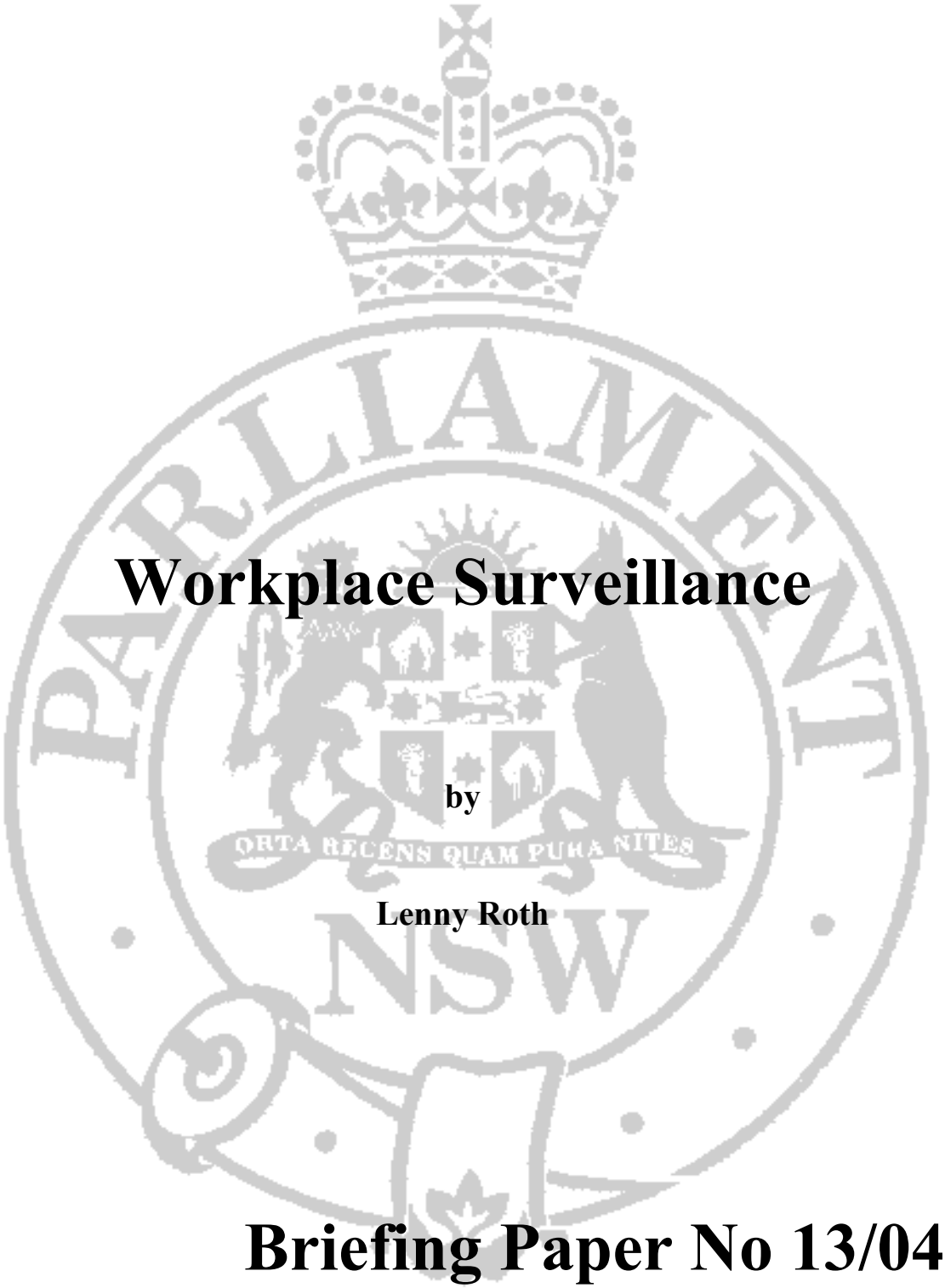
NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE



Workplace Surveillance

by

Lenny Roth

Briefing Paper No 13/04

RELATED PUBLICATIONS

- *Listening Devices and other forms of surveillance: issues and proposals for reform* – Briefing Paper No. 20/97 by Rachel Simpson.

- *Privacy Law Reform: Issues and Recent Developments* – Briefing Paper No. 20/98 by Gareth Griffith.

ISSN 1325-4456
ISBN 0 7313 1770 X

October 2004

Workplace Surveillance

by

Lenny Roth

NSW PARLIAMENTARY LIBRARY RESEARCH SERVICE

David Clune (MA, PhD, Dip Lib), Manager ..... (02) 9230 2484

Gareth Griffith (BSc (Econ) (Hons), LLB (Hons), PhD),
Senior Research Officer, Politics and Government / Law ..... (02) 9230 2356

Talina Drabsch (BA, LLB (Hons)), Research Officer, Law ..... (02) 9230 2768

Rowena Johns (BA (Hons), LLB), Research Officer, Law ..... (02) 9230 2003

Lenny Roth (BCom, LLB), Research Officer, Law ..... (02) 9230 3085

Stewart Smith (BSc (Hons), MELGL), Research Officer, Environment ... (02) 9230 2798

John Wilkinson (MA, PhD), Research Officer, Economics ..... (02) 9230 2006

Should Members or their staff require further information about this publication please contact the author.

Information about Research Publications can be found on the Internet at:

www.parliament.nsw.gov.au/WEB_FEED/PHWebContent.nsf/PHPages/LibraryPublications

CONTENTS

EXECUTIVE SUMMARY

Exposure Draft Workplace Surveillance Bill 2004 (p 1-4)

On 23 June 2004, Hon Mr Bob Debus MP released an exposure draft *Workplace Surveillance Bill 2004* for public consultation. This Bill would extend the regulatory scheme in the *Workplace Video Surveillance Act 1998* to two other forms of surveillance: (1) tracking surveillance, and (2) computer surveillance, including monitoring of employees' emails and internet browsing. Employers would be required to notify employees, in the manner specified, before engaging in these types of surveillance. Covert surveillance could only be used if authorised by a magistrate for the purpose of establishing whether an employee was involved in any unlawful activity at work. The Bill would also regulate blocking of employees' emails and access to websites, including by prohibiting the blocking of union emails.

Background to Workplace Video Surveillance Act 1998 (p 5-16)

The Workplace Video Surveillance Act 1998 was introduced following a report on the issue by the NSW Privacy Committee and a subsequent majority report by a Working Party commissioned by the NSW Attorney General. Employer groups and the Coalition opposed the legislation on the basis that it would unduly restrict employers' ability to deal with theft in the workplace. The competing interests relating to video surveillance have been summarised as follows: 'To employers, video surveillance is a means to expose theft, vandalism and misconduct; to reduce security risks and legal liability; and to replace other forms of security and supervision. Employees see its potential to dehumanise their working environment; to deny them a reasonable expectation of privacy; to harass individuals and to put them under constant surveillance.'

Computer surveillance of employees (p 17-35)

Employers argue that they own the computer equipment being used by employees and that they should be entitled to monitor employees' use of that equipment for legitimate reasons such as (i) detecting excessive personal use of computers, (ii) avoiding legal liability, including in relation to sexual harassment claims arising from office emails containing pornography, (iii) preventing employees from leaking confidential information, and (iv) maintaining the security of the computer system. On the other hand, unions, privacy groups and others claim that regulation is needed to prevent employers from unjustifiably using covert surveillance and from otherwise using computer surveillance in a way that denies workers their reasonable expectation of privacy, particularly with respect to their email communications.

Tracking surveillance of employees (p 35-42)

Tracking surveillance includes the tracking of employees outside the office, through tracking of company vehicles and mobile phones, as well as tracking employees inside the office, through the use of office access cards and "active badges". Vehicle tracking is the most common and this is used to increase efficiency, to enhance customer service, for security, and to comply with safety requirements. There have been a number of union complaints about the use of tracking devices. Employees do not want their

employers secretly tracking their movements – and they also resent employers overtly tracking their every movement throughout the day, including during break times. They also fear that tracking devices will be used to unfairly discipline drivers.

Current regulation of workplace surveillance (p 43-47)

Workplace video surveillance is regulated by the *Workplace Video Surveillance Act*. Other laws of potential relevance to workplace surveillance can be summarised as follows. There is no common law action for breach of privacy. There is doubt as to whether federal telecommunications interception laws prohibit email monitoring. Federal privacy legislation provides only limited protection to workers because of exemptions relating to "small businesses" and "employee records". The latter exemption is under review. Under NSW industrial laws, surveillance can be addressed in awards and enterprise agreements and can form the basis of an industrial dispute. Under federal industrial laws, surveillance cannot be included in an industrial dispute but can be a negotiated condition of an industrial agreement. Unfair dismissal laws may provide relief against dismissals that are based on surveillance evidence.

NSW Law Reform Commission Interim Report (p 48-51)

The NSW Law Reform Commission's Interim Report (2001) recommended comprehensive surveillance legislation, which would also be applicable to the workplace context. The Commission's proposal, as it relates to workplace surveillance, is similar in structure to the draft Bill but there are some significant differences between the two. The main difference is that the Commission proposes regulation of overt surveillance in addition to regulating covert surveillance. Employers would need to comply with eight legislative principles when undertaking overt surveillance. The Commission's final report is due in December 2004.

Some stakeholder views on proposed legislation (p 52-58)

Unions & privacy bodies: The Labor Council supports the extension of the current regulatory regime to computer and tracking surveillance. The Council also submitted that biometrics should be regulated. The Office of the NSW Privacy Commissioner and the Australian Privacy Foundation have criticised the Bill for failing to also regulate overt surveillance, as recommended by the Law Reform Commission. Both privacy organisations also argue that enforcement mechanisms should be improved.

Employers: The Australian Retailers' Association maintains its position that self-regulation is adequate and that employers should not be required to seek approval from a magistrate to use covert surveillance. The NSW State Chamber of Commerce and Australian Business Industrial support that view and argue that notice requirements in the legislation will impose substantial costs on businesses. They also refer to the problems of having different state legislation for businesses that operate across state borders. It is also argued that the prohibition on blocking union emails is unreasonable.

Workplace surveillance laws elsewhere (p 59-73)

Australia: No other state or territory has introduced specific workplace surveillance legislation However, Victoria has recently proposed two alternate options for regulation of workplace surveillance and testing. The first option would require employers to seek authorisation from a regulator before undertaking either some or all surveillance or testing. The second option would require employers to comply with a set of principles on how they implement and conduct surveillance and testing.

Overseas: In the US, two legislative proposals at federal level to require notice of monitoring have failed but similar laws have been introduced in at least two US states. The UK has issued a code of practice on workplace monitoring to guide employers on compliance with privacy laws. In Canada and New Zealand, where privacy laws apply to the workplace, no such regulatory guidance has been issued. Some European countries have adopted specific workplace surveillance legislation or issued guidance. The EU has recently proposed a Directive on the protection of employees' data.

Other workplace privacy issues (p 74-79)

A number of other workplace privacy issues have been raised in recent years. One of those issues is biometric identification, which is the identification of employees based on physical characteristics such as fingerprints or irises. This is generally used to control access to and within buildings and in relation to time clocks. Another current issue is testing of employees and prospective employees. Testing includes medical testing, psychological testing, drug and alcohol testing, and genetic screening.

1. INTRODUCTION

1.1 Release of draft Workplace Surveillance Bill

On 23 June 2004, the NSW Attorney General, the Hon Mr Bob Debus MP, released an exposure draft *Workplace Surveillance Bill 2004* for public consultation. The effect of this Bill would be to extend the regulatory scheme in the *Workplace Video Surveillance Act 1998* to two other forms of surveillance, namely tracking surveillance and computer surveillance, including the monitoring of employees' emails and internet usage. This is the first legislation of its kind in Australia but the Victorian Law Reform Commission has also recently proposed legislation in this area.[1] The draft NSW Bill has been released before the NSW Law Reform Commission has delivered its final report on Surveillance.[2] In its 2001 *Interim Report*, the Commission recommended legislation to regulate surveillance generally, including in the workplace.[3]

On tabling the draft exposure Bill in Parliament, the Hon Mr Bob Debus said:

> … During the past two decades the complexion of the workplace has changed dramatically with the introduction of new technologies. Email and the Internet, in particular, have revolutionised workplace communication and provided unparalleled access to information.
>
> However, these new freedoms have also brought risks to individual privacy that could not have been imagined 20 years ago. Employers have had to come to terms with and create strategies to deal with overuse of email and the problems associated with the downloading and dissemination of inappropriate material. In a number of cases, employers have resorted to a range of practices to monitor email use, including covert surveillance of their employees. Union and employee disquiet has been growing—justifiably—about the use of covert surveillance in the workplace. While some employers argue that it is necessary to protect their legitimate interests, employees expect that their private correspondence, like their private telephone calls or private conversations, should never be the subject of secret monitoring. We do not tolerate employers unlawfully putting cameras in change rooms and toilets. We should not tolerate bosses snooping into the private emails of workers either.
>
> The Government recognises these competing entitlements, and seeks to strike the right balance between privacy rights and business interests. In 1998 the Government established a balanced legislative model to deal with visual surveillance in the workplace. Under that model, employers are required to give employees notice of any visual surveillance undertaken in the workplace, unless—an important qualification—they have obtained an authorisation from the Local Court. Authorisations for covert surveillance are only granted where there is a legitimate reason for secrecy, such as unlawful activity reasonably suspected in the workplace. An employer who secretly undertakes visual surveillance without court authorisation is guilty of a criminal offence. The Government's draft exposure bill extends this fair and entirely straightforward scheme to all other forms of workplace surveillance, not only those that monitor email usage, but other technologies, such as tracking devices, which have been used on occasion to trace employees' whereabouts as part of performance monitoring.
> …

[1] This is discussed below at section 9.2.1.

[2] The final report is scheduled for release in December 2004.

[3] This is discussed below at section 7.

> It is worth mentioning that the existing workplace video surveillance has proved a highly effective approach to the matter. In 2003 only 16 out of 154 applications for authorisations were refused, which is a very high level of success. The exposure bill will provide unions, employees and the owners of small and large business the opportunity to have input into the development of a comprehensive commonsense solution. [4]

1.2 Current status of draft Bill

The consultation period for the Bill was scheduled to end on 4 August 2004 however submissions were received later than this date.[5] As at 7 October, the Attorney General's Department had reviewed the submissions and was preparing an internal report.[6]

2. SUMMARY OF DRAFT WORKPLACE SURVEILLANCE BILL

2.1 Types of surveillance regulated

The three forms of surveillance that would be regulated by the draft Bill are:

> ***Camera surveillance:*** the monitoring or recording, by electronic means, of visual images of the employee (such as by means of a closed-circuit television system);
>
> ***Computer surveillance:*** the monitoring or recording by means of software or other equipment of the information input or output, or other use, of a computer used by the employee (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites),
>
> ***Tracking surveillance*****:** the monitoring or recording of the geographical location or movement of the employee by means of an electronic device (such as tracking of the employee or of any vehicle driven by the employee by means of a Global Positioning System tracking device).[7]

2.2 Surveillance by employers of employees at work

The draft Bill would regulate these three types of surveillance by *employers* of *employees* (defined broadly) *at work* (also defined broadly, ie meaning at a workplace or at any other place while working).[8]

---

[4] *NSWPD*, Legislative Assembly, 23/6/04.

[5] Telephone communication with Attorney General's Department on 7 October 2004. The department received around 40 submissions.

[6] Ibid.

[7] Draft exposure *Workplace Surveillance Bill 2004,* clause 3.

[8] Clauses 3, 4.

