creates social capital for intimacy, and forms the basis of structuring many diverse social relations (Introna 1997; Westin 1967). It is generally accepted that it is in the interest of the individual to have maximum control over her privacy—here taken to be the *freedom from the inappropriate judgement of others*. For the collective or institution transparency secures control and thereby efficiency of resource allocation and utilisation, as well as creating mechanisms for disciplinary intervention (Foucault and Sheridan 1979). It is generally accepted that it is in the interest of the collective or institution to have maximum control over surveillance—here taken to mean *subjecting all individuals in the institution to reasonable scrutiny and judgement*. If the individuals are given an absolute right to privacy they may act only in their own interest and may thereby defraud the institution. If the institution is given a complete right to transparency it may strip the individual of autonomy and self-determination by making inappropriate judgements which only serve its own interest.

Thus, from a justice perspective we need a framework that would distribute the rights to privacy—of the individual (the employee in this case)—and right of transparency—of the collective (the employer in this case)—in a way that would be seen to be fair to all concerned. I would argue that wher-

ever individuals and institutions face each other the distribution of privacy and transparency rights will become an issue to be resolved. In this regard the institution can be as diverse as the family, the workplace, the community, the state, and so forth. At this stage I will exclude from my discussion the conflict of privacy and transparency rights between different institutions such as between the corporation and the state. Given this conflict between the individual employee and the institutionalised workplace how can we decide on a fair distribution of privacy and transparency rights? I will propose that we may use the Rawlsian theory of justice as a starting point. Obviously one could use other frameworks. I am not arguing that Rawls is the only or even vastly superior perspective. Nevertheless, it does seem as if the Rawlsian framework is useful in this regard.

Rawls in his seminal work "A Theory of Justice" of 1971 proposes a framework of justice as fairness in opposition to the leading theory of the day viz. utilitarianism. For Rawls utilitarianism puts no restrictions upon the subordination of some people's interests to those of others, except that the net outcome should be good. This would allow for any degree of subordination, provided the benefit to those advantaged was great enough. Rawls argues that a theory of justice can not allow disadvantages to some be justified by advantages to others. In our case this would imply a view that may posit the limited cost of the loss of individual privacy against the enormous economic benefit to the collective of securing effective control over productive resources. Such utilitarian arguments can easily make the individual's claim to privacy look trivial in the face of the economic prosperity of the whole. I would claim that it is exactly this utilitarian type logic that continues to limit the legitimacy of the individual employee's claim to privacy in the workplace.

If this is so, how can we establish as set of rules that would ensure a fair distribution of privacy and transparency rights? Rawls (1972) argues that this can only happen behind a 'veil of ignorance' in the so-called original position. According to this formulation a fair set of rules for this distribution would be a set of rules that *self interested* participants would choose if they were completely ignorant about their own status in the subsequent contexts where these rules will be applied. What would be the rules for distributing privacy and transparency rights that may be selected from behind such a veil of ignorance?

As a starting point we need to outline the facts—about interests and positions—that we may assume to be available to those in the original position. This information will provide the force that may shape their choices. Obviously these need to be debated but I would propose the following fact are known—first from the perspective of the individual, then from the perspective of the collective.

From the individual perspective:

- That there are no such things as neutral or objective judgements. Every judgement implies interests. Once data is recorded it can in principle become incorporated into a judgement process that may not serve the individual's interests. It would therefore seem reasonable that the self-interested individual would try to limit all forms of capturing of data about themselves and their activities.
- In the context of typical organisational settings the employee is normally in a disadvantaged position—in a relation of severe power asymmetry. Thus, it is not possible for the individual, as an individual, to bargain for, and ensure the fair use of data once it is captured. It would therefore be in the interest of the individual to limit all forms of capturing of data about themselves and their activities.
- If data about themselves and their activities are captured it is in their interest to have maximum control over it—what is captured, who sees it, for what purposes, and so forth.

