2006

Workplace Privacy and Surveillance: A Matter of Distributive Justice

Geoffrey A. Sandy
Victoria University, Geoff.Sandy@vu.edu.au

Workplace Privacy and Surveillance: A Matter of Distributive Justice

Associate Professor Geoffrey A Sandy
School of Information Systems
Victoria University
Melbourne, Australia
Email: Geoff.Sandy@vu.edu.au

Abstract

ICT professionals should be concerned about the use made of their artefacts. ICT enable workplace surveillance on an unprecedented scale and increasingly at a level that no employee activity can escape it. We cannot expect employees and employers to formulate an agreed set of rules regarding privacy and surveillance rights that are considered fair or just to both. The reality is that there exists an asymmetrical distribution of power that favours the employers and so they would prevail. This paper suggests an approach to resolving the conflicting interests associated with workplace privacy and surveillance. It suggests the discourse be in terms of justice and applies Rawls theory of distributive justice. It then evaluates the Workplace Surveillance Act 2005 of New South Wales. It is one of the few examples of specific workplace surveillance legislation in the world. It finds that when evaluated against Rawls fair rules it is seriously deficient and represents a missed opportunity to resolve the conflicting interests.

Keywords

Workplace surveillance, workplace privacy, distributive justice

INTRODUCTION

The issue of workplace surveillance is not new. The idea of personal privacy is not new either. In ancient Rome transparency of home and work arrangements was central to that society. Prior to the Industrial Revolution, village life had always been communal where the concepts of individualism and personal privacy were foreign. Even after the industrial revolution life in the cities was still closely regulated and communal. However, in the west the concept of Human Rights was developed and personal privacy was included. The concept of Human Rights has been increasingly expanded in the post WW2 period to the present. Even then we must remember that in that period workplace surveillance was the norm. The time and motion era of Taylor is one example[1]. Surveillance extended beyond the workplace. Henry Ford's "sociological department" visited homes of employees to determine whether they gambled, drank or sent money to foreign relatives. The policy of workplace surveillance and the use of technology to enable it is not a recent phenomenon. It is a truism but information and communications technologies (ICT) enable workplace surveillance on an unprecedented scale and increasingly at a level that no employee activity can escape it. Refer to the Schulman (2001) study and the American Management Association (2005) annual survey of workplace monitoring and surveillance for example.

ICT professionals should be concerned about the use made of their artefacts. They should be professionally and ethically obliged to not participate in the design and use of an artefact that will harm. In a addition they have an obligation to inform other professionals and members of society of the relevant issues associated with the use of ICT. At times this obligation extends to political intervention, either individually or collectively through a Professional Body, to influence the State or private organisations to undertake or not undertake an action.

Workplace surveillance is a sub set of surveillance prevalent in today's society. ICT provides the capability to create a Panopticon society.[2] A police state characterised by omniscient surveillance and mechanical law enforcement. The so-called "war on terror" has accelerated this trend. The ultimate impact will be the virtual (excuse the pun) disappearance of privacy. However, this paper is concerned with workplace surveillance. Specifically, after Itrona (2004) it suggests that the discourse should be in terms of justice and particularly applies Rawls theory of distributive justice (1958) and (1971). It then evaluates the recent Workplace

[1] Parenti (2003) has documented America's history of surveillance and repression from the pre civil war period to the war on terror.
[2] The 18th century utopian philosopher Jeremy Bentham's panopticon was a prison designed so jailers could observe all prisoners at any time but the prisoners were unaware when they were being observed.

Surveillance Act (2005) of New South in accordance with Rawls theory. It then discuses useful lessons for others who need to address the issue of workplace privacy and surveillance.

BACKGROUND

It is always important to define the important entities under investigation and the scope of the discussion and this area is no exception. Accordingly we need to at least address the entities of privacy, workplace and surveillance.

Privacy International (2003) reviews some of the definitions offered for privacy. They range from the simplest offered by Louis Brandeis in the 1890s as "the individuals right to be left alone" to the more contemporary Robert Ellis Smith who defines privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves". The Calcutt Committee in the United Kingdom (1990) stated that they were unable to find a wholly satisfactory statutory definition of privacy. Nevertheless, they believed it could be defined legally as "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information". Traditionally, privacy has been viewed as a Human Right and the United Nations Declaration of Human Right in article 12 states "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

Privacy International (2003) provides a useful framework for consideration of the concept of privacy. It identifies four separate but related dimensions. First, information privacy involves the establishment of rules governing the collection and handling of personal data such as credit, medical and government. Second, bodily privacy concerns the protection of a person's physical self against invasive procedures like genetic testing, drug testing and cavity searches. Third, communications privacy includes the security and privacy of mail, telephones, e-mail and other communication forms. Finally, territorial privacy concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and identity checks.