2.3 The way in which workplace surveillance is regulated

In summary, the draft Bill would:

(1) Prohibit these three types of surveillance unless (a) employees have been notified in the manner specified of the surveillance (see below); or (b) covert surveillance (ie surveillance without such notice) has been authorised by a magistrate for the purpose of establishing whether an employee is involved in any unlawful activity at work.[9]

(2) Prohibit video surveillance (and tracking and computer surveillance) in any change room, toilet or shower facility.[10]

(3) Prohibit employers from blocking delivery of an email or access to a website unless: (i) the employer has a policy on email and internet access and is acting in accordance with that policy; and (ii) in the case of emails - the employee is notified that delivery of an email has been blocked (except for certain emails eg, offensive emails, Spam). But note that an employer's policy cannot provide for blocking merely because the email/website relates to industrial matters.[11]

2.4 The notice requirements

In relation to point 1(a), above, the notice requirements in the draft Bill are as follows. For all three types of surveillance employees must be notified in writing of the intended surveillance at least 14 days before it begins. In addition:

- For *camera surveillance* the cameras must be clearly visible and signs must notify people that they may be under surveillance in the place where the surveillance is taking place and at each entrance to that place;

- For *computer surveillance* employees must be notified by a sign which is clearly visible on or near the computer concerned; or by audible or written notice given by means of the computer concerned when the employee logs onto the computer or starts a program that is subject to surveillance;

- For *tracking surveillance* employees must be given notice that is clearly visible on the vehicle or thing which is being tracked.[12]

[9] Clause 8.

[10] Clause 9.

[11] Clause 11.

[12] Clause 5(2).

There are two exceptions to the above notice requirements. Both exist in the *Workplace Video Surveillance Act 1998* and are more relevant to video surveillance than computer or tracking surveillance. One exception is if: (a) the employee (or a body representing employees) has agreed to the use of surveillance at premises for a purpose other than surveillance of employees, and (b) surveillance is carried out in accordance with that agreement.[13] The other exception is if (a) surveillance is carried out solely for the purpose of ensuring security of the workplace and surveillance of any employee was extrinsic to that purpose; and (b) the employee was notified in writing in advance.[14]

2.5 Covert surveillance authorities

In relation to point 1(b), above, the draft Bill would regulate:

(i) The issuing of covert surveillance authorities;
(ii) The carrying out of covert surveillance under such authorities (e.g. a Licensed Security Operator must oversee the surveillance);
(iii) Access to and destruction of covert surveillance records; and
(iv) Restrictions on use and disclosure of such records.[15]

These provisions are summarised in **Appendix 1** to this paper.

2.6 Penalties for contraventions

Contraventions of the Act would be an offence, with a maximum penalty of 50 penalty units ($5,500 fine) for some offences and a maximum of 20 penalty units ($2,200 fine) for others.[16]

[13] Clause 5(3).

[14] Clause 8(3), (4). Note, this provision is expressed in the draft *Bill* as a defence to the general prohibition against covert surveillance rather than as an exception to the notice requirements

[15] See Part 3 of the draft *Bill*.

[16] See clauses 8(1),9, 10, 11, 21, 26(1), 27(1),(2).

3. BACKGROUND TO WORKPLACE VIDEO SURVEILLANCE ACT

3.1 Introduction

As the exposure draft Bill would, in effect, extend the regulatory scheme in the *Workplace Video Surveillance Act* to computer and tracking surveillance, it is relevant to provide some background to the introduction of that Act.

3.2 Minister's second reading speech

On the second reading of *Workplace Surveillance Bill* 1998, the Hon J W Shaw MLC stated:

> The object of the bill is to regulate the covert video surveillance of employees in the workplace by their employers. This is an industrial issue of great importance. Currently video surveillance in the workplace is unregulated. A number of major industrial disputes have arisen over video surveillance by employers. The fact that the area is presently unregulated has both surprised parties to disputes and contributed to the escalation of the disputes. The Government has developed a balanced system of regulation to address the issue.
>
> The bill is the outcome of extensive consultations between employee and employer organisations. In 1996 I commissioned a working party comprising employer groups, trade union representatives and government departmental officers to inquire into the use of surveillance cameras in the workplace.. The working party was convened following a series of industrial disputes arising from the covert video surveillance of employees at work. The working party was commissioned to pursue the following terms of reference:
>
> > To advise the Attorney General, and Minister for Industrial Relations on the use of video surveillance in the workplace, with a view to recommending:
> >
> > (a) the most appropriate legislative means to regulate covert workplace video surveillance; and
> > (b) to consider and take into account the recommendations of the September 1995 Report of the Privacy Committee of New South Wales, "*Invisible Eyes*".
>
> The working party report was delivered in December 1996 and recommended legislative change to require employers to obtain a court order before secretly filming employees. The court order will require employers to show why the undisclosed surveillance is necessary, and will impose strict limits on the scope of the surveillance. In implementing the recommendations of the working party, the bill strikes a balance between the competing interests of different parties. The privacy of employees is important in the workplace. Workers should be able to undertake their duties with as little interference as possible to their privacy.
>
> The thought of being constantly surveyed or monitored is of great concern to most people. The thought of being secretly surveyed is of even stronger concern. It can unnecessarily introduce distrust and suspicion into the workplace. On the other hand, employers should have the opportunity to investigate serious problems in the workplace. The bill defines what employers may investigate, that is, suspected unlawful activity by employees in the workplace. It is reasonable to provide a mechanism for employers to investigate unlawful activity, however, it should not be at the expense of employees' privacy any more than it needs to be.[17]

[17] *NSWPD,* Legislative Council, 26/5/98.

3.3 Parliamentary debates on Workplace Video Surveillance Bill

3.3.1 Coalition[18]

The coalition opposed the *Workplace Video Surveillance Bill.* The Hon J.P Hannaford MLC said that 'the coalition believes there is a need to address problems with workplace video surveillance equipment, but the approach of the Government is aimed directly at employees and does not provide an appropriate balance.' Mr Hannaford agreed with a submission from a major organisation in the video surveillance industry, which expressed the views that (1) the real problem lay with the Security Protection Act and the Private Inquiry Act – ie the persons working in the surveillance industry; and (2) video surveillance had significantly reduced employee theft in registered clubs.

Mr Hannaford said that if the Bill was passed 'an employer who is unable to point the finger at a particular employee or employees and specify that he or they are doing something wrong [would] be unable to obtain video surveillance to prove it…The commercial reality is that employees who want to fiddle the till for $10 at a time…will now be able to do so with impunity.' Mr Hannaford said that 'employers have a right to protect their own property and to ensure that fraud and misappropriation are not occurring in their workplace. The Bill effectively ensures that no employer will be able to provide that element of self-protection….' In conclusion, Mr Hannaford said 'this legislation will alienate the owners of every small and medium business in the State.'[19]

3.3.2 Australian Democrats[20]

In the second reading debate, the Hon Elisabeth Kirkby MLC expressed opposition to the Bill. Her greatest concern was that 'surveillance is to be overseen by a licensed security operator.' Mrs Kirkby stated, 'the current training and the standard of many people security firms employ is still not of a sufficiently high standard to make me feel confident that a licensed security operator is a suitable person to oversight covert video surveillance.' Mrs Kirkby also said that it was unsatisfactory that an employee would be left with little right of redress in the case of a breach of the voluntary code of practice on overt video surveillance. In committee, Mrs Kirkby said 'at the time I spoke I was not aware that apparently it is the practice for many employers to use covert surveillance without any regulation whatsoever. I still believe that the regulation in this Bill is inadequate, however, if it is the practice of some employers…to put in hidden cameras without the knowledge of employees, it is quite obvious that something has to be done to regulate what I believe to be an appalling practice.'

---

[18] See *NSWPD,* Legislative Council, 17/6/98.

[19] Note the Hon J.W Shaw made comments in reply. See *NSWPD,* Legislative Council, 17/6/98.

[20] See *NSWPD,* Legislative Council, 17/6/98.

3.3.3 Others[21]

The Greens generally supported the Bill, as did the Hon R.S.L Jones MLC. Reverend the Hon F.J Nile MLC said 'The Christian Democratic Party shares the concerns of other honourable members about the…Bill." At a later point in his speech, Reverend Nile said 'there seems to be some concern about the wording of the legislation, not the principle behind it.' Like the Hon Elisabeth Kirkby, Reverend Nile was 'concerned that security officers should be qualified.'

3.4 NSW Privacy Committee report

3.4.1 Introduction

In December 1994, the Privacy Committee of NSW launched an inquiry into workplace video surveillance.[22] The Committee initiated the inquiry following an industrial dispute relating to video surveillance in mid-1994, considering that 'an inquiry offered significant potential benefit to the community in lessening the scope for future industrial disputation.'[23] The *Privacy Committee Act 1975* authorised it 'to conduct research and make reports in respect of any matter relating to the privacy of persons.'[24] The Committee 'received written submissions from individuals and groups representing employers and employees; and from consultants, suppliers and installers from the security industries…. In March 1995, the Committee conducted public hearings to receive further evidence from interested parties.'[25] The inquiry culminated in a 132-page report published in September 1995, entitled *Invisible Eyes: Report on Video Surveillance in the Workplace*. The report is summarised below.

3.4.2 Summary of the Privacy Committee's report

Chapter 1 - Introduction

The issue in brief: In its report, the Committee summarised the issue as follows:

> Few technologies match the potential of video cameras to place people under constant surveillance and yet be undetectable. Because of its extraordinary capacities, video surveillance has emerged as a contentious issue both in the workplace and in public places. To employers, video surveillance is a means to expose theft, vandalism and misconduct; to reduce security risks and legal liability; and to replace other forms of security and supervision. Employees see

[21] See *NSWPD*, Legislative Council, 17/6/98

[22] The Privacy Committee of New South Wales, *Invisible Eyes: Report on Video Surveillance in the Workplace*, Report No. 67, September 1995, at p 9.

[23] Ibid, p 10-11

[24] Ibid, p 10-11.

[25] Ibid, p 11.

> its potential to dehumanise their working environment; to deny them a reasonable expectation of privacy; to harass individuals and to put them under constant surveillance.[26]

Privacy, the Workplace and Video Surveillance: The Committee referred to an International Labor Organisation (ILO) report summarising the concerns of employees relating to surveillance technologies in the following terms.

> 1. Their use is a violation of basic human rights and dignity, and is often carried out without adequate consideration for such interests.
>
> 2. [Electronic workplace] monitoring make prying into the private lives of workers easier and more difficult to detect than ever before.
>
> 3. Monitoring and surveillance give employees the feeling that they are not being trusted and thus foster a divisive mentality which is destructive to both workers and employers.
>
> 4. Such practices can be used to discriminate or retaliate against workers, which may be difficult for workers to discover.
>
> 5. Monitoring and surveillance involve both issues of exercising control over workers and control over data relating to specific workers.[27]

On the other hand, the Committee noted that employers:

> assert their right to use methods of surveillance in the workplace which they believe provide adequate protection for both assets and employees. Employers claim that the privacy rights of employees…are limited by the employer's interest in supervising the work of employees. Employers also frequently state that they simply see video surveillance as an effective means of improving security and in some instances, serving specific functions such as improving quality control and maintaining compliance with regulations. Many employers refute concerns about employee privacy, claiming to have no interest in the personal habits of employees.[28]

Increasing use of video surveillance[29]: The report notes that 'while it is difficult to determine the current extent of video surveillance in the workplace, it is clear that video cameras have become a standard feature of security systems for medium to large organisations.' Factors which helped explain this development included (1) the cost of video surveillance has fallen to the point where it is now affordable to all but the smallest businesses (2) the range of features offered in video surveillance equipment has widened just as costs have fallen dramatically (3) the increasingly competitive business environment has made companies look for every possible avenue to reduce costs and improve customer service; (4) video surveillance has become a more attractive option as other security measures have not performed to expectations or have been unable to deal with new threats to employers' property; (5) there is a natural and almost organic growth of video surveillance (ie "function creep").

---

[26] Ibid, p 11.

[27] Ibid, p 12.

[28] Ibid, p 13.

[29] This paragraph is a summary of the report at p 16.

Unique characteristics of video surveillance[30]*:* The Committee explained that, while initially it might seem that a surveillance camera in the workplace is little different to a pair of human eyes which might belong to a supervisor, video surveillance possesses a number of unique characteristics which distinguish it from traditional forms of workplace oversight:

- The conduct of surveillance is constant rather than casual or periodic;
- An extensive area can be surveyed quickly by video surveillance;
- It is possible to focus immediately and closely on a particular area or person through the zoom capacity of cameras;
- It is relatively cheap to install and to upgrade;
- Video surveillance is able to create a permanent and reproducible record of an event, while human visual surveillance is only able to create a memory; as a result, video cameras may be considered to be more reliable and consistent than a human being;
- Video camera evidence may be more persuasive in a court of law;
- Suspects whose illegal acts are filmed on camera may be far more likely to confess guilt than those whose acts were witnessed by people;
- Some video cameras may be able to film in conditions of virtually complete darkness;
- Video surveillance makes possible live viewing of activities in remote areas through electronic transmission.

Chapter 2 – Uses of video surveillance

Reasons for video surveillance in the workplace[31]*:* In summary, the report cited the following reasons for workplace video surveillance:

- Protection from the risks of internal and external theft
- Protection of premises from threats such as sabotage, arson and vandalism;
- Monitoring individual employee work performance (ie productivity);
- To improve customer service by observing peak periods and planning the allocation of staff throughout the day;
- To assist in staff training;
- To enhance health and safety standards;
- To ensure that employees comply with legal obligations;
- To protect employers from liability and unfair dismissal claims;
- To monitor production processes (including for machine malfunction);
- For a range of other purposes (eg investigation of compensation claims by employees – although this is often conducted outside the workplace);

[30] This paragraph is a summary of the report at p 21-22.

[31] This paragraph is a summary of the report at p 27-39 (see also p 2)

Chapter 3 - Privacy issues in video surveillance

Privacy concerns: The Committee summarised privacy concerns as follows:

> The widespread use of video surveillance in workplaces raises fundamental questions relating to the employee's right to privacy. The systematic observation of employees, regardless of any involvement in wrongdoing, is prima facie, privacy invasive, and has the potential to inhibit employees' privacy and to change the working environment.
>
> A reasonable respect for the human dignity of employees requires that employers should not use methods of surveillance which are excessively intrusive. Only information which is directly relevant to the employer's legitimate interests in the employee's work conduct and work output should be collected, and this should be done in the least intrusive manner possible. One of the main reasons for minimising the intrusiveness of surveillance raised by employees and unions is concern that personal behaviour and habits are sometimes embarrassing, and video recordings could be humiliating to an individual. There is also the potential for recordings to be compiled in such a way that they create a false impression as to actions or conduct…
>
> It is important for people to be able to preserve a distinction between their public and private worlds. The private world includes the employee's beliefs, personal habits and conduct relating to their own body…The constant conduct of video surveillance can weaken the dividing line between an individual's public and private worlds. During the course of a working day, employees might reasonably assume that their conduct is not being watched and may at particular times conduct themselves in a manner which is consistent with the private world…Conduct which is entirely normal in the individual's private context…can be acutely embarrassing in a public context…
>
> [In addition] [e]mployees may feel restricted and oppressed in an environment which is under constant surveillance. Their behaviour may be conditioned by a fear that any number of people may obtain a video recording and view their conduct. This can lead to higher stress levels, and may hinder innovation, creativity and useful communication between employees because of their fear that a supervisor reviewing a tape may see their interactions with other employees and assume that they are not using company time effectively.
>
> Employees' expectations of workplace privacy differs according to the nature of their occupation. Employees in occupations which involve regular contact with the public will have a reduced expectation of privacy while in contact with the public…On the other hand, in offices and many other workplaces, it is reasonable for employees to expect a greater level of privacy. A supervisor may oversee an employee's work and conduct at any time, but such surveillance is only random, employees are generally aware that a person is watching them, and the only "record" created is that of the supervisor's memory.
>
> It is sometimes argued that if an individual has a concern to protect their personal privacy, they must have "something to hide". It is implied that measures taken to protect personal privacy may give protection and legitimacy to illegal conduct and malpractice. The argument overlooks the fact that crime and other unlawful conduct is perpetrated by a very small number of people.
>
> The majority of law abiding people should not suffer a substantial invasion of privacy because of the actions of a small number of wrongdoers. Further, the argument fails to acknowledge that privacy is more than just a preference of an individual, but that it is also an internationally recognised human right. As such, it should not be necessary for employees to justify their desire to protect their privacy. Such a desire is a legitimate expression of the employee's expectation that they be treated with dignity and respect.
>
> ……

> Nevertheless, the right to privacy is not an absolute right, just as the right of employers to take measures to protect their business interests is not absolute. It is necessary to balance the interests of employers and employees in situations in which these interests compete. [32]

Data Protection Principles[33]*:* The Committee discussed how its ten Data Protection Principles (DPPs) might be applied to video surveillance in workplaces. Having regard to these principles, relevant issues would include: (1) whether the use of surveillance is fair; (2) the extent to which employees are informed in relation to the conduct of surveillance and its purposes; (3) whether the manner in which the information is collected and the extent of its use is relevant and not unreasonably intrusive; (4) Security of tape storage and length of time for which recordings are retained; (5) whether employees may have access to any retained recordings relating to them; (6) the rights of an employee to explain conduct recorded by a video camera; (7) whether using only part of the recording may create a misleading impression; (8) ensuring that employers do not use video surveillance for purposes beyond the original reasons of installation without the consent of employees; and (9) the circumstances in which video recordings may be disclosed to any third parties.