From the perspective of the collective

- Without the capturing of complete and comprehensive information about the relevant activities of the individual, resources can not be efficiently and effectively allocated and control over the use of these resources can not be maintained. Without such control the collective would suffer. It would therefore seem reasonable to monitor all relevant activities of the individual. Relevant here would be understood to be those activities that imply the allocation and utilisation of collective resources.
- Self-interested individuals would not always tend to use resources—allocated by the collective—for the sole purposes of furthering the aims and objectives of the collective. In fact they may use it completely for their own purposes. It would therefore seem reasonable to monitor all individual activities that allocate and utilise collective resources.
- The collective needs to use data collected to co-ordinate and control the activities of the individuals for the good of the collective. It would be in the interest of the collective to have maximum control over the capturing and utilisation of relevant data about the individuals.

Given these facts—and other similar ones we may enumerate—what rules would those behind the veil of ignorance choose in distributing individual privacy and collective transparency rights? Before attempting to suggest some rules it may be important to highlight Rawls' 'difference principle'—which he argues those behind the veil of ignorance would tend to choose. This principle states that an inequality is unjust except insofar as it is a necessary means to improving

the position of the worst-off members of society. Without this principle it would be difficult for those behind the veil of ignorance to establish rules for distributing privacy and transparency rights as it seems equally reasonable to grant and limit these rights both to the individual and the collective. However, we know—as indicated above—that in the context of the modern organisation the individual is in a position of severe power asymmetry. In the prevailing climate it would be difficult to argue that the individual employee is not ‘the worst-off’ with respect of securing a fair and reasonable level of privacy rights in the workplace. This would seem to indicate that most individuals behind the veil of ignorance would tend to want to argue for some bias towards securing the rights of the individual over and against that of the institution. With this in mind I will suggest—mostly for illustrative purposes—a set of fair ‘rules’ or guidelines that may be put forward by those behind the veil of ignorance. I would contend that they would acknowledge the following:

- That the collective (employer) does indeed have a right to monitor individuals’ activities with respect to the allocation and utilisation of collective resources. The collective also has a right to use the data collected in a fair and reasonable way for the overall good of the collective as a whole.
- That the individual (employee) does have a legitimate claim to limit the surveillance of their activities in the workplace. The individual also has a right to secure a regime of control that will justify all monitoring and that will ensure that the data collected will be used in a fair and reasonable way.
- Based on the ‘difference principle’ it will be up to the collective (employer) to justify the collection of particular data in particular contexts. Furthermore, that the regimes for controlling the collected data should be biased towards the individual.

Obviously one could develop these rules in much more detail. However, even this very limited, initial reflection, would seem to suggest that the prevailing organisational practices that favour the collective (both in capturing and control) would seem to be unfair.

Obviously this analysis is still too crude and unsophisticated. However, it does illustrate that one may arrive at very different conclusions if one takes the issue of workplace pri-

vacuity to be one of fairness rather than as a matter of working out the private/public distinction in the workplace—since it will always be relatively easy to argue that the workplace is a *de facto* public space, devoid of almost any privacy rights.

Conclusion and some implications

The potential for workplace surveillance is rapidly increasing. Surveillance technology is becoming cheap, silent, and diffused. Surveillance technology has created the potential to build surveillance into the very fabric of organisational processes. How should we concern ourselves with these facts? Clearly each workplace will be different. Some will be more bureaucratic, some more democratic. Nevertheless, the conflict between the individual right to privacy and the institutional right to transparency will always be there. In each individual case different tactics will be used by the different parties to secure their interests.

In the case of workplace privacy the prevailing legal and institutional infrastructure makes it difficult for the individuals to secure their interests, leaving them power-less, but by now means powerless. One of the major reasons for the unsuccessful challenge of modern workplace surveillance is the inappropriate manner in which the workplace privacy debate has evolved. In my opinion it incorrectly attached itself to the public/private distinction which leaves the employee in a position of severe power asymmetry. In opposition to this debate I have argued that if one articulates the issue of workplace surveillance along the lines of competing, but equally legitimate claims (for privacy and transparency), that needs to be fairly distributed the possibilities for the individual to resist inappropriate workplace surveillance increases dramatically. Using the Rawlsian theory of justice I argued that those behind the veil of ignorance would tend to adopt a position that biases the right of the employee—the worst off—over that of the employer. This would suggest that a fair regime of workplace surveillance would tend to avoid monitoring unless explicitly justified by the employer. It will also provide mechanisms for the employee to have maximum control over the use of monitoring data. Both of these rules seem to suggest that most of the prevailing organisational surveillance practices are unfair. This, I believe, is the challenge to us. To set up the intellectual and organisational resources to ensure that workplace surveillance becomes and stays fair. ♦