In this paper our major concern is with handling of personal data and communications. Obviously we are also concerned with "territorial privacy" as we need to be able to define "workplace" and distinguish it from other spaces like "domestic" or "public". As a starting point if you access the internet a number of definitions are returned. They include:

- the workplace includes but is not limited to the physical work site, restrooms, cafeterias, training sessions, business travel, conferences, work related social gatherings, etc.
- "Workplace" means any plant, yard, premises, room or other place where an employee or employees are engaged in the performance of labor or service over which the employer has the right of access or control.
- a place where work is done; "he arrived at work early today"
- Workplace means a place (whether or not within or forming part of a building, structure, or vehicle) where any person is to work, is working, for the time being works, or customarily works, for gain or reward; and in relation to an employee, includes a place, or part of a place, under the control of the employer (not being domestic accommodation provided for the employee).

Like Privacy it is difficult to find a wholly satisfactory definition of "workplace". The key notions are a place where work is performed, it is performed for gain or reward and at a place rightfully under the control or access of an employer. Work for gain or reward can however be performed at an employee's home. Whether this is included as a "workplace" seems to depend on the whether an employer has the right of "control or access". This right would probably apply where an employee is using employer-provided resources like a computer. Would it apply if it was employee-provided resources? In order to answer this question we need a definition of "work". The Surveillance Act (2005) of NSW defines "at work" for purposes of the legislation. It states that an employee is at work for an employer when the employee is at a workplace of an employer whether or not the employee is actually performing work at the time or at any place while performing work for the employer. In the latter case if work is performed "at home" regardless of who provides the resources it would appear to come under the act. Thus, what may be regarded as a "domestic space", like an employees home, may at least in part and for some period of time be considered a "workplace" and therefore subject to access or control of the employer.

Again defining the concept of workplace surveillance is not as straightforward as would first appear. Surveillance is not primarily of the "workplace" as such but rather the employee "at work". Workplace surveillance refers to the formal and informal practices of monitoring and recording aspects of an individual

employee or group of employers "at work". The NSW Act makes a distinction between Covert and Overt Surveillance but curiously does not explicitly define the latter. Covert Surveillance basically means that the employee is not formally made aware of the surveillance. Overt Surveillance, by implication, means that the employer is formally made aware of the surveillance. Employers choose to undertake surveillance for many reasons but basically it is for the purpose of making some judgement about an employee's behaviour. The judgement may be about appropriateness or whether it is productive or desirable.

In summary, the key concepts are not easy to define. For purposes of this paper we believe that the concept of privacy that encompasses the four dimensions, previously referred to, is useful. Again we believe that a "workplace" must be where the employer has a right of control or access. Finally, surveillance refers to those formal and informal practices of monitoring and recording aspects of an individual employee or groups of employees at work.

Given these understandings, can we expect employees and employers to formulate an agreed set of rules regarding privacy and surveillance rights that is considered fair or just to both. With few exceptions we assert the answer is no. Employees and employers have competing interests or in our case competing rights. Employees have the right to privacy and employers have the right to undertake surveillance of the employee in the workplace. The reality is that an asymmetrical distribution of power exists which favours the employers and so they would prevail. Also in many workplaces each party views each other with suspicion and more fundamentally do not trust each other. See for instance the important work of Mayer and others (1995) regarding trust. As result it is unlikely that both parties can formulate a set of just rules to which they both agree. For employers to use their dominant power to force employees to "agree" to surveillance would leave them angry and aggrieved.

At the risk of simplification philosophers essentially view ethical behaviour in terms of the golden rule "do to others as you would have them do to you". If this was followed in workplace relations then there is a greater probability of formulating a just set of rules. Employers would sensitively provide for greater workplace privacy. They would do so because they put themselves in the place of the employee who desires greater workplace privacy. Alternatively employees would recognise the employer's need to monitor and record certain employee activities. Every right has a commensurate obligation for the recipient to behave ethically. We know that unethical behaviour by employees is prevalent and gives rise to the employers demand for increased surveillance to counter such behaviour. The reality is, particularly in the workplace, that the golden rule is seldom or at best imperfectly followed. We know that worldwide there are concerns that employee privacy is increasingly violated. The use of ICT enables this increased violation as it becomes more sophisticated, relatively cheap and easy to install and use

This paper suggests an alternative approach to resolving the conflicting interests associated with workplace privacy and surveillance. It suggests the discourse be in terms of justice and applies Rawls theory of distributive justice. In such an environment the type of technology and its level of sophistication becomes largely irrelevant.

RAWLS THEORY OF JUSTICE

Rawls theory of justice as fairness is offered as a means to assist us with the practical issue of evaluating some action, rule or institution. A problem is that these will involve good effects for some but bad effects for others. There are conflicting interests. In terms of the issue addressed here the conflict is essentially between the privacy interests of employees against the organisational goals of the employers. Surveillance can assist organisational goals in terms of effective and efficient resource allocation but can violate the privacy of the organisation's employees. Distributive justice is a means by which rules of justice may be used to make decisions, in this case about workplace surveillance. Our key question is what is a fair distribution of privacy and surveillance rights?

Rawls adopts the concepts of the "original position" and the "veil of ignorance" in his theory of justice. It is only behind the "veil of ignorance" that the rules of justice can be developed. In the "original position" participants choose rules they consider would have the best effect. However, they choose these rules ignorant about themselves and context. For instance they do not know if they are an employee or employer and therefore their relative power in the organisational context. In other situations participants would be ignorant of gender, age, physical strength etc. The motive of the participants is not fairness or some net increase in happiness (after the manner of utilitarianism) [3] but self interest which is much more pragmatic. Nor do we have to rely on each participant following the "golden rule".

[3] Rawls disagree with the utilitarianism as it ignores the subordination of one group to another so long as the net outcome of a choice is good. Rawls believed justice to be violated by acceptance of any degree of subordination so long as the good is increased.

What rules are likely to formulated from the perspectives of an employee and an employer? Introna (2004) suggests the following and addresses them in terms of the individual and collective perspective and is summarised here. Employees out of self interest would suggest rules that would limit all forms of capturing data about themselves and their activities. There are two main reasons for this. First, is an acceptance that there are no such things as neutral or objective judgements. Surveillance information would be incorporated into the judgement process with a risk it will not serve the employees interest. Second, is the recognition that an employee usually lacks the power of the employer and therefore is weaker in bargaining for the fair use of the information once captured. If surveillance information was captured then as a fall back the employees would suggest rules to ensure maximum control over what information is captured, who is able to access it, how it is used etc.

Employers would make rules for the complete and comprehensive capture of the activities and use of the organisations resources by employees. This is considered necessary to ensure the goals of the organisation are achieved. This depends on effective and efficient resource usage of all employees and for the benefit of the organisation only. These rules would ensure maximum control over the capture of data and activities for every employee.

Before we identify the likely rules for distributing workplace privacy and surveillance rights generated in the "original position" behind the "veil of ignorance" there is one other important relevant concept. In the "original position" Rawls argues that participants would choose two principles of justice, lexically ordered. One affirms the equality of basic rights and the other that views inequalities according to the "difference principle". 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. However, it is not enough to say inequalities act as incentives it has to be demonstrated that a degree of inequality is necessary to achieve a high level of welfare for the lowest group in society. Rawls believes that these principles are necessary to ensure those participants behind the "veil of ignorance" will produce a set of just (fair) rules for distributing these rights. He believes people in the "original position" will select the "difference principle" because what they want is their own individual (selfish) welfare. What restricts their egoism is that they do not know what arrangement favours them over others. So they play safe.

Most would agree that in organisations the individual employee (and even when collectivised as unions) have less power than individual employers (or groups of employers or their representative bodies). It is therefore difficult to argue that in terms of the "difference principle" it is the employee that is the "worst off" in terms of securing fairness over privacy in the workplace. It is therefore highly likely that participants behind the "veil of ignorance" will formulate rules with a bias in favour of the employee. What then are the likely rules to be formulated? These can easily be found in other legislation and Codes of Practice especially those concerning privacy of personal data. Refer for instance to NSW Government (1996, 1988), ILO (1997), OECD (1980), Australian Government (1988). Those "fair" rules relevant to workplace surveillance include:

1. Information collected is necessary for the performance of organisational functions and employees will be informed of this. This recognises that employers have a right to monitor employee activities and resource usage. Based on the "difference principle" the onus is on the employer to justify such monitoring.
2. Information is collected where practicable from the employee. This recognises that in some circumstances the information can be directly obtained from the employee.
3. Employees will be informed about who is collecting the information.
4. Employees will be informed how they may access the information relating to them and how to make corrections if necessary.
5. Employees will be informed about who else has access to the information relating to them and why.
6. Employers must ensure information on employees is accurate, complete and current for the organisational purpose.
7. Employers must take reasonable measures to protect information from misuse, loss, unauthorised access, modification or disclosure.
8. Employers must provide and actively publicise "best practice" policy on email use and the consequences of not abiding by the guidelines
9. Employers must provide and actively publicise "best practice" policy on network use and the consequences of not abiding by the guidelines.

10. Employers must provide and actively publicise a clearly expressed current policy on the collection, storage, use and management of employee information

THE WORKPLACE SURVEILLANCE ACT 2005

On the 23 June 2005 the Workplace Surveillance Bill was assented to in the parliament of the Australian state of New South Wales (NSW). It is one of the few examples of specific workplace surveillance legislation in the world (referred to in this paper as the Act). The Act extends the regulatory scheme in the Workplace Surveillance Act 1998 that concerned video to two other forms of surveillance. These are tracking and the computer, including monitoring of employees' emails and internet browsing. Employees are defined broadly under the Act as "at work" which means at a workplace or another place while working. It prohibits the following:

1. Camera, computer and tracking surveillance unless employees have been notified in the manner specified by the Bill or in the case of covert surveillance it has been authorised by a magistrate for the purpose of establishing whether an employee is involved in any unlawful activity at work.
2. Camera, computer and tracking surveillance in any change room, toilet or shower facility.
3. Employer blocking delivery of an email or access to a website unless the employer has a policy on email and internet access and is acting in accordance with that policy and in the case of emails the employee is notified that delivery of an email has been blocked (except for certain emails eg offensive, SPAM). The employer's policy cannot provide for blocking merely because the email/website relates to industrial matters.

The response to its preparation and subsequent debate indicates the reality when the conflicted participants do not operate behind a "veil of ignorance". It also underlines why it necessary for the State to legislate to ensure some measure of fairness in the workplace. First, because the parties position on rights are significantly different, often intransigent. Second, because there is the recognition that power largely rests with the employer.

The Labour Party governs NSW. It is a party that historically developed from organised labour and has close ties with the union movement. Such legislation is more likely from the Labour Party than the main opposition coalition of the conservative parties of Liberal and National Party who opposed the Act. The coalition argued the Act was biased in favour of the employees. The Democrats (centrist party) and the Greens (left of centre party) both argued the Act was an improvement in better securing privacy rights but it was weak especially in enforcement.

In tabling the draft Bill in Parliament the minister responsible stressed how new technologies had dramatically changed the workplace. However, these bring risks to individual privacy but also create problems for employers with overuse of email and downloading and dissemination of inappropriate material. The minister indicated that the government will not tolerate secret monitoring of private telephone calls and conversations, cameras in change rooms and toilets and "bosses snooping into the private emails of workers". The minister also stated that " the government recognises these competing entitlements and seeks to strike the right balance between privacy rights and business interests".

The Labour Council of NSW, the peak body for trade unions, predictably supported the extension of the current regulatory regime (on video) to computer and tracking surveillance. It argued that the Bill should have gone further and included biometrics.

Equally predictably, the Australian Retailers Association argued that the legislation was not needed and that self regulation was adequate. Moreover, it argued that employers should not be required to seek approval from a magistrate to use covert surveillance. Both the NSW Chamber of Commerce and Australian Business Industrial Support, peak bodies of employers, agree with the Retailers. They also argued that the notice requirements will impose substantial costs on business and that the prohibition on blocking union emails is unreasonable. They also refer to the problem of different State/ Territory legislation for business that operate across state/ territory borders as problems created for business.

Without the "veil of ignorance" the creation of just (fair) rules on the distribution of privacy and surveillance rights would be very unlikely given the significantly different views of employees and employers. Given that power largely rests with the employers then the prospect of a fair distribution of rights requires the intervention of the State.

THE NSW ACT AND RAWLS THEORY

If we accept that the rules previously discussed are likely outcomes from Rawls theory then to what degree to they apply to the Act. It should be viewed as a positive attempt by the Government of New South Wales to establish just rules on the distribution of privacy and surveillance rights. However, it is seriously deficient when evaluated against the rules established from Rawls theory. The deficiencies emanate from a rigid distinction drawn between overt and covert surveillance and its associated prohibited surveillance. Covert surveillance is defined as "surveillance of an employee while at work for an employer carried out or caused to be carried out by an employer and not carried out in compliance with the requirements of Part 2". Part 2 is mainly concerned with the notice requirements that employers must provide to employees including some additional requirements associated with each of three surveillance types of cameras, computer and tracking. Overt surveillance is not defined in the Act but covers all other surveillance (other than covert and prohibited) activities.

The Act prohibits any surveillance of employee change rooms or toilet/ shower/ bath facility at the workplace. For some it may be a surprise that this must be legislated against at all as most would consider it a clear case of violation of personal territorial privacy. However, numerous instances of this surveillance are reported usually when some one is charged with sexual gratification under the Summary Offences Act. As an aside the Act does not cover surveillance in these places of non employees, for example, customers or general members of the public. Thus, hidden cameras in public toilets or changing rooms of retail stores are not prohibited by this Act nor is this adequately covered by other legislation.

It also prohibits surveillance of an employee who is not at work unless the employee has the use of equipment or resources provided by the employer (presumably to be used at home for work purposes). Thus, tracking devices on work provided vehicles or mobile phones for instance will effectively track employees on the road or at home.

Again, the Act prohibits the blocking of emails and internet access of employees. However, if an employer acts in accordance with an Acceptable Use Policy (AUP) that has been publicised to the employee then it is lawful. In the case of blocking the delivery of an email the employer must give a "prevented delivery notice" as soon as practicable to the employee. There are exceptions to this requirement. One is if the email was Spam, under the definition of the Federal Spam Act 2003, and it might damage the network or is menacing, harassing or offensive and, the employer was not aware (and could not be reasonable expected to be aware) of the identity of the employee who sent it. The Act also specifically prohibits reference in the AUP to blocking emails or internet access solely for the reason industrial matters (presumably trade union).
Part 4 of the Act deals with covert surveillance of employees at work and is prohibited unless authorised by a magistrate as necessary to establish whether an employee is engaged in unlawful activity. The exceptions are law enforcement, correctional centres, casino and courts. However, the positive impact of this regulation on privacy is likely to be undermined by allowing justification by employers claiming surveillance is justified on the grounds of security.

The Act makes a distinction between Covert and Overt Surveillance. This distinction is deficient First, there is no regulation of overt surveillance beyond the employer requirement to meet the notice and other requirements. Apart from notification and signage requirements most of the fair rules associated with the collection, storage, use, disclosure, accessibility and accuracy of information obtained through overt surveillance are violated. The Act requires that notice be given as whether surveillance is camera or computer or tracking), how it will be carried out, when the surveillance will begin, whether it will be intermittent and whether it will be for a specified period or ongoing. The Act is silent on the more important privacy concerns of which specific area(s) is surveillance to be undertaken, the specific purpose(s) for it, employee access to personal information, a mechanism to correct any inaccuracies and disclosure to other parties. It also does not require a consultation process with employees on matters like the nature and capacities of the surveillance devices, how the data collected will be used, how any disputes can be settled or mechanisms for ongoing consultation.

Second, the Act may place employers at risk at meeting notice requirements through forgetfulness or accident and transform overt surveillance into covert surveillance. The Australian Privacy Foundation - APF (2005) provide an example where "the employer who accidentally gives only 13 instead of 14 days prior notice to employees that she is taking delivery of new fleet cars which will have their GPS systems switched on". The APF (2005) also provide the example where "a home owner who has installed a CCTV system to protect their home employs a person (say a nanny) and forgets to provide the nanny with written notice of its existence". The homeowner as employer is in breach of the Act.

Third, the Act may impact the privacy of other persons other than employees and employers. Clause 14 of the Act allows for surveillance of the workplace for purposes other than that of employees so long as a substantial number of employees have agreed to do so. It would appear that customers or members of the public could be

subject to surveillance and without none of the notification, visibility or signage requirements. It may allow CCTV for example in foyers or public toilets.

SUMMARY AND CONCLUSION

Rawls theory of justice as fairness is offered as a means to assist us with the practical issue of workplace privacy and surveillance. It is an issue where a conflicting interest exists. A conflict between the privacy interests of employees against the organisational goals of the employers. Surveillance can assist organisational goals in terms of effective and efficient resource allocation but can violate the privacy of the organisation's employees. Distributive justice is a means by which rules of justice may be used to make decisions that resolves a conflict. Our context is workplace surveillance. It recognises that whilst a just negotiated set of rules between employees and employers may be possible it is unlikely. First, because of the significant different views of employees and employers. Second, because of the distribution of bargaining power overwhelmingly rests with employers. A better approach is to identify those rules to distribute workplace privacy and surveillance rights that would be formed behind the "veil of ignorance" and enforce them by legislation.

Using Rawls theory of justice a number of rules for distributing workplace privacy and surveillance rights behind the veil of ignorance were proposed. The NSW Workplace Surveillance Act 2005 was evaluated in terms of these fair rules. The NSW parliament is commended for passage of the legislation as one of the few in the world to specifically seek to balance the conflict of interests between employee privacy and the organisational goals of the employer. However, it represents a missed opportunity to do so as it fails to regulate overt surveillance beyond some signage and notification problems. In particular the employee is denied the right to know what is the specific purpose of the surveillance, to have access to information about them, together with a mechanism to challenge and correct any inaccuracies, and, little security against loss, unauthorised access, use, alteration or disclosure of such information. The Act may also allow employers to conduct covert surveillance of employees while not at work and those of customers and visitors to the workplace.

ICT professionals should be concerned about the ethical use of artefacts, whether surveillance, censorship, crime or terrorism for example. All influential professional bodies of the ICT domain have Codes of Conduct or Codes of Ethics. Individual ICT professionals should act in accordance with these codes. The Professional Society should exercise leadership in pro-active promotion of the Codes and seeking compliance. They should also actively promote discussion on important ethical and societal issues, like workplace surveillance, and where necessary adopt a position on an important issue. The ICT professional cannot have recourse as a defence "not my problem".

REFERENCES

American Management Association (2005). *Electronic Monitoring & Surveillance Survey.* ePolicy Institute.

Australian Privacy Foundation (2005). *Analysis of the Workplace Surveillance Bill 2005*. http://www.privacy.org.au/Campaigns/Workplace/ date accessed December 20 2005.

Commonwealth of Australia, (1988). *Privacy Act.* Act no. 119.

International Labour Organisation, (1997). *Protection of Workers' Personal Data*, ILO Publications, Geneva, Switzerland.

Introna, L. D. (2004). "Workplace Surveillance, Privacy and Distributive Justice", in Spinello, R. A. et al. (eds.) *Readings in Cyberethics*, pp.476-487,Jones and Bartlett, MA, USA.

Mayner, R, Davis, J and Schoorman, D. (1995). "An Integrative Model of Organizational Trust". *Academy of Management Review*, Vol. 20, No. 3.

New South Wales, (1996). "Video Surveillance in the Workplace", *Report of the Working Party to the Hon J W Shaw Attorney General and Minister for Industrial Relations*, NSW Department of Industrial Relations, Sydney.

New South Wales, Parliament. (2005). *Workplace Surveillance Bill.* Act no. 47.

New South Wales Parliament (1998). Privacy and Personal Information Protection Act.

New South Wales Library Research Service. (2004). *Workplace Surveillance*. Briefing Paper no. 13/04.

Parenti, C. (2003). *The Soft Cage: Surveillance in America from Slave Passes to the War on Terror.* Basic Books.

Rawls, J. (1958). "Sense of Justice", *Philosophical Review*, vol. 67, no. 2, 164-194.

Rawls, J. (1971). *The Theory of Justice*. Belkap Press of Harvard University Press, Cambridge, MA.

Roth, L. (2004). Workplace Surveillance: Briefing paper No 13/04, NSW Parliamentary Library Research Services.

Report of the Committee on Privacy and Related Matter ("the Calcutt Report"). (1990). HMSO Cmnd 1102.

Schulman, A. (2001). The Extent of Systematic Monitoring of Employee E-mail and Internet Use. Privacy Foundation, http://www.sonic.net/~undoc/extent.htm date accessed March 28 2006.

COPYRIGHT