Complaints: [34] The Committee received 'an increasing number of complaints relating to workplace privacy, and in particular video surveillance. These complaints highlighted privacy invasion through covert surveillance, the use of surveillance for purposes beyond those for which it was originally installed, for monitoring employee work performance, and to harass an individual within an organisation….'

Effects of surveillance: [35] The Committee stated, 'It is clear from the complaints made to the Privacy Committee that employees believe that the use of video surveillance has a substantial impact on their working environment. When introduced without adequate justification, consultation and controls, video surveillance has the potential to undermine workplace morale and create distrust and suspicion between employees and their supervisors or management.' The Committee also noted that 'the conduct of constant video surveillance may also add to levels of stress and anxiety in the workplace…Some overseas studies have found that the overall impact of employment monitoring may be to decrease productivity because of these concerns.'

Locations of surveillance cameras[36]*:* Several submissions to the Inquiry 'discussed whether there should be a prohibition on the use of video surveillance in particular areas of the workplace. Such a prohibition would reflect the fact that there are some areas where employees have a greater expectation of personal privacy.' The areas which were most sensitive were toilets, showers and change rooms; while other sensitive areas

---

[32] Ibid, p 40-42.

[33] This paragraph is a summary of the report at p 2-3, and p 43-46.

[34] This paragraph is taken from the report at p 3. See p 46-51.

[35] This paragraph is taken from the report at p 51-52.

[36] This paragraph is taken from the report at p 54-56.

included meal and recreation rooms. Some employers opposed a general ban on video surveillance in these areas, arguing that there were exceptions which would justify surveillance in such parts of the workplace. They submitted that this issue should be resolved through guidelines or negotiation between employers and employees.

Chapter 4 - Covert video surveillance

Justifications for covert video surveillance: The justifications for covert video surveillance in the workplace are summarised as follows:

> The first and most general argument is that employers have an absolute and overriding right to protect their fixed property, assets and employees, and that covert surveillance is an effective means of achieving such protection. While acknowledging that it may be preferable to conduct surveillance overtly, employer groups have argued that there are situations in which covert surveillance may be more effective. It is claimed that overt video cameras, company procedures, management supervision and the presence of security staff, are not always effective in resolving security problems.
> …
> A second argument in favour of covert surveillance is that it can be a far more affordable option than overt surveillance. If cameras are placed in the areas where theft is known to be taking place, it is unlikely to be necessary to install a large number of cameras to identify a thief. If only overt cameras are used, it might otherwise be thought necessary to cover every vulnerable part of the workplace with surveillance. This would also put a much larger number of employees under surveillance.
>
> A third argument for covert surveillance raised by security consultants is that some employers who are concerned about 'turning the workplace into a prison' and about industrial action resulting from the open display of cameras have elected to use covert cameras. It is a strategy that risks much greater conflict for the sake of avoiding a smaller one.
> …
> A fourth argument raised by employers is that covert surveillance can be used strategically in an area where a security problem exists, to identify the individual responsible. If overt video surveillance was introduced, it is likely that the individual would shift their activities elsewhere, outside of the camera's gaze. A submission from a security consultancy highlights the related argument that if covert surveillance was prohibited, a more extensive installation of overt surveillance cameras might become necessary. [37]

Controls on covert surveillance[38]*:* The Committee notes that unions and civil liberties groups submitted that covert surveillance should be prohibited – one point they made is that overt surveillance could achieve the same outcomes. Employer groups, on the other hand, argued that they should have the right to use covert surveillance in situations where other security methods did not prove effective. In their view, covert surveillance should be controlled through self-regulation. The Committee expressed its view that:

> …covert surveillance cannot be justified simply because it may be more effective than overt surveillance in certain circumstances. Many of the arguments presented…to justify the use of covert surveillance are ultimately based on a pragmatic assessment of the employer's interests. The weakness in these arguments is that they fail to take into account the importance of privacy

[37] Ibid, p 58-59.

[38] This section is based on the report at p 60-63.

> as a fundamental human right. The breach of personal privacy involved in covert video surveillance is of the utmost seriousness, and requires a very high degree of justification.

In the Committee's view, self-regulation would not be adequate. The Committee stated that, 'the strongest privacy protection would be a prohibition of all covert surveillance except for that conducted by law enforcement officers. However, resource constraints including the limited number of surveillance cameras, limit the capacity of police to respond to every case where criminal activity is suspected.' The issue to be considered was 'whether it is possible to introduce a level of control on covert surveillance which finds an appropriate balance between the interests of employers, customers and employees.' The Committee outlined what, in its view, were the minimum requirements of a policy on covert surveillance. In brief, 'any policy on covert surveillance must make [covert surveillance] a last resort for exceptional problems when other security methods have been ineffective. It should be used only for a specific identified risk, in a limited area for a specific time period, under strict controls.'[39]

Chapter 5 - Regulation

The Committee summarised its discussion of regulation in Australia and overseas:

> Although regulation on video surveillance in workplaces in industrialised nations is still taking shape, many countries have already imposed some limitations on its use. Constitutional provisions, statutes and court rulings reflect a belief that video surveillance in the workplace is a threat to employees' rights to privacy, dignity and personal autonomy. The two main areas in which video surveillance has been regulated relate to covert surveillance and the use of surveillance for monitoring individual employee work practices. The sources of these protections have been the application of broad constitutional, common law or code recognition of fundamental human rights; privacy and data protection legislation; industrial relations legislation; and in one nation, a specific law relating to video surveillance.
>
> A comparison between Australia's existing regulation of video surveillance in the workplace with the protections afforded in other countries highlights the weaknesses in Australian law. There are no effective controls on the covert use of video surveillance, nor on the use of surveillance for workplace monitoring…[40]

Chapter 6 - Future options

The Privacy Committee raised various options for reform, as outlined below:[41]

OPTION	IMPLEMENTATION
1. No change to existing non-regulatory situation	Rely on ethical conduct of employers and pressure of employees, unions and public opinion considerations
2. Self-regulation	2.1 A single code on video surveillance to cover all industries 2.2 Many codes for separate sectors and industries

[39] Ibid, p 4. See minimum requirements on p 63-64.

[40] Ibid, p 93-94.

[41] Ibid, p 95.

3. Co-regulation	3.1 Privacy Committee Guidelines 3.2 Workplace Codes developed in the industrial relations context
4. Legislative control	4.1 Mandatory Code, pursuant to privacy and data protection legislation 4.2 Mandatory Code, pursuant to industrial relations legislation 4.3 Amendments to industrial relations legislation to prohibit certain practices, backed up by either mandatory or voluntary Codes; 4.4 Specific legislation; 4.5 Licensing

The Committee discussed the strengths and weaknesses of each option.[42] As to the first option, the main arguments against any action were that:

- any form of regulation will impose a cost on business which will reduce the competitiveness of New South Wales businesses;
- the extent of problems with video surveillance have been exaggerated, and any form of legislated response would be disproportionate to the problem, and
- to the extent that there are problems with the use of video surveillance in the workplace, these problems can be solved in the appropriate forums of industrial relations and the development of Codes of Conduct in industry groups.[43]

However, the Committee was of the view that 'there is strong justification for measures to be taken to protect the privacy of employees from the unrestricted use of video surveillance in the workplace. The Committee believes that the manner in which video surveillance is being introduced into workplaces is unsatisfactory and is inconsistent with a democratic society which values privacy and the dignity of individuals.'[44] The Committee noted that problems relating to video surveillance were likely to grow in the future and that industrial disputes might continue to arise. The Committee believed that 'an appropriate level of regulation will not impose unreasonable costs on employers.'[45]

Recommendations: Ultimately, the Committee recommended a layered approach, which would prohibit some uses of surveillance and establish a general policy framework for the legitimate use of surveillance.[46] The first layer (consistent with option 4.3) would involve amendments to the *Industrial Relations Act 1991(NSW)* to:

(a) Prohibit video surveillance for monitoring employee work performance;
(b) Prohibit video surveillance in certain areas such as toilets and change rooms;
(c) Require a permit from the Industrial Relations Court for:
    - The use of surveillance in locker rooms and employee recreation rooms;
    - Any use of covert surveillance in the workplace, including a requirement of compliance with strict guidelines relating to its operation. [47]

[42] See report at p 98-111 and at p 6-7 (Executive Summary).

[43] Ibid, p 96.

[44] Ibid, p 96.

[45] Ibid, p 97.

[46] Ibid, p 112.

[47] Ibid, p 114.

The second layer (consistent with option 4.1) would involve the enactment of privacy legislation and the development of a Code of Conduct:

> Privacy legislation should be enacted to establish the Office of the Privacy Commissioner of NSW, to oversee the application of the Data Protection Principles to the public and private sectors. The legislation would include provisions for the Commissioner to develop Codes of Conduct in consultation with industry. The Commissioner would have powers to receive complaints, and to investigate and report on breaches of the Data Protection Principles or Codes of Conduct. A Code of Conduct on video surveillance could be developed, perhaps based on the attached Guidelines, and after any necessary modifications the Privacy Commissioner could enact the Code, making it enforceable. The Commissioner could grant exceptions from the Code for particular activities or workplaces.[48]

3.5 Working Party's report

As outlined in the second reading speech, a Working Party report was published in December 1996, which formed the basis for the legislation.[49] The Working Party's recommendations did not go as far as the Privacy Committee's recommendations; and the Working Party recommended changes to the *Listening Devices Act 1984* rather than to the *Industrial Relations Act*. The former Act would be amended to include:

- Prohibitions on the use of *covert* video surveillance (i) for monitoring work performance; and (ii) in areas such as toilets, change-rooms and showers.

- If selected, a system for prior judicial authorisation for the use of covert video surveillance whereby applicants must obtain a permit from a Magistrate in the Local Court.

- Video surveillance would be covert if conducted without prior notice to employees, or with cameras that are not clearly visible, or in the absence of signs notifying employees of the fact of surveillance.[50]

- A prohibition on the use of video tape recordings (whether as a result of covert or overt surveillance) for illicit or unconscionable purposes.

---

[48] Ibid, p 115.

[49] See NSW Department of Industrial Relations, *The Working Party on Video Surveillance in the Workplace: Report to the Hon J W Shaw QC MLC Attorney General and Minister for Industrial Relations*, December 1996. The working party comprised representatives from the following organisations: the Australian Liquor, Hospitality and Miscellaneous Workers Union, the Labor Council of New South Wales, the National Union of Workers, the Employers Federation of New South Wales, the Australian Chamber of Manufactures, New South Wales Branch, the Retail Traders Association of New South Wales, the Registered Clubs Association of New South Wales, the Public Employment Office, the Privacy Committee of New South Wales, the Attorney General's Department, and the Department of Industrial Relations.

[50] Ibid, p 3.

The Working Party also recommended that employers adopt a *voluntary* Code of Practice on the use of overt video surveillance in the workplace.

Opposition: The Working Party report was a majority report, which was not endorsed by the Employers' Federation of NSW. The Federation opposed the regulation of covert video surveillance by legislative means and argued that the Privacy Committee's report failed to give 'reasonable weight to the considerable difficulties faced by business.'[51] The Federation submitted that regulation on the use of video surveillance was not justified but conceded that 'there may be a need to regulate *the viewing and distribution of video tape footage* to ensure it is only used for limited purposes.'[52] Other employer bodies such as the Retail Traders' Association of NSW and Registered Clubs Association of NSW also opposed the introduction of legislation.[53]

3.6 The Workplace Video Surveillance Act 1998

The *Workplace Video Surveillance Act 1998 (NSW)* came into effect on 31 July 1998. In addition, a non-binding *Code of Practice for the use of Overt Video Surveillance in the Workplace* was adopted by a number of the members of the Working Party.[54] The Act was to be reviewed after a period of five years.[55]

[51] Ibid, p 11.

[52] Ibid, p 11 (original emphasis).

[53] Ibid, p 14.

[54] The Code appears on the website of Privacy NSW: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_wvsact#5

[55] *Workplace Video Surveillance Act 1998,* s 30.

4. COMPUTER SURVEILLANCE OF EMPLOYEES

4.1 Introduction

The draft Bill defines "computer surveillance" as 'the monitoring or recording by means of software or other equipment of the information input or output, or other use, of a computer used by the employee (including, but not limited to, the sending and receipt of emails and the accessing of Internet websites).'[56] The draft Bill would also regulate the blocking of employees' emails and the blocking of employees' access to internet websites. Since blocking is undertaken for similar reasons to monitoring, it is convenient to deal with both in this section of the paper although the focus will be on monitoring, which is the most controversial issue. Use of the term "computer surveillance" in this section will refer to both "monitoring" and "blocking".

4.2 Growth in business use of computers, internet and email

The number of Australian businesses using computers, the internet and email has grown rapidly over the past decade. According to the Australian Bureau of Statistics (ABS), as at June 2003, 83 percent of Australian businesses used computers, compared with 49 percent in June 1994.[57] Most of the businesses that did not use computers were small businesses with less than five employees.[58] In the period from June 1998 to June 2003, the proportion of businesses with internet access grew from 29 percent to 71 percent (91 percent for businesses with between 20 and 99 employees).[59] ABS does not report on the use of Internet or email by employees but a study on the 'Internet Economy and Australian businesses in 2002' by the Allen Consulting Group found that 74 percent of the Australian businesses surveyed provided more than half of their staff with access to email.[60] In its 2001 *Interim Report on Surveillance* the NSW Law Reform Commission commented, 'the rise of the internet and the boom in email traffic over the past decade has been something of a communications revolution, particularly in the workplace.'[61]

---

[56] Draft Bill, clause 3.

[57] Australian Bureau of Statistics, *Measures of a knowledge-based economy and society, Australia: Information and Communications Technology Indicators*, 2003. On ABS website at http://www.abs.gov.au/Ausstats/abs@.nsf/94713ad445ff1425ca25682000192af2/c642f3b7dfe50b7eca256d97002c8647!OpenDocument

[58] Ibid.

[59] Ibid.

[60] The Allen Consulting Group and Cisco Systems, *Built for Business II: Beyond Basic Connectivity; The Internet Economy and Australian Businesses in 2002,* October 2002.

[61] New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report 98, February 2001 at p 60 (para 2.43).

4.3 Reasons for computer surveillance

While the use of email and internet can bring benefits to an organisation[62], they can also pose several problems. Computer surveillance is undertaken to address these problems, as well as for other reasons, as outlined below.

4.3.1 Preventing excessive personal use of computers

Employers want to ensure that employees are not wasting time by using their computers for recreational or other personal purposes when they should be working – in particular, by surfing the internet and sending personal emails. Without electronic monitoring, what has become known as "cyber-bludging" can be difficult for employers to detect. An article in the Sydney Morning Herald in 2003 states:

> It's never been easier to put in a hard day at the office without actually getting any work done. By the time you check your email, swap instant messages, play a few games and watch the latest movie trailers, there's hardly any time left for reading Dilbert, scanning the news headlines and taking a few online surveys…Cyber-bludging was always going to take off among a people who consider bludging a national pastime but are quick to embrace new technologies.[63]

Surveys have been conducted to quantify the extent of personal use of emails and Internet at work. These surveys have mostly been carried out by companies that sell computer monitoring software – mainly in the US.[64] These software companies have also estimated the cost to businesses from diminished productivity. For example, in its July 2000 *Cyberbludging Report,* SurfControl estimated that non-work related internet use cost Australian businesses $300 million a year.[65]

4.3.2 Preventing bandwidth drain resulting from personal use of computers

Recreational use of the internet at work by employees 'can also have a devastating effect on a company's bandwidth. Employees who download music, pay bills online, play games or just browse the web impede the work-related activity of colleagues. The bandwidth problem becomes acute during periods of personal emailing peaks at work. Servers often crash on Valentine's Day and around Christmas…SurfControl's Charles Heunemann says: "One person watching a live feed would drain more than 50% of the

---

[62] See report by Allens Consulting Group and Cisco Systems, supra, p 22ff.

[63] 'Time Bandits', *Sydney Morning Herald*, 26/8/03.

[64] For example, see: Websense, *Web@Work Survey Results 2004*; and American Management Association, *2004 Workplace E-mail and Instant Messaging Survey Summary* (and similar surveys for previous years); and Webspy, *Internet Use Statistics* located at http://www.webspy.com. See also reports of surveys in the media: eg, 'Behind the Scenes, *Sydney Morning Herald,* 15/5/04; 'Sex, lies and office email', *Ninemsn,* 24/4/02; 'Email snooping almost banned', *Sydney Morning Herald,* 26/6/01.

[65] 'Snooping on the job', *The Bulletin,* 19/2/03.

bandwidth of most small to medium enterprises. Larger organisations…could have it clogged if just 10 people logged on to a live feed simultaneously.'"[66]

4.3.3 Avoiding legal liability

It has been suggested that inappropriate use of email and Internet by an employee may expose an employer to liability from claims by other employees in relation to sexual harassment, or discrimination. Sexual harassment claims may arise from pornographic web-browsing by an employee or from emails sent by an employee to another containing pornography or other sexually explicit material or offensive jokes.[67] Similarly, discrimination claims may arise if an employee circulates by email racially offensive material or jokes.[68] Employers might also be liable if they fail to protect employees from 'bullying and intimidation or other forms of harassment…that may adversely affect an employee's health and safety in the workplace.'[69] Aside from any liability issues, such conduct can be disruptive to the workplace environment.

It has also been suggested that employers may become liable for defamatory emails that are sent by an employee via the company's email system.[70] In addition, employers could become liable for copyright infringement by employees. Paterson states, 'the issue of copyright infringement is an important one given the ease with which it is possible for employees to make digital copies not only of text, but also of graphics, software, audios and videos, and also to republish this information to others…[T]here is a real risk that copyright owners will seek redress against businesses whose computer systems are detected as engaging in infringing activities.'[71]

---

[66] 'Sex, lies and office email', *Ninemsn online,* 24/4/02. See also 'Email snooping almost banned', *Sydney Morning Herald,* 26/6/01 (third column); and 'Internet spies watching you "in real time"', *Daily Telegraph,* 30/8/01.

[67] Paterson M, 'Monitoring of Employee Emails and Other Electronic Communications' (2002) 21(1) *University of Tasmania Law Review* 1 at 6. A report of a case in the US states, 'the world's most expensive email is "25 reasons why beer is better than women"…It cost the US resources company, Chevron, US$2.2 million in a 1995 harassment settlement.' Cited in 'Sex, lies and office email', *Ninemsn*, 244/02.

[68] Ibid, p 6. For example, in the US a $70 million claim was made against the brokerage firm Morgan Stanley for racist jokes that appeared on the company's e-mail system. See Geist M, *Computer and E-mail Workplace Surveillance in Canda: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance,* March 2002 at p 7.

[69] Australian Business Industrial, *Submission on Exposure Draft Workplace Surveillance Bill 2004,* 2004, p 9-10.

[70] Paterson, supra, p 4-5. In the UK, Western Provident Association brought libel proceedings against Norwich Union 'following the appearance of messages on Norwich Union's internal email system falsely suggesting that Western Provident was in financial difficulty. The case was settled with Norwich Union paying $450,000 and making a public apology.' See NSWLRC Interim Report, Note 61, p 118-19.

[71] Paterson, ibid, p 4-5.

Other ways in which businesses could incur liability through employee computer use include breaches of privacy legislation, eg improper employee disclosure of customer information by email; and breaches of new federal legislation, which regulates the sending of "spam" messages (ie unsolicited commercial electronic messages).[72] In addition, businesses may be concerned about employees using computers for criminal activity such as accessing, and downloading, child pornography on the internet.

4.3.4 Preventing actions that may otherwise harm employer: eg leaking secrets

Employers also undertake computer surveillance to minimise the risk of employees viewing, taking or leaking (intentionally or unintentionally) confidential information or trade secrets to third parties, including competitors.[73] In other words, to guard against the risk of employees violating the employer's privacy.[74] Other ways in which employee' computer use has the potential to harm their employer include defrauding the business of funds and posting on the internet, or circulating by email, views or information that are damaging to the reputation of the business.[75]

4.3.5 Protecting security of computer system from external threats

According to Paterson, 'security threats may arise from breaches of security protocols and from the introduction of computer worms and viruses…[T]he integrity of computer systems…may be threatened by the activities of hackers, criminals and disgruntled employees. The risks posed by breaches of security range from the possibility of damage to, or alteration of, important data or systems, theft of trade secrets, fraud and breaches of privacy obligations.'[76] For example, emails to employees may contain viruses and employees may unintentionally download Trojan horse programs[77], both of which can adversely impact on the operation of the computer system.

4.3.6 Blocking Spam e-mails

Employers block Spam emails, which have been sent to employees and which, amongst other things, can waste employees' time and reduce productivity.

---

[72] See for example, 'Legislation sending mixed messages', *Australian Financial Review,* 19/3/04; and 'Want to check my email? See you in court, boss', *Australian Financial Review,* 8/5/04. For more detailed information on the *Spam Act 2003* see the Australian Government Information Office website: http://www.noie.gov.au/

[73] See Paterson, Note 67, p 4 and Geist, Note 68, p 8-9.

[74] Hartman L.P, 'The Economic and Ethical Implications of New Technology on Privacy in the Workplace', (1998) 102 *Business and Society Review* 1 at 11.

[75] Schulman A, 'Computer and internet surveillance in the workplace', (2001, July) 8(3) *Privacy Law and Policy Reporter* 49 at 54.

[76] Paterson, Note 67, p 7.

[77] Schulman, supra, p 54.

4.3.7 Performance monitoring and quality assurance

Computer surveillance may be used to monitor 'the performance of employees, such as data entry operators, who spend the majority of their work time on a computer.'[78] Software can track 'the number of keystrokes per minute, error rate, time taken to complete each task and time spent away from the computer.'[79] In addition, employers may monitor emails of employees for quality assurance and training purposes, in the same way that they monitor telephone calls of employees in customer service roles.[80]

4.4 An explanation of computer surveillance

This section will focus on monitoring and blocking of emails and internet usage although computer surveillance can also involve review of computer files on an employee's hard drive and monitoring of other computer usage.[81] Keystroke monitoring has also been mentioned above as a method of performance monitoring.

4.4.1 Nature of emails

The Federal Privacy Commissioner makes the following points about email.[82] First, that 'email is often compared to a postcard in that anyone who receives it can read it. E-mail may also be read if it is stored on servers during transmission.' Second, 'system administrators are…capable of reading the contents of e-mails sent and received by the corporate network.' Third, 'many people think that if they delete their e-mail it is gone forever. This is not so as most electronic documents are backed up and recoverable.'

4.4.2 Routine logging of employee emails and internet usage

The Commissioner also states, 'most software used to operate networks, including web servers, mail servers and gateways, logs transactions and communications. These logs will normally include the e-mail addresses of senders and recipients of e-mail at the time of transmission. The content of e-mails themselves would not normally be logged but may be stored on mail servers. Similarly, web server logs record information on the sites that people visit. The keeping of these logs is usually necessary for the routine maintenance and management of networks and systems.'[83]

---

[78] NSWLRC Interim Report, Note 61, p 285.

[79] Ibid.

[80] Schulman, Note 75, p 54.

[81] See, for example, Lane III F.S, *The Naked Employee: How Technology is Compromising Workplace Privacy,* Amacom, United States, 2003, p 130ff.

[82] Office of the Federal Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy (30/3/2000)* at p 2.

[83] Ibid.

4.4.3 Software for monitoring employees' emails and internet usage

Software companies have 'quickly filled the marketplace with dozens of different products that offer employers the opportunity to easily monitor their employees' computer habits.'[84] The low cost of such products have made them attractive.[85] Geist states, '…each [product] can generate customisable reports that disclose how employees use their computers. For example, most products will monitor Internet activities such as how frequently employees spend time surfing the World Wide Web along with which sites they visit. Most products can also provide detailed reports about e-mail activity including the frequency of incoming and outgoing email messages, as well as what email messages employees drafted but chose to delete prior to sending.'[86]

Schulman discusses different types of reporting by different products.[87] First, some products by default make a log record of everything they see, while also highlighting or raising an alert for violations such as accessing an 'inappropriate' website. Other products only record infractions, or at least have this as their default behaviour. Second, logs may be tied to specific employees (eg Joe made five visits to playboy.com), or the employer may only keep aggregate statistics (eg we had 10 visits to playboy.com last month). Similarly, records may include details such as complete website addresses (Joe visited these specific pages at playboy.com) or they may provide an aggregate per individual (Joe spent a total of 30 minutes at a site on our prohibited list).

4.4.4 Software for blocking delivery of emails and access to websites

Employers 'use filtering or blocking technologies to prevent workers accessing particular types of material on the internet. For example, an employer may block access to pornographic websites or may prevent workers accessing websites containing particular words or phrases. Employers may also block spam, as well as email messages of certain sizes or types.'[88] One of the leading products works 'by intercepting Web page requests from each browser and comparing the website address to the addresses listed in a database of over 3.5 million websites. The websites contained in the database are organised into thirty one categories; companies that install the software can choose which categories of sites the software should block.'[89] Categories include, for example, adult material, drugs, gambling, racism as well as entertainment, shopping and job search sites.[90] Many products not only block access to a site or an email but also make a

[84] Geist, Note 68, p 10.

[85] See Schulman, Note 75, p 54-55.

[86] Geist, supra, p 10.

[87] The following is taken from Schulman, supra, p 51-52.

[88] Victorian Law Reform Commission, *Workplace Privacy: Options Paper,* 2004, p 25.

[89] Lane, Note 81, p 145.

[90] Ibid.

record of the attempted access.[91] Note, while monitoring and blocking software have been discussed separately above, many products perform both functions.

4.4.5 Software that allows for more extensive computer monitoring[92]

The programs that are most commonly used to monitor email and internet activity are *server-based* programs, which are installed on the employer's computer network. These programs can only monitor activities that occur on the network such as internet browsing, emails (including emails sent from web-based email accounts like Hotmail) and instant messaging. Schulman notes some limitations of these products from a surveillance perspective. These programs 'can't catch [employees] viewing porn that they've already downloaded to their computer, nor can it see how much time they waste playing games off a CD ROM…nor could it see them copy company secrets onto a floppy disk, or polish their resume in Word.' Such activities can be monitored with the use of *PC-based* programs that are installed directly on an employee's computer and can monitor computer activity whether or not the user is connected to the network.

Schulman gives some examples of these programs. One product 'records the names of programs run, the titles of windows that are open on a computer, and – most significantly – the keystrokes typed, including ones that you subsequently deleted.' Another product, 'in addition to capturing keystrokes and logging programs run and websites visited…can capture 'screenshots' (that is, graphic images of the entire computer screen) at specified intervals (down to once per minute) and then email them out for remote viewing. The screenshots can then be "played back" on another computer to see what the employee was doing, literally every minute of the day.' According to Schulman, these PC-based programs 'demonstrated what was technically possible with employee monitoring software [but] such programs were not in widespread use.'

4.4.6 Who in an organisation conducts email and internet monitoring?

The Victorian Law Reform Commission states, 'email an internet monitoring activities are generally carried out in larger organisations by IT professionals, usually a network administrator. Network administrators and other IT professionals require a high degree of access to organisations' computer systems to effectively manage the systems.'[93]

4.5 The extent of computer surveillance

4.5.1 In Australia and New South Wales

The extent of computer surveillance in the workplace in Australia and NSW is not entirely clear. The law firm Freehills conducted a survey on email monitoring in the year 2000, which received responses from 67 of Australia's top 200 companies.[94] It found that 76

[91] Schulman, Note 75, p 51.

[92] The information in this section is taken from Schulman at 56 –57.

[93] VLRC Options Paper, Note 88, p 25.

[94] Freehill Hollingdale & Page, *Internet Privacy Survey Report*, 2000, available on Freehills'

percent of respondents periodically monitored employees' email content – mostly for systems maintenance and trouble shooting purposes or where email abuse was suspected – and five percent of respondents monitored email on a routine basis.[95]

It is also relevant to note the results of a survey in January 2004 of around 100 businesses by the NSW State Chamber of Commerce and Unisys. The survey found that of the respondents that had a policy on employee use of IT facilities (eg internet, email, mobile phones), only 16 percent said they used page blocking or other forms of technology to regulate compliance; almost 40 percent said they relied on managers to monitor misuse; and 32 percent of respondents had no clear method of policy enforcement.[96] The survey report does not state what percentage of respondents actually had such a policy.

4.5.2 In the United States

More surveys of computer surveillance have been conducted in the US. A 2001 *Electronic Policies and Practices Survey* by the American Management Association (AMA) found:[97]

- Monitoring internet connections – 63 percent of respondents did this in 2001 (up from 54 percent in 2000);
- Blocking connections to unauthorised or inappropriate websites – 40 percent of respondents did this in 2001 (up from 29 percent in 2000);
- Storage and review of email messages – 47 percent of respondents did this in 2001 (up from 15 percent in 1997);
- Storage and review of computer files – 36 percent of respondents did this in 2001 (up from 13 percent in 1997);
- Monitoring computer use (time logged on, keystroke counts etc) – 19 percent of respondents did this in 2001 (up from 16 percent in 1997).

According to Schulman, 'a closer look at the AMA report reveals that "most respondent firms carry on surveillance practices on an occasional basis in the manner of spot checks rather than constantly or on a regular routine." Systematic, constant or routine monitoring is usually what the word "monitoring" evokes.'[98] The results of a 2004

---

website: <http://www.freehills.com.au>. The information about the scope of the survey is not contained in the survey report but was obtained by the writer in a private communication with a representative of Freehills. What the survey report says about the scope of the survey is, "some of Australia's leading companies completed this survey. Survey respondents were from a cross-section of industry sectors with 48% of respondents being from the telecommunications/information technology and banking and financing sectors."

[95] Ibid, p 9. Note 19% did not monitor emails and 5% had no policy on the issue (p 9).

[96] State Chamber of Commerce (NSW) and Unisys, *Getting a Grip on the Internet: Information Technology Survey,* Industry Leaders Series #1, p 10. Note that the figures in the table on p 10 differ from the figures that appear in the commentary that appears above the table. A representative from the Chamber of Commerce informed the writer that the figures in the commentary were the correct figures.

[97] These are the AMA results as reported in Schulman, Note 75, p 49.

[98] Schulman, ibid, p 50.

survey by the AMA on email monitoring were that 60 percent of respondents used software to monitor external email (in 2003, 51% monitored incoming emails, and 39% monitored outgoing emails); and 27 percent of respondents used software to monitor internal email between employees (19% in 2003).[99]

4.5.3 In the United Kingdom

United Kingdom: KPMG conducted 'a small survey in late 2000 and found that around 50 per cent of the surveyed companies monitor internet use "infrequently", around 20 per cent monitor on a monthly basis, and only 11 per cent monitor on a daily basis.'[100] Also, an *Information Security Breaches Survey 2004*, sponsored by the UK Department of Trade and Industry, and conducted by Price Waterhouse Coopers, found that 20% of businesses (55% of large businesses) logged and monitored which websites staff accessed and 15% of businesses (50% of large businesses) blocked access to inappropriate websites.[101]

4.6 Employee awareness of computer monitoring

4.6.1 Employees have made incorrect assumptions about privacy of computer usage

In a 2002 article, Paterson stated, 'employees are largely unaware of the imperatives for monitoring and usually abysmally ignorant about the prevalence, ease and scope of monitoring.'[102] Paterson points out that employees have made incorrect assumptions about the ability of employers to monitor their computer usage. One such assumption is that the use of passwords would protect the privacy of their computer use, including their email messages.[103] Another assumption is that electronic documents disappear once they have been deleted.[104] Employees may also have assumed that employers would respect their privacy in e-mails and internet use in the same way as their telephone calls; and/or that it would be unlawful for employers to do otherwise.

---

[99] Several other US surveys have been conducted. For example, a *Government Technology* article on 27 August 2004 reports, 'a July 2004 survey by Forrester Consulting showed 48 percent of large U.S. companies regularly read outgoing e-mail sent by employees.' An article in the *Sydney Morning Herald* on 15/5/4 entitled 'Behind the Scenes' reports that 'a US study looking at the monitoring practices of nearly 200 companies found that 26 percent of managers monitored employees' online activities all the time, not just when something gave them a reason to investigate.' See also Schulman, Note 75, p 50-51.

[100] Schulman, Note 75, p 51.

[101] Price Waterhouse Coopers on behalf of UK Department of Trade and Industry, *Information security breaches survey 2004*. See Figure 66. Available online http://www.dti.gov.uk/industries/information_security/downloads.htmlne

[102] Paterson, Note 67, p 9.

[103] Ibid at 9.

[104] Ibid.

4.6.2 To what extent have employees been notified of monitoring?

The extent to which employers in Australia have notified (or now notify) employees of computer monitoring is not entirely clear. The Freehills survey (2000), referred to above, found that 65% of the companies that monitored employees' email did so without notifying their staff or customers.[105] Other surveys referred to above do not adequately address this question. Some of those surveys report on the percentage of respondents that had written policies on acceptable usage of internet and emails.[106] However, it is not clear whether such policies notified employees about monitoring or whether employers had communicated such policies to employees. It is likely that notification has increased following the issue in March 2000 of *Guidelines on Workplace E-mail, Web-browsing and Privacy* by the Federal Privacy Commissioner and with growing publicity of the issue.[107]

4.7 Privacy issues relating to computer monitoring

4.7.1 Introduction

Like other forms of workplace surveillance, computer monitoring[108] intrudes on employees' privacy. As may be evident from the above, the impact which computer monitoring has on employees' privacy may depend on the type of monitoring that is conducted. For example, computer monitoring will be more privacy invasive if it is covert as distinct from notified; if it is constant as opposed to infrequent; if it is indiscriminate rather than targeted; and if it involves reading the content of emails and websites visited instead of merely monitoring email traffic data and time spent on the internet. While this section focuses on privacy issues associated with the collection of information through computer monitoring it is important to note that privacy concerns also arise in relation to the use, storage, and disclosure of such information by the employer.

4.7.2 Privacy issues in the context of covert computer monitoring

Covert computer monitoring, in particular, can result in employers monitoring and recording their employees 'engaging in very personal and private behaviour of the type that they would not ordinarily choose to reveal.'[109] In relation to email monitoring, Paterson states, 'while it might be expected that people would exercise more caution when using a work computer, email is far closer to speech than written communication,

[105] Freehills survey, Note 94, p 9.

[106] For example the AMA survey (2001) reported that 81% of respondents had a written policy on acceptable email usage and 77% had a written policy on acceptable internet usage.

[107] As to the Privacy Commissioner's Guidelines, see below at paragraph 6.4.2.

[108] This section focuses on *monitoring* of employees' computer usage (including emails and internet) as distinct from *blocking* of employees' emails and access to internet sites. Blocking, of itself, does not raise privacy issues but raises other issues such as employee autonomy.

[109] Paterson, Note 67, p 10.

and typically lacks the care given to written communication. Its informality, coupled with its ease of use, may result in a greater level of candour about personal matters than would occur in the context of a written letter.'[110] The National Workrights Institute in the US outlines privacy concerns, as follows:

> …employer's efforts to prevent abuse often lead to serious invasions of privacy. People are not robots. They discuss the weather, sports, their families, and many other matters unrelated to their jobs while at work. While many of these non-work related conversations are innocuous, some are highly personal...In today's world, these "discussions" may well take place over e-mail or the office telephone. An employer who monitors for legitimate reasons may well inadvertently "eavesdrop" on such a sensitive private conversation.
>
> These problems are compounded by the disappearing wall between the world of work and our home lives. Not long ago, work was done in the office and home was for private life. But this world is rapidly disappearing…When work and home become a seamless whole, not only does work come home, but personal matters come to work…As personal communication from the workplace increases, so does the risk that employer monitoring programs will capture private messages in which the employer has no legitimate interest.[111]

The types of personal information about an employee that can be captured monitoring emails and internet browsing includes, for example, information about relationships, sexual orientation, financial state, physical and mental health problems, drug or alcohol problems and political views.[112] Emails may also contain criticism or gossip about work colleagues and superiors and discussions about industrial matters.[113]

Paterson argues that 'systematic covert surveillance amounts to a gross infringement of informational privacy – the right of individuals to control how much of their personal lives they wish to share with others.'[114] According to Paterson, loss of informational privacy is problematic 'because of its adverse impact on personal autonomy, integrity and dignity, and consequently on our development of individuals, as well as on our relationships with others. These values may be summed up as being largely concerned with "achieving individual goals of self-realization".'[115] In addition, Paterson states:

---

[110] Ibid, p 10.

[111] US House of Representatives, Subcommittee on the Constitution of the House Committee on the Judiciary, Legislative Hearing on H.R 4908, the "Notice of Electronic Monitoring Act", Testimony of Lewis L. Maltby, President- National Workrights Institute, 6 September 2000.

[112] Victorian Law Reform Commission, *Privacy Law: Options for Reform* (2001) at 48 cited in Paterson, supra, p 10.

[113] See Nolan J, 'Employee privacy in the electronic workplace Pt 1: surveillance, records and emails' (2000, November) 7(6) *Privacy Law and Policy Reporter* 105 at 108. Note also a case in which two council workers were dismissed from Narrabri Shire Council in November 1999 for referring to their superiors as Huey, Dewey and Louie in office email: see 'Govt acts on e-mail at work', *Illawara Mercury,* 17/5/00.

[114] Paterson, Note 67, p 10-11.

[115] Ibid, p 11. For a more in-depth discussion of the concept of privacy and the values of dignity and autonomy see, for example, Victorian Law Reform Commission, *Defining Privacy,* Occasional Paper, 2002.

> The need for control over personal information has been further explained in terms of its relationship to personal identity. Data surveillance creates records containing isolated pieces of information that are used for making decisions about individuals. Rosen suggests that the growing unease about information surveillance results from justifiable unease about the tendency to view people as the sum of the discrete data held about them…[116]

Paterson also argues that loss of informational privacy makes 'an individual more vulnerable to discrimination and exploitation by others.'[117] She explains:

> Anti-discrimination legislation outlaws the discriminatory use of information relating to issues such as race, disability and sexuality for the purposes of employment-related decisions. However, persons who are discriminated against in employment and other contexts may have no means of knowing, let alone proving, that particular information has been used as a basis for unlawful discrimination.[118]

The Australian Privacy Foundation has also raised concerns about the potential for discrimination. It says that email and internet surveillance could 'be abused if an employer has a grudge against a worker and decides they want to go fishing [for information] to find something they have done wrong in order to have grounds to sack them.'[119]

4.7.3 Privacy issues in the context of overt computer monitoring

Computer monitoring that has been notified to employees still intrudes upon their privacy. However, as Paterson states, 'the employee has greater potential to control the degree to which he or she exposes aspects of his or herself to the employer.'[120] The extent to which this statement is true will depend on the nature of the notice given to employees.

Two of the primary values that underpin, or are associated with, the right to privacy are "autonomy" and "dignity".[121] The former is 'often said to mean people's ability to make their own choices and control their own destinies'[122]; while the latter 'is often invoked to justify the idea that human beings should not be treated as if they are things, that is, that they should not be commodified.'[123] To the extent that overt computer surveillance allows employees to adjust their computer use and email communications, it may be less harmful to their dignity than covert surveillance.[124] However, to the extent that overt surveillance

---

[116] Paterson, Ibid, p 12.

[117] Ibid, p 11.

[118] Ibid, p 11.

[119] As reported in 'Big Brother may not be allowed to watch you', *The Sun Herald,* 16/12/01.

[120] Paterson, supra, p 12.

[121] Victorian Law Reform Commission, *Workplace Privacy: Issues Paper*, 2002, p 13ff.

[122] Ibid at 14.

[123] Ibid at 15.

[124] See Paterson, Note 67**,** p 12. See also US House of Representatives, Subcommittee on the Constitution of the House Committee on the Judiciary, Legislative Hearing on H.R 4908, the

causes employees to adjust their computer use, it impacts more on their autonomy.[125] Craig discusses the potential impact of overt surveillance on employees' autonomy:

> …pervasive employer monitoring of employee movements, conversations and telephone calls impacts directly upon the autonomy of workers. Such monitoring limits the range of options available to employees, not simply because it actively discourages activities unrelated to work, but also because it places a chill on what employees will say or do even during their personal time (ie lunch hours, coffee breaks etc). The practice of e-mail monitoring illustrates this point. The use of inter-office electronic message systems is now widespread and employees routinely use such systems for both work-related and personal matters…Employees who are aware that their messages may be accessed and read by supervisors will no doubt feel constrained in their use of e-mail. They may be less candid, or may choose not to send personal messages at all, even if the employer has no stated policy against the personal use of e-mail.[126]

Similarly, Ford states, 'knowledge that one is being watched or listened to, or may be being watched or listened to, has a chilling effect on one's freedom of action and inhibits one's engagement with others.' [127] Ford adds, 'the amount of time most people spend at work, and the importance to individual flourishing of relationships developed at work, support protecting autonomy there, just as it should be protected in the home...'[128]

4.7.4 Privacy issues relating to third parties arising from email monitoring

Paterson states, 'an issue that is frequently overlooked is that [email] monitoring also has privacy implications for persons who correspond with employees (including legitimate business contacts) who may reveal information about themselves. It also has implications for the informational privacy of third parties whose affairs are the subject of discussion in any of the communications.'[129] Those third parties might even be other employees.

4.8 Impact of computer monitoring on workplace environment

It has been suggested that like other forms of workplace surveillance, computer monitoring may impact adversely on employee morale and workplace relations:

> E-mail is progressively becoming the preferred mode of communication among employees, and protection against employer interception has thus become increasingly important to employee morale. Employees need some sort of conversational outlet during the workday, and the

---

"Notice of Electronic Monitoring Act", testimony of James X Dempsey, Senior Staff Counsel, Center for Democracy and Technology, 6 September 2000. He said that a legislative requirement for employers to give workers notice of monitoring would 'go a long way to restoring to workers their sense of dignity, which is a large part of the concept of privacy.'

[125] Cf Paterson, Note 67, at p 12, stating that, arguably, in the case of notified monitoring, the sense of loss of autonomy may be less harmful for an employee.

[126] Craig J.D.R, *Privacy and Employment Law,* Hart Publishing, US and Canada, 1999 at 22.

[127] Ford M. *Surveillance and privacy at work,* Institute of Employment Rights, 1999, p 17.

[128] Ibid.

[129] Paterson, Note 67, p 12.

> employment context would become unhealthy if employees were not comfortable freely conversing with one another on the preferred mode of communication…Employees may also experience apprehension or mistrust if they believe that the employer's monitoring is due to a suspicion or belief that the employees are dishonest.[130]

Similarly, Craig states, 'the imposition of policies impacting upon workers' private interests risks alienating those same employees, who may feel that their dignity is being attacked by an employer who does not trust them to do their jobs. This in turn creates a breakdown in the employment relationship, adversely affects employee loyalty and motivation, and may well undermine worker productivity.'[131] Lee also reports that 'studies show that employee surveillance in general takes its toll on workers and companies in terms of stress, fatigue, apprehension, motivation, morale, and trust; this results in increased absenteeism, turnover, poorer management, and lower productivity…'[132]

On the other hand, there is some evidence suggesting that employees do not object to computer monitoring provided they have been notified. An online *Ninemsn* article in April 2002 reported that 'an Australian survey, Internet Privacy and Surveillance, conducted late last year by psychologist Dr Monica Whitty, and Ray Archee, both from the University of Western Sydney (UWS), found that 74% of workers were happy to be monitored providing they were first informed by their employer.'[133] However, the survey focused on 'opinions about filtering software' and, therefore, it may be incorrect to interpret the results as meaning that that percentage of workers was happy for employers to *read* their emails.[134]

4.9 The debate about computer monitoring[135]

3.9.1 Argument for employers

Employers argue that they own the computer equipment being used by employees and that they should be allowed to monitor employees' use of that equipment for the legitimate reasons outlined above (eg to prevent 'cyberbludging', to guard against legal liability and to prevent leakage of confidential information). These legitimate reasons are mainly directed towards protection of the employers' business interests but some also involve protection of employees' interests (eg protection from sexual harassment). It is argued that

---

[130] Gantt II L.O, 'An affront to human dignity: Electronic mail monitoring in the private sector workplace', (1995, Spring) 8(2) *Harvard Journal of Law and Technology* 345 at 406.

[131] Craig, Note 126, p 25. See also Ford, Note 127, p 5.

[132] Lee L.T, 'Watch your e-mail! Employee e-mail monitoring and privacy law in the age of the "electronic sweatshop"', (1994-95) 28 *Marshall Law Review* 139 at 144. See also NSWLRC Interim Report, Note 61, at p 138-39 discussing detrimental effects of performance monitoring.

[133] 'Sex, lies and office email', *Ninemsn online,* 24/4/02.

[134] For a discussion of survey results, see Whitty M, 'Should Filtering Software be utilised in the Workplace? Australian Employees' Attitudes towards Internet Usage and Surveillance of the Internet in the Workplace' (2004) 2(1) *Surveillance & Society* 39, especially at p 50.

[135] See also Section 8 of this paper, 'Stakeholder views on the draft Bill'.

employers are justified in protecting these interests even if doing so intrudes on employees' privacy. Employers also argue that any legislative requirement for them to notify employees in the way set out in the draft Bill would subject them to substantial compliance costs.[136] It has even been suggested that such onerous requirements would lead small businesses to impose a total ban on the personal use of computers.[137]

4.9.2 Argument for employees

Unions, privacy groups and others argue that employees have a reasonable expectation of privacy in their computer use in the workplace. It is not suggested that employees are entitled to absolute privacy. What is said is that employees are entitled to be free from unreasonable intrusions on their privacy at work. In other words, that computer monitoring should operate within certain limits. The next question is, what limits?

(1) Employees are at least entitled to notice of computer monitoring
Unions, privacy groups and some commentators have argued that *covert* computer monitoring is an unreasonable intrusion on their privacy. They are at least entitled to be notified of any computer monitoring that is taking place. Firstly, because covert computer monitoring involves a serious invasion of privacy. And secondly, because it is unnecessary for employers to use covert monitoring. The National Workrights Institute in the US states, 'secret monitoring is not only unnecessary, it is counter-productive. The purpose of monitoring is to ensure that employees are following company policy regarding the use of electronic communications technology. If employees know that the company monitors email or internet access, they will be more careful to follow the rules.'[138]

(2) Limits should also be imposed on notified computer monitoring
Some also argue that a requirement that employers notify employees of monitoring does not go far enough; and that notified monitoring should operate within limits.[139] It is argued that (a) it is reasonable for employees to engage in some personal use of email and internet while at work, and (b) that they are entitled to some level of privacy when doing so. This position emphasises the importance of protecting privacy and autonomy in the workplace. Not just for the benefit of employees but also for the benefit of the workplace[140] and of society.[141] In support of this position, reference is made to the fact that work and home life

---

[136] See submissions by employer groups in Section 8 below. See also, for example, Gant II L.O, cited above at Note 130. See also Watson N, 'The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" enough?', (2001-02) 54 *Federal Communications Law Journal* 79 at 95 (outlining arguments on whether a notice requirement goes far enough – in Gant's view, it does go far enough).

[137] Ibid.

[138] US House of Representatives, Subcommittee on the Constitution of the House Committee on the Judiciary, Legislative Hearing on H.R 4908, the "Notice of Electronic Monitoring Act", Testimony of Lewis L. Maltby, President- National Workrights Institute, 6 September 2000.

[139] See in particular the submissions by privacy bodies in Section 8 below.

[140] See above as to impact of monitoring on the workplace.

have become increasingly intertwined, and to the fact that email has become an important mode of personal communication. It might also be argued that, overall, only a small percentage of employees engage in unacceptable email and internet usage.

For supporters of this position, the next question is what limits should be imposed on computer monitoring? Or, when is, and what form of, computer monitoring constitutes and unreasonable intrusion on employees' privacy? Some general limits on monitoring have been proposed by the NSW Law Reform Commission[142] and in other jurisdictions[143] – which not only limit monitoring itself but also the way in which information obtained by monitoring may be used or disclosed.[144] Academics have also discussed this issue. For example, one US academic's view has been summarised as follows:

> Dr Lee suggests adoption of a "flexible" federal policy "aimed at preventing unreasonable intrusions relative to varying types of business operations, organizational needs, and employee privacy needs." Such a policy would demand that electronic monitoring be "reasonable" requiring employers to (1) have a "legitimate" business purpose for engaging in monitoring; (2) use the least intrusive means possible to satisfy the business purpose; (3) limit the access, use, and disclosure to information reasonably meeting that objective…[145]

4.10 Complaints about dismissals of employees for computer misuse

4.10.1 General

Union discontent has also arisen in relation to dismissals of employees for computer misuse, which has usually been detected through computer surveillance.[146] Typically, dismissals have been for accessing pornographic websites or for distributing pornographic or other sexually explicit or offensive material via email. Three main objections have been raised by, or on behalf of, dismissed employees. Firstly, their employers did not have, or did not properly communicate to them, the employer's policy on acceptable computer usage (ie clearly setting out what employees could and could not do). Secondly, they were not told what the consequences would be for breaching such a policy. Thirdly, their employer did not notify them that their computer use would be monitored.

---

[141] As to privacy as a social value, see Victorian Law Reform Commission, *Issues Paper*, p 18-19.

[142] See summary of NSWLRC Interim Report below at Section 7 of this paper.

[143] See summary of position other jurisdictions at Section 9 of this paper. In relation to the position of the Victorian Law Reform Commission, see *Options Paper,* Note 88, p 71. There the Commission states (in part), 'employers' use of workplace surveillance may in some cases be a disproportionate response to the issues they are trying to prevent, limit or manage.'

[144] See below in Section 8 of this paper.

[145] Rodriguez A I, 'All bark, no byte: Employee e-mail privacy rights in the private sector workplace', (1998) 47 *Emory Law Journal* 1439 at 1465-66. Geist, Note 68, discusses elements of "reasonable" internet and email surveillance. See also Paterson, Note 67, at p 2-8 for a criticism of the use of *indiscriminate* computer surveillance in the workplace.

[146] Either general computer surveillance of employees or targeted computer surveillance of one or more employees after receiving a complaint about their conduct.

An article in the *Australian Financial Review* in May 2004 reports:

> Employers are facing growing resistance to systems that monitor email and internet use at work following a spate of sackings and demotions for employees who have shared joke emails and internet pornography.
>
> Unions, employee groups and disgruntled workers have lashed out at businesses for inflicting harsh sanctions on employees who misuse the internet, saying the rules for online behaviour are often unclear.
> …
> NSW Labor Council deputy assistant secretary Michael Gadiel said employers were failing to inform staff properly about their computer-use policies, which were often "in some human resource manager's bottom drawer and only came out when there was a problem."
>
> "We're not saying employees should be free to do what they want, but they should be aware of any monitoring that is put in place and they should also know what the rules are."[147]

The article refers to the "resignation" of an employee of the Department of Defence after he was caught sending smutty emails and pornography around the office. The worker said that he did not know that his behaviour was inappropriate and he also complained that he had never received a warning that he was breaching office policy. The Defence Department maintained that it used a warning screen that had to be acknowledged when workers logged on and which included conditions of use of the internet and advice on disciplinary action that could be taken. The article states that 'at the heart of the problem is lack of clarity about correct behaviour.' It also refers to research done by Dr Whitty, a psychologist with Queen's University in Belfast, showing that in general:

> …employees did not realise the seriousness of the sanctions they faced for internet misuse.
>
> She said staff were partly flaunting workplace policies, but were also caught up in the workplace culture of sending jokes and porn.
>
> Others, she said, simply perceived cyberspace as private space and thought sending a joke email that contain[ed] sexual material to a friend…was their own business.

The article notes that moves to introduce legislation come 'as internet experts warn of a rise in the number of staff dismissed or disciplined after their emails were checked and their office equipment was inspected.' According to the article, 'last year, Australian businesses lost more workers because of workplace internet misuse than in any previous year and the problem is accelerating. At least 14 cases were reported in 2003, compared with eight so far this year, including the Defence Department, Centrelink, NSW Police and Woolworths.'[148] An earlier article in April 2002 stated that:

> Thousands of people have lost their jobs in recent years in Australia for misuse of company technology. Cases include NSW Police, Telstra, FAI Insurance, Centrelink, Ansett, The Sydney Morning Herald, and Toyota. Overseas sackings have occurred at Intel, Xerox, The New York Times, BBC, Dell, Merck, Salomon Smith Barney, and Dow Chemical.[149]

---

[147] 'Log off! Backlash over office spies', *Australian Financial Review,* 14/5/04.

[148] Note, it is not clear whether these are reported instances of dismissals for computer use or unfair dismissal cases in an industrial tribunal relating to dismissals for computer misuse.

[149] 'Sex, lies and office emails', *Ninemsn online,* 24/4/02. As to acceptable usage policies, see

4.10.2 Unfair dismissal cases[150]

Williamson and Calderdone (March 2004) discuss unfair dismissal cases, relating to internet and email misuse, decided by the NSW Industrial Relations Commission and the Australian Industrial Relations Commission.[151] They refer to the 'basic principle in email and internet misuse cases which provides that so long as employers have clearly defined policies about email and internet use, and can establish that employees have been trained in relation to those policies, employers can rely on those policies to discipline, and in appropriate cases, dismiss employees for breach of those policies.'[152]

4.11 Blocking emails and websites containing industrial information

The draft Bill proposes to regulate the blocking of employees' emails and access to websites. One controversial aspect of this proposal from the employer's perspective is the provision prohibiting employers from blocking emails and access to websites that contain industrial information.[153] An article in the *Sydney Morning Herald* outlines union arguments in support of the prohibition as follows:

> Last year, Channel Seven won a fight [in the Australian Industrial Relations Commission] to block union emails during enterprise agreement negotiations.
>
> The NSW Labor Council, which supports the NSW government's proposal, said noticeboards were an ineffective way to communicate with members as organisations become more geographically dispersed.
>
> "Email is the modern equivalent to the old union noticeboard and right of entry provisions", NSW Labor Council deputy assistant secretary Michael Gadiel said. The law "certainly wouldn't involve using [email] in a way that was harmful to the organisations" he said.
>
> Mr Gadiel said email and the internet allowed members to establish more easily and quickly what their rights at work might be. He also said the legislation would only marginally change workplace practices because there were very few cases of employees trying to block union emails.[154]

---

for example, the NSW Premier's Department *Protocol for the Acceptable Use of Internet and Electronic Mail,* March 1999, located at: http://www.premiers.nsw.gov.au/pubs_dload_part4/prem_circs_memos/prem_circs/circ99/c99attachments/c99-09attach2.PDF

[150] Unfair dismissal laws are discussed below at paragraph 6.5.2.

[151] Williamson B and Calderdone F, 'Smut, Smut, Smut – A Tale of Email Porn: Internet and Email use in the Workplace', The College of Law, Continuing Professional Education, Seminar Papers, *Industrial Relations* 04/35, p 11.

[152] Ibid at p 20. The authors outline a number of guidelines drawn from the case law on what employers must have done for a dismissal on the grounds of computer use to be considered not unfair (see p 20-21).

[153] Another controversial aspect of this proposal is the requirement for employers to notify employees when their emails have been blocked. See employer submissions at Section 8.

[154] 'Employers fear incitement to strike under email law', *Australian Financial Review*, 13/7/04.

The article describes employer objections to the proposal as follows:

> The Chief Executive of business advisory group Employers First, Gary Brack, said he would fight for the clause to be removed from the draft NSW Workplace Surveillance Bill…."If its allowing your equipment to be used by a union in a fashion that could incite activity inimical to your interests, you should be able to block it."
>
> Workplace relations partner at law firm Deacons, Neil Napper, said the legislation was a Trojan horse in its present form. "It talks very much of privacy for individuals and protection of civil liberties but what it doesn't mention is the way it helps parties like unions ensure access to employer property."
>
> "Proponents will say it's no more than having unions currently come in and put notices up on noticeboards but it goes further than that [because] email is a fundamental tool of employers."[155]

5. TRACKING SURVEILLANCE OF EMPLOYEES

5.1 Introduction

The draft Bill defines "tracking surveillance" as 'the monitoring or recording of the geographical location or movement of [an] employee by means of an electronic device (such as tracking of the employee or of any vehicle driven by the employee by means of a Global Positioning System tracking device).'[156] Goldberg outlines the use of tracking surveillance in the workplace as follows:

> …GPS devices on company vehicles permit employers to monitor where [vehicles are], how fast they are driving, and where and how long the employee stops at a location. Using smart identification and clothing technology allows employers to monitor where employees are in the workplace and how long they are spending on certain tasks. [Tracking] technology in cell phones and handheld computers allows an employer to determine an employee's exact location while working or sending messages…
>
> Tracking technology is a benefit to employers for it has been found to increase productivity and efficiency, cut down on overtime, prevents theft and maintains compliance with company policies. Employees, on the other hand, are concerned regarding their right to privacy.[157]

Of course, tracking employees' movements is not a completely new phenomenon. Lane states, 'even before the Industrial Revolution and the wave of invention that followed, employers had some basic tools for tracking what their employees were doing during the

---

[155] Ibid.

[156] Draft exposure *Workplace Surveillance Bill 2004*, clause 3.

[157] Goldberg R, 'Tracking employees: Employee monitoring technology use must be fair', *Office Technology Magazine*, Business Technology Association, August 2004. Accessed online at http://www.bta.org/public/articles/details.cfm?id=1392

course of a day: Delivery records, customer receipts, travel logs, expense reports, and other types of business records could be used by an employer to analyze the effectiveness and efficiency of their employees.'[158] However, '[a]s various technological innovations became commonplace, the information companies have been able to collect regarding employee behaviour has grown steadily more comprehensive and detailed.'[159] A 2004 *ComputerWorld* article states, 'today's tracking systems can record, display and archive the exact location of any employee, both inside and outside the office, at any time...'[160]

5.2 Tracking employees outside the office

5.2.1 Vehicle tracking

What is vehicle tracking and who uses it?

Vehicle tracking devices use Global Positioning System (GPS)[161] technology to provide historical or real time data about company vehicles. This includes information about the vehicle's 'location, distance travelled, speed, travel time, idle time, fuel consumption and time at locations. Information…can then be downloaded and superimposed on a map to plot a vehicle's route or used to generate reports regarding the movements of vehicles over a particular period. Devices which can be located in a vehicle's suspension…can be linked to [tracking devices]. This can be used to determine whether cargo has been loaded or unloaded at an unexpected time or location.'[162] Discussing the use of tracking devices in the US, Lane (2003) states:

> Long range trucking companies have shown the greatest interest in GPS tracking data…As early as 1997, some major trucking companies were using GPS and onboard computers to track the movement of individual trucks, monitor repair schedules, and provide assistance in case of emergencies.
>
> Over the last few years, the increased affordability and power of the GPS system has made it possible for even modest-sized businesses to track their vehicles – and their employees' movements – with amazing precision. Employers are hailing the reams of incredibly specific information that can be gathered: a log of the times a vehicle spent moving and parked; a detailed map of the

[158] Lane, Note 81, p 188.

[159] Ibid.

[160] 'Can't hide your prying eyes', *ComputerWorld*, 1/3/04. Accessed online at http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,90518,00.html

[161] An article in the *Wall Street Journal* dated 14 May 2004 and entitled 'On the road again, but now the boss is sitting beside you' describes GPS technology as follows: Developed in the 1970s for military use, GPS relies on cluster of satellites orbiting 12,500 miles above Earth. The satellites emit coded signals, which a ground based receiver can pick up to triangulate its own position. GPS trackers remained expensive niche products through much of the 1990s largely because they were difficult to use and it was expensive to relay location data from a moving truck back to a company's home base. Now, thanks to the spread of cheap cellular-phone service the devices can send the information as easily as a commuter can make a call from the road.' See also Lane, Note 81, p 199ff.

[162] VLRC Options Paper, Note 88, p 21-22.

> vehicle's route, highly accurate mileage tallies (without the need for employee recording); the speed of a vehicle during the course of the day; increased security (some systems can record and report on the times and locations that cargo doors were opened); and the ability to provide drivers with accurate instructions.
> …
> Employers unquestionably find it valuable to know where their vehicles have been during the course of a day. But increasingly, they are demonstrating a willingness to purchase and install GPS systems that are capable of giving them real-time information about where their employees are located.[163]

The use of tracking devices appears to be most common in the transport industry, especially for heavy vehicles and/or vehicles which engage in long-distance transport and/or those that carry dangerous goods.[164] However, tracking devices have also been used in industries that involve technicians providing customer service at various locations[165] A US company that sells tracking systems has said that 'Our customers cover a range of field service operations…including government fleets, waste haulers, pest control, and auto glass installation services and tow truck operations, among others.'[166] The extent to which tracking devices are used in Australia is unclear although the Victorian Law Reform Commission has said recently that tracking devices 'are becoming more widespread.'[167]

What are the reasons for using vehicle tracking?

Different organisations may have different reasons for using vehicle tracking. In a submission to the Victorian Law Reform Commission, the Victorian Transport Association stated briefly the reasons for transport operators using tracking:

> Transport operators utilise vehicle management information systems and GPS tracking applications largely to provide increased productivity, customer service (information/freight tracking), security and monitoring of legal obligations with regard to speed, travel times and driving hours.[168]

The Victorian Law Reform Commission refers to employers' concerns as follows:

> Trucks can be very expensive pieces of equipment and employers in the transport industry have an interest in knowing where their vehicles are and how they are being used. This is important to

[163] Lane, Note 81, p 201, 203.

[164] Based on private communication on 27/9/04 with Hugh McMaster of the NSW Road Transport Association.

[165] See the report on use of tracking devices for Xerox photocopier repair workers below at paragraph 5.4.1.

[166] 'On Call: wireless monitoring, tracking and reporting solutions can benefit local transportation and mobile workforce operations', *Transport Technology Today,* Jan-Feb 2003.

[167] VLRC Options Paper, Note 88, p 21.

[168] Victorian Transport Association, Submission to Victorian Law Reform Commission re: Workplace Privacy, 15 January 2003, p 2.

> employers, not only from a management perspective, but also to ensure they are fulfilling legal obligations relating to occupational health and safety.[169]

The NSW Road Transport Association states:

> The underlying purpose for which [tracking] technologies are used is to improve the safety of the driver and other road users. These technologies will also assist in improved management of a transport fleet and improved customer relations.[170]

Vehicle tracking can be used to increase productivity and improve customer service in several ways. For example, tracking systems can be used to optimise delivery routes, to find a driver who is nearest a customer (eg repair technicians), to give customers more accurate indications of when to expect goods or consultants to arrive, and to give directions to drivers who are lost. Tracking systems can also be used to ensure that drivers do not take inappropriate detours and to check that they are not indulging in excessive break times.[171] Use for this purpose involves the most controversy.[172]

5.2.2 Mobile phone tracking

A March 2004 article in the *Telegraph* (UK) reports:

> Rapidly growing numbers of workers are having their movements monitored by their bosses through signals from their mobile phones.
>
> An estimated 40,000 employees are registered to new services which allow managers to pinpoint their locations at the click of a computer mouse. The figure is growing at a rate of around 20 per cent per month.
>
> …
>
> Several British companies began offering what the industry calls location-based tracking last year. Subscribers can pull a map on a computer screen showing the location of chosen mobile phones.
>
> Under the European Commission's privacy and electronic communications directive, as adopted by Britain in December, a mobile user can be tracked only if he or she gives consent.
>
> The services are popular with companies who want to keep track on delivery or sales team members.

---

[169] VLRC *Options Paper,* Note 88, p 61. The Commission refers to a submission which summarised to the benefits of tracking devices as: 'improved safety, productivity and competitiveness through maximising vehicle and driver utilisation.' (p 22, para 2.15).

[170] NSW Road Transport Association Inc, Submission to Attorney General on Workplace Surveillance Bill 2004, p 1. This organisation also notes that it is currently 'involved in consultations with the Roads and Traffic Authority, WorkCover and the National Transport Commission that can be expected to extend the scope of the use of these technologies by enforcement agencies and by the road transport industry.' (p 1).

[171] See Lane, Note 81, p 202.

[172] One company markets its vehicle tracking products as follows: (1) Track, monitor and communicate with your mobile workforce; (2) Reduce your overtime and operating, maintenance and insurance costs;(3) Increase safety and security; (4) Improve your customer satisfaction. See Navtrack website <http://www2.navtrak.net/enterpriseBusiness.cfm

It allows them to tell clients when to expect goods or consultants more accurately.[173]

Various methods for tracking mobile phones have been developed, including use of GPS technology.[174] However, the extent to which this technology is available or being used to track workers in Australia is unclear. The Australian Communications Authority published a discussion paper in January 2004 on the 'future use of location information to enhance the handling of emergency mobile phone calls', which states that 'although the use of location techniques for asset tracking and fleet management is becoming increasingly common, very few [location based services] are currently available to Australian mobile phone users.'[175]

5.3 Tracking employees inside the office

5.3.1 Access cards

Access cards or key cards issued to employees regulate their ability to open electronically locked doors within an office building.[176] Lane refers to the common use of magnetic strip, or "magstripe" technology, similar to that found on the back of credit cards.[177] These cards, which usually double as ID cards, are typically encoded with information about the employee such as their name, identification number, and security level. The cards are usually wired into network, so that when an employee swipes his or her card, the information in the strip can be verified by a central database. In addition, most such systems are designed to record the date, time, and identity of each employee who goes through access points. In this way, access cards collect information on employee movement within a building, although their main purpose is building security. More recently, access cards have incorporated biometric technology, which can identify users on the basis of physical characteristics such as fingerprints or irises.[178]

---

[173] 'Snooping protest as firms track workers' mobiles', *Telegraph (UK),* 15/3/04

[174] These methods are discussed in Australian Communications Authority, *Location Location Location: The future use of location information to enhance the handling of emergency mobile phone calls,* January 2004, p 27ff.

[175] Ibid, p 8. The discussion paper notes that 'at present, a mobile call to the emergency call service is accompanied by very broad mobile location information' which 'can range from 2,000 to 500,000 square kilometres'; and it discusses the future use 'of higher accuracy location technique' to provide data within 50 to 500 metres. See also Lane, Note 81, p 196-97.

[176] ABI submission p 6.

[177] The following section is based on Lane, Note 81, p 109ff.

[178] See below at paragraph 10.2.

5.3.2 Active Badges[179]

More effective tracking of employee movements is possible with "Active Badges", which rely on infrared technology. Employees are given a special ID card equipped with an infrared device that sends out a unique signal every fifteen seconds or so. If the card is within a certain distance of an infrared sensor (mounted on a wall or ceiling), the code is read by the sensor. The sensor is connected to a network of other sensors, all of which are linked to a central station. The central station periodically retrieves data from each of the sensors and uses the information to compile a map of each badge's current location. More recent forms of Active Badges rely on Radio Frequency Identification Data technology.[180]

Active Badges are said to make for a more efficient workplace by making it easier to locate co-workers. The use of Active Badges appears to be most common in hospitals. Lane reported that, in the US, 'by 1997, nurses in over 200 hospitals were wearing infrared badges'[181]; and an ABC News (US) article in January 2001 stated, 'in the hospital industry….55,000 employees now wear an electronic monitor as a condition of employment.'[182] In the UK, a May 2004 article in the *Financial Times* reported that 'district nurses and GPs are being fitted with high-technology tracking devices as part of [a National Health Service] pilot scheme to make life safer for lone health workers.'[183] These identity badges would only emit a location signal upon staff pushing a button.[184]

5.4 Complaints about tracking surveillance of employees

5.4.1 Complaints by Australian workers about use of vehicle tracking

Outlined below are some examples of complaints raised in relation to vehicle tracking.

Botany council workers: In February 2000, Botany Council outdoor workers went on strike over the installation of tracking devices in council vehicles, apparently without consultation with workers.[185] A union report of the dispute states that 'Botany Council

---

[179] This section is a summary of Lane, Note 81, p 109ff.

[180] See Lane, ibid, p 110. As to RFID technology generally, see James M., 'Where are you now? Location detection systems and personal privacy, Commonwealth Parliamentary Library, *Research Note No. 60,* 15 June 2004.

[181] Lane, ibid, p 113.

[182] 'Every step you take…', *ABC News online,* 4/1/01.

[183] 'NHS workers fitted with tracking device', *The Financial Times,* 26/5/04.

[184] Ibid.

[185] See 'Fighting Botany's Big Brother Spies', United Services Union Industrial update, 7/2/00 at <http://www.meu.org.au/updates/4.html> and 'Council's Hollow Consultation Offer', United Services Union Industrial update, 25/2/00 <http://www.meu.org.au/updates/2.html>

installed the devices allegedly to increase productivity and enhance driver safety, but failed to disclose that the device has surveillance capabilities.'[186]

AGL workers: A dispute involving AGL employees arose in 2001 after workers 'discovered they were being spied on.' [187] A union report of the dispute states:

> The workers had agreed to have tracking devices installed in their vehicles in 1998 to assist to respond to emergencies. At the time AGL promised that the devices would not be used to track individuals.
>
> But the AWU's Jeff Byrne says that in recent months staff have been disciplined for the use of their vehicles and movements are now being used to validate overtime claims.
> …
> Labor Council will raise the issue with NSW Attorney General Bob Debus, who is currently considering a Law Reform Commission Report into Privacy. [188]

Patrick Autocare workers: In March 2003 the Victorian branch of the Transport Workers Union lodged an application in the AIRC over Patrick Autocare's use of GPS technology in its motor vehicle fleet.[189] The union argued that, under the Victorian legislation, the company required the consent of the 60 owner/drivers to implement the technology.[190]

Xerox photocopier repairers: On 22 September 2004 it was reported that around 120 photocopier repairers in NSW went on strike over a plan by their employer, Xerox, to monitor staff movements using GPS tracking technology.[191] A further 80 Xerox workers in Victoria threatened to strike. The President of the Australian Services Union (ASU) said that that the 'technicians used their cars like their offices, and they resented being monitored every moment of the day. For them it's just an issue of trust, number one. And number two, it's just another layer of monitoring…that they're not prepared to cop.' Xerox said it had no immediate plans to install tracking devices in technicians' vehicles or equipment but it wanted to be able to use such technology in the future. The ASU and Xerox are currently negotiating a new pay and conditions agreement.

---

[186] Ibid.

[187] 'New Spying tactics hit work cars' <http://workers.labor.net.au/106/news3_spies.html>

[188] Ibid.

[189] Patrick Corp defends GPS technology', Thompson Privacy Alert, Issue 41 19/3/03. Located at << http://www.cpd.com.au/cpdnews/pa/Archive/PA41.htm>>. See also 'Union says company tracking workers illegally', *The Age,*12/3/03.

[190] Ibid.

[191] 'Xerox workers striker over spying', *The Age,* 22/9/04. As at 29 September 2004, the workers remained on strike. The following is a summary of the article. See also 'Union halts Fuji Xerox GPS plan', *Australian IT,* 23/9/04, and 'Xerox workers to strike over satellite tracking plan', *ABC Online,* 22/9/04.

Labor Council: In a 2003 submission relating to the review of the *Workplace Video Surveillance Act 1998*, the NSW Labor Council stated:

> In one NSW statutory authority, the vehicles of workers are fitted with GSM cellular monitoring in an attempt to determine the location of the vehicle for safety purposes and to make sure different jobs were appropriately allocated on geographical basis. However well-intentioned, the privacy implications for these workers during break times or whilst off duty have not been considered and there are policy issues in relation to how the employer may use that surveillance information.[192]

5.4.2 Complaints by US workers about vehicle and phone tracking

A Wall Street Journal article dated 14 May 2004 reports:

> As employers increasingly turn to GPS technology to keep track of their fleets, more workers are baulking at having the boss constantly looking over their shoulders. Independent snowplow drivers in Massachussetts staged a demonstration at the state capitol last year after they were required by the state to carry GPS-enabled cellphones. Washington state garbage collectors are protesting the installation of the devices on their trucks. And Teamsters union officials are watching closely to make sure their devices aren't used to punish employees.[193]

The article refers to frustrations of 'independent-minded workers such as truckers, who have long treasured their freedom from close supervision. Many of those workers are accustomed to being paid for…getting a shipment from one place to another…and chafe at the idea of having their routes closely tracked.' The Teamsters union were concerned that workers had been told 'they could be in trouble if the tracker reports they are straying from their routes.' United Parcel Service officials said that it 'would use the technology to improve customer service…and not driver discipline.' The article also reports a case in which police officers were dismissed after tracking devices installed in their vehicles, without their knowledge, allegedly showed they were absent from duty.

5.4.3 Complaints by workers about use of active badges

The article in US press on the use of active badges in hospitals, which was referred to above, reported that while some employees thought that the badges made their job easier, others were concerned that the devices tracked employees everywhere they went, even on trips to the bathroom and during break times.[194] Concerns were raised about pressure on nurses to account for every moment and it was argued that privacy was being traded for efficiency. In addition, there were concerns that monitoring could stifle union organising and whistleblower activity. The article in the UK press on the use of tracking devices by health workers (which would only be activated if staff pressed a button) reported that public sector unions in the UK were in favour of this proposal but wanted 'strict guidelines to prevent Big Brother style snooping.'[195]

---

[192] NSW Labor Council, 'Submission to the NSW Government on the Workplace Video Surveillance Act 1998, p 4.

[193] 'On the road again, but now the boss is sitting beside you', *Wall Street Journal,* 14/5/04

[194] 'Every step you take…', *ABC News online,* 4/1/01.

[195] 'NHS workers fitted with tracking device', *The Financial Times,* 26/5/04.

6. CURRENT REGULATION OF WORKPLACE SURVEILLANCE

6.1 Introduction

While the *Workplace Video Surveillance Act 1998* is currently the only legislation that specifically regulates any form of workplace surveillance, other legislation and laws need to be considered in relation to workplace surveillance. This includes legislation regulating specific forms of surveillance (eg interception of telecommunications), general common law, privacy legislation, and industrial laws and agreements.[196]

6.2 Federal laws regulating interception of telecommunications

Under the *Telecommunications (Interception) Act 1979 (CTH)*, it is generally unlawful to intercept a communication passing over a telecommunications system without the knowledge of the person making the communication.[197] This legislation clearly applies to the monitoring of telephone conversations but there has been doubt as whether it applies to monitoring of emails. One issue is whether email monitoring would be an interception of a communication *passing over a telecommunications system.* It has been pointed out that 'surveillance of internet and email communications may occur at points either before or after they have passed through the telecommunications system: eg, email may be monitored, read or down-loaded when in the mailbox or the hard drive of the sender or recipient.'[198] As the uncertain application of the Act has been an issue for police, an amendment Bill has been introduced into federal parliament to clarify the situation.[199] If the amendment is passed, it would not be unlawful to intercept a 'stored communication' (eg stored emails, voicemail, and SMS messages).[200]

---

[196] The focus in this section is on current laws relevant to surveillance at work, and in particular computer surveillance and tracking surveillance. Regulation of the use of listening devices (ie "bugs") to monitor or record a private conversation (by the *Listening Devices Act 1984 (NSW))* is not covered here. Nor is regulation of the interception of telecommunications – including telephone conversations. The latter is covered by federal legislation (*Telecommunications (Interception) Act 1979*), which is discussed below in the context of email surveillance.

[197] A communication includes a conversation and a message, whether in the form of speech, music or other sounds, data, text, visual images or signals.

[198] NSWLRC Interim Report, Note 61, p 64-65 (para 2.48)

[199] *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004.* The Bill was proposed as a temporary solution (for 12 months) pending a review of the Act, and in particular its application to electronic communications. On 16 June 2004, the Senate referred the provisions of the Bill to the Senate and Constitutional Legislation Committee for inquiry and report by 22 July 2004. On 22 July, the majority of the Committee (coalition and ALP) recommended that the Bill proceed. See Electronic Frontiers Australia website: http://www.efa.org.au/Issues/Privacy/tia-bill2004-sc.html

[200] Note also that in relation to telephone monitoring it has been pointed out that employers may be able to rely on an exception in the Act, which applies to an interception carried out by 'a person lawfully on premises to which a telecommunications service is provided by a carrier, by means of equipment that is part of that service.' See VLRC Options Paper, Note 88, p 26, at footnote 129. In this regard, note that Privacy NSW states, 'an employer who sets up a system

6.3 Privacy rights under general law

There is presently no common law action for breach of privacy although it is possible that a limited form of action in tort may become recognised in the future.[201] There are, however, existing common law actions that provide some indirect protection of privacy. Two such actions are relevant to workplace surveillance, or more specifically, to the use of information obtained by workplace surveillance. Paterson refers to these actions as follows, 'if the information was surreptitiously gathered concerning a confidential communication to a third party, then its dissemination may give rise to an action for *breach of confidence* in circumstances where the employee can establish some detriment. There is also obvious potential for *defamation* proceedings.'[202]

6.4 Privacy legislation

6.4.1 Federal privacy legislation[203]

The *Privacy Act 1988* regulates the collection, use and disclosure of personal information about individuals. The Act originally only covered the Commonwealth public sector, but since 2001, it has applied in relation to much of the private sector as well. The Act contains a number of privacy principles that organisations must comply with.[204] Commonwealth public sector employees and employees in the private sector may receive some protection with respect to workplace surveillance. However, 'the protection which the Act gives workers in the private sector is limited' because (1) the Act does not apply to (1) "small business operators" and (2) information which is held by the employer in an "employee record".[205] There has been doubt about whether employer monitoring of emails would fall within the latter exemption.[206] The Victorian Law Reform Commission notes that this exemption is currently under review:

> The Privacy Act's employee records exemption has been a source of controversy. The Commonwealth Government indicated soon after the enactment of the Privacy Act that the

---

to listen to or record employee's calls is not breaching the Act.' (See Privacy NSW website).

[201] See *Kalaba v Commonwealth of Australia* [2004] FCA 763, Heerey J at [6]. See also Sneddon M and Troiano R, 'New tort of invasion of privacy and the internet', (2003) 6(6) *Internet Law Bulletin* 61.

[202] Paterson, Note 67, p 16 (emphasis added).

[203] The following paragraph is largely based on Victorian Law Reform Commission, *Issues Paper: Workplace Privacy*, 2002, p 49. For more information on the Privacy Act 1988 see website of Federal Privacy Commissioner, http://www.privacy.gov.au

[204] The Act contains 11 Information Privacy Principles (IPPs) which apply to Commonwealth and ACT government agencies; and 10 National Privacy Principles (NPPs) which apply to parts of the private sector and all health service providers.

[205] VLRC Issues Paper, supra, p 49.

[206] See for example, 'Emails at work a grey area under extended Privacy Act', *Sydney Morning Herald,* 26/6/01.

exemption would be reviewed as part of a general review of the Privacy Act following its second year of operation. The Commonwealth Attorney General's Department and the Department of Employment and Workplace Relations released *Employee Records Privacy: A discussion paper on information privacy and employee records* for public comment in February 2004. The Discussion paper posed a range of options in relation to employee records exemption, including:

- retaining the exemption;
- non-legislative measures such as education, guidelines or policies;
- amendments to the Privacy Act to delete or modify the employee records exemption;
- enacting specific employee records privacy principles
- enhancing protection of employee records in workplace relations legislation

Responses to the paper were due in April 2004.[207]

6.4.2 Privacy Commissioner's Guidelines on Workplace Email and Internet

As noted above, in March 2000, the Federal Privacy Commissioner, which oversees the *Privacy Act 1988*, released *Guidelines on Workplace E-mail, Web-browsing and Privacy*.[208] For Commonwealth government agencies the guidelines are 'strongly recommended as constituting compliance with the *Privacy Act 1988*. For the private sector and other organisations not covered by privacy legislation the Guidelines are recommended as good privacy practice.'[209] The Commissioner states, 'the purpose of these Guidelines is to recommend steps that organisations can take to ensure their staff understand the organisation's position on [the] issue through the development of clear policies.'[210]

A few key points from the *Guidelines* are noted here. The *Guidelines* state that the policy should be 'explicit as to what activities are permitted and forbidden.' In addition, the policy should clearly set out what information is logged and who in the organisation has rights to access the logs and content of staff email and browsing activities.' The policy should also 'outline…how the organisation intends to monitor or audit staff compliance with its rules relating to acceptable usage of e-mail and web-browsing.' The policy should be communicated to 'staff and management should ensure that it is known and understood by staff. Ideally the policy should be linked from a screen that the user sees when they log on to the network.' In relation to monitoring and in conclusion, the *Guidelines* state:

---

[207] VLRC Options Paper, Note 88, p 11. Review of the employee records exemption is also discussed in Australian Law Reform Commission, *Essentially yours: Protection of Human Genetic Information in Australia,* Report 96, March 2003, p 847-55. The Commonwealth Attorney General's Department is currently reviewing the submissions made in response to the February 2004 discussion paper (as at 14 October 2004).

[208] Office of the Federal Privacy Commissioner, *Guidelines on Workplace E-mail, Web-browsing and Privacy*, March 2000. Available from website at http://www.privacy.gov.au/internet/email/.

[209] Ibid, p 1. The Guidelines were released before the amendment to the *Privacy Act* in 2001 extending the Act to part of the private sector. A notation on the Guidelines states 'the Office is reviewing the guidelines to look at how they might apply to the private sector.'

[210] Ibid.

> While it is acknowledged that access to staff e-mails and browsing logs by system administrators may be required in certain circumstances, it is unlikely that pervasive, systematic and ongoing surveillance of staff e-mails and logs should be necessary.
>
> Organisations are encouraged to foster an environment where staff are assured that the privacy of their communications will be respected as long as they abide by the organisation's stated policy.'[211]

6.4.3 NSW privacy legislation

The *Privacy and Personal Information Protection Act 1998 (NSW)* regulates the way in which NSW state and local government agencies deal with personal information. The NSW Privacy Commissioner, who administers the Act, provides a brief summary of it:

> The *Privacy and Personal Information Protection Act 1998* (or PPIP Act) deals with how all NSW public sector agencies manage personal information. The Act includes 12 information protection principles (IPPs), establishes methods for enforcement of privacy, establishes a mechanism for complaints if you think that your personal information has been mishandled, and sets out the role of the NSW Privacy Commissioner.
> …
> The 12 information protection principles form the backbone of the Act and must be adhered to by all NSW public sector agencies. They can be grouped under five main headings - collection, storage, access and accuracy, use, and disclosure.
>
> The Act also contains lawful exemptions from these principles, as well as the power to investigate and conciliate complaints concerning breaches. Remedies can be enforced against public sector agencies by the Administrative Decisions Tribunal.
>
> The PPIP Act allows the NSW Privacy Commissioner to investigate and conciliate privacy complaints made against any person or organisation. These investigations are not limited to complaints about mishandling of personal information.[212]

6.5 Industrial laws and employment contracts[213]

The primary industrial relations statute in New South Wales is the *Industrial Relations Act 1996 (NSW),* with its federal counterpart being the *Workplace Relations Act 1996*. Neither of these Acts expressly regulates surveillance in the employment context. However, they do provide the potential for surveillance to be regulated indirectly.

---

[211] Ibid, p 4-5.

[212] Privacy Commissioner NSW website, accessed at: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipact. Note that the Attorney General's Department is currently undertaking a statutory, five-year review of the Act to 'determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives.' See Lawlink website: http://www.lawlink.nsw.gov.au/lap.nsf/pages/privacystatreview

[213] Unless otherwise indicated, this section is a summary of NSWLRC Interim Report, Note 61, p 291ff.

6.5.1 Inclusion of surveillance in industrial instruments and disputes

The surveillance of employees in the workplace is listed as an example of an "industrial matter" in the NSW legislation. Accordingly, surveillance can be the subject of negotiations regarding employment conditions, addressed in awards and enterprise agreements. As an industrial matter, surveillance may form the basis of an industrial dispute, which can be arbitrated by the NSW Industrial Relations Commission. Under the federal legislation, only "allowable award matters" can be included in an industrial dispute, which can be addressed by the Australian Industrial Relations Commission by way of arbitration or an award. Surveillance is not listed as an allowable award matter. Despite not being an allowable award matter at federal level, surveillance can be a negotiated condition of a certified agreement or an Australian Workplace Agreement under the federal legislation.[214] There are 'a number of [certified] agreements that deal with [workplace surveillance issues] such as email monitoring, keystroke monitoring, call monitoring, and video surveillance.[215]

6.5.2 Unfair dismissal laws

Under state and federal industrial legislation, employees are able to apply for relief in respect of a dismissal that was harsh, unjust or unreasonable. Relief is potentially available where the dismissal is based on evidence collected using surveillance. However, at both state and federal level, relief is only available to a limited range of employees (eg it is not available to many casual employees). Determination of an unfair dismissal claim is a discretionary exercise and each case is considered in light of its own particular circumstances. However, both state and federal legislation set out a number of matters (eg whether a warning was given before the dismissal), which the respective Commissions must take into account. Under both state and federal legislation, the remedies for unfair dismissal are (1) reinstatement to the employee's former position; (2) re-employment in a different, suitable position; (3) if neither of those remedies are appropriate, the applicant may be awarded compensation.

6.5.3 Employment contracts

For those employees not covered by an award or other similar industrial instrument, or by the statutory unfair dismissal provisions, any regulation of surveillance depends upon the express and implied terms of their employment contract. Employees may be able to negotiate a contractual provision regulating the use of surveillance by their employer. In addition, a possible source of control on the use of surveillance is the term implied in employment contracts that an employer will not unreasonably damage or destroy the relationship of trust and confidence between employer and employee. The purpose of this implied term is to protect the employee from oppression, harassment, and loss of job satisfaction. According to the NSW Law Reform Commission, use of covert surveillance by an employer could implicate this purpose.

---

[214] This is discussed in VLRC Issues Paper, Note 88, p 64-65.

[215] Ibid, p 65-66.

7. NSW LAW REFORM COMMISSION INTERIM REPORT

7.1 Introduction[216]

In 1996 the Commission received a reference from the then Attorney General, the Hon Jeff Shaw QC, MLC, to inquire into and report on matters pertaining to the *Listening Devices Act 1984* (NSW), the use of visual surveillance equipment, and any related matter. In May 1997, the Commission released an *Issues Paper* inviting submissions from the public. Over 37 submissions were received. The Commission then published its 500-page Interim Report in February 2001. The Interim Report recommended the introduction of a new *Surveillance Act*, the details of which are outlined in over 100 recommendations in the report. Consultation has occurred since the Interim Report and a final report is due to be released in December 2004.[217]

7.2 Summary of recommendations in Interim Report

The recommendations made by the Commission are summarised in the Executive Summary to the Interim Report:

> …The Commission recommends the introduction of a new Sur*veillance Act* which, among other things, would replace the *Listening Devices Act 1984* (NSW) and the *Workplace Video Surveillance Act 1998* (NSW). In making its recommendations, the Commission takes the approach that, in order to be optimally effective, any new legislation designed to govern surveillance should be as broad in scope as the nature of surveillance itself. The legislation should not be device specific to ensure that the law is not outpaced by technological developments.
>
> …..
> The Commission's recommended regime includes surveillance conducted overtly (ie with the knowledge of the person being monitored) or covertly. It covers surveillance regardless of where it is conducted (both public and private places are covered, as well as the workplace), or who it is conducted by (law enforcement officers, employers, private investigators, the media, and any person conducting surveillance in the public interest are all included in the proposed legislative regime). The Commission's recommended regime will also cover aspects of internet and e-mail surveillance and data surveillance.
>
> Under the Commission's recommendations, surveillance should be considered to be overt where adequate notice is given to the subject prior to, or simultaneously with, the occurrence of the surveillance. Notice would be proven where there are clearly visible signs or other warnings, such as audio announcements etc, that are widely understood and indicate that surveillance is, or may be, occurring. Where surveillance of employees is conducted by an employer, the Commission recommends that an additional notice requirement should apply in order for the surveillance to be considered overt, due to the added rights and responsibilities inherent in the employer/employee relationship. Surveillance conducted in circumstances that do not meet these notice requirements would be considered to be covert.
>
> So far as overt surveillance is concerned, the Commission recommends that this should be regulated flexibly, requiring adherence to eight legislative principles to be supplemented by codes of practice for those conducting a significant amount of overt surveillance.

---

[216] This paragraph is based on NSWLRC Interim report, Note 61, p 4.

[217] Information as to the release of the final report was obtained via private communication with the NSW Law Reform Commission in early October 2004.

…..
Failure to comply with the principles would expose those conducting overt surveillance to the threat of a civil action under the proposed surveillance legislation.

Since covert surveillance is conducted without the knowledge of the subject, and is thereby more intrusive than surveillance conducted overtly, it should be regulated more stringently.

The Commission recommends that the approval of an independent arbiter should have to be obtained before any covert surveillance may occur under the proposed Surveillance Act. In circumstances where such prior approval is not possible or practicable, it may, where appropriate, be obtained retrospectively. The Commission has isolated three main areas where covert surveillance may legitimately be conducted. Those are law enforcement, in the course of employment, and in the public interest.

- Covert surveillance by, or on behalf of, law enforcement officers should be regulated by a warrants procedure similar to that…in the *Listening Devices Act 1984* (NSW), with applications made to and warrants issued by "eligible judges" in the courts system.

- Covert surveillance by, or on behalf of, employers should be authorised by members of the Industrial Relations Commission.

- Covert surveillance conducted in the public interest by anyone other than law enforcement officers or employers (or people acting on their behalf) must be authorised by an appropriate issuing authority, being either members of a court or a tribunal.

The proposed Surveillance Act should also specify measures to promote accountability for the conduct of covert surveillance and the use of material obtained as a result. Breach of the provisions of the proposed Surveillance Act regarding covert surveillance would give rise to a criminal offence. In addition, liability for a civil action resulting in damages or other appropriate remedies may be incurred as a result of a breach of the Act.[218]

7.3 Comparison between recommendations and draft Bill

It may be seen from the above that the NSW Law Reform Commission has proposed a similar framework for regulating workplace surveillance as that contained in the draft exposure Bill. The main difference between the two proposals is that the Commission proposes regulation of overt surveillance in addition to covert surveillance. Employers would need to comply with eight legislative principles when undertaking overt surveillance (eg it should not be used in a way that it breaches an individual's reasonable expectation of privacy). These principles would need to be supplemented with codes of practice for 'significant users' of surveillance. Contravention of the principles would give rise to a civil action. This and other significant differences between the two proposals are summarised in **Appendix 2** to this paper**.**

[218] NSWLRC Interim Report, supra, p xii-xvii.

7.4 The case for reform

7.4.1 The case for legislation dealing with covert workplace surveillance

Putting the case for specific legislative regulation of covert surveillance in the workplace, the Commission stated:

> …serious questions must be asked about the desirability of leaving surveillance to be addressed as a negotiable condition of employment. One obvious concern is the inequality in bargaining power between employee and employer that often exists. This inequality is potentially exacerbated by the abstract nature of privacy interests…A further concern is that any bargaining process may not be an informed one, if employers are not required to disclose their surveillance practices. In addition to these practical concerns, there is the issue of whether it is appropriate to reduce a fundamental interest, such as privacy, to a bargaining issue.
> ……
>
> The current regulatory framework does not provide comprehensive regulation of surveillance by employers. Many forms of surveillance are, at best, only indirectly regulated. Furthermore, in order to trigger the indirect protection of industrial remedies such as relief against unfair dismissal, extreme circumstances must be involved. The Commission considers that it is inappropriate for a matter of fundamental importance, such as personal privacy, to be addressed in such a piecemeal and indirect