References

1. (ILO), International Labour Organisation. 1993. Conditions of work digest: Monitoring and surveillance in the workplace. Geneva: International Labour Office.
2. Association, American Management. 1999. Workplace monitoring and surveillance: American Management Association.
3. Commissioner/Ontario, Information and Privacy. 1993. Workplace Privacy: The need for a Safety-Net, [Http://www.ipc.on.ca/web_site/ups/matters/sum_pap/papers/safnet-e.htm](http://www.ipc.on.ca/web_site/ups/matters/sum_pap/papers/safnet-e.htm): Information and Privacy Commissioner/Ontario.
4. Cozzetto, D and T.B' Pedeliski. 1999. Privacy and the Workplace: Technology and Public Employment, [Http://www.ipma-hr.org/pubs/cozzfull.html](http://www.ipma-hr.org/pubs/cozzfull.html): International Personnel Association.
5. Dichter, MS and MS Burkhardt. 1996. Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing employee communications in the Internet Age. In *The American Employment Law Council: Fourth Annual Conference*. Asheville, North Carolina.
6. Dreyfus, Hubert L. 1992. *What computers still can't do: A critique of artificial reason*. Cambridge, MA: The MIT Press.
7. Dreyfus, Hubert L and Stuart E Dreyfus. 1986. *Mind over machine: The power of human intuition and expertise in the era of the computer*. New York: The Free Press.
8. Foucault, M. 1977. Truth and Power. In *Power / Knowledge: Selected Interviews & Other Writings 1972-1977*, ed. C. Gordon. New York: Pantheon Books.
9. Foucault, Michel and Alan Sheridan. 1979. *Discipline and punish: the birth of the prison*. Harmondsworth: Penguin.
10. Heidegger, Martin. 1962 {1937}. *Being and time*. Translated by John Macquarrie
11. Edward Robinson. Oxford: Basil Blackwell.
12. Introna, L.D. 1997. Privacy and the Computer: Why we Need Privacy in the Information Society. *Metaphilosophy* 28, no. 3: 259-275.
13. Johnson, BT. 1995. Technological Surveillance in the Workplace, [Http://www.fwlaw.com/techserv.html](http://www.fwlaw.com/techserv.html): Fairfield and Woods P.C.
14. Johnson, J.L. 1989. Privacy and the Judgement of Others. *The Journal of Value Inquiry* 23: 157-168.
15. Latour, Bruno. 1987. *Science in action: How to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.
16. Latour, Bruno and Steve Woolgar. 1986 {1979}. *Laboratory life: The construction of scientific facts*. Princeton: Princeton University Press.
17. Lyon, David. 1994. *The Electronic Eye: the rise of the surveillance society*. Cambridge: Polity Press.
18. Marx, G.T. 1986. Monitoring on the Job: How to Protect Privacy as well as Property. *Technology Review*.
19. Merleau-Ponty, M. 1962. *Phenomenology of Perception*. Translated by Colin Smith. London: Routledge.
20. Piller. 1993. Bosses with x-ray eyes. *MacWorld*, no. July: 118-123.
21. Posner, R. 1978. The Right to Privacy. *Georgia Law Review* 12: 383-422.
22. Rawls, J. 1972. *A Theory of Justice*. Cambridge, Mass: Harvard University Press.
23. Santarelli, N. 1997. E-mail Monitoring in the Work Place: Preventing Employer Liability, [Http://wings.buffalo.edu/complaw/complawpapers/santarelli/html](http://wings.buffalo.edu/complaw/complawpapers/santarelli/html): Computers and Law Internet site.
24. U.S. Congress, Office of Technology Assessment (OTA Report). 1987. The Electronic Supervisor: New Technology, New Tensions. Washington DC: US Congress.
25. Westin, A. 1967. *Privacy and Freedom*. New York: Ateneum.

¹ Sweden is the exception here. The Swedish Codetermination Act of 1976 require employers and employees to participate in decisions about electronic monitoring (U.S. Congress 1987, Appendix A).

² There has been attempts to change this in the unsuccessful Privacy of Consumers and Workers Act (PCWA) of 1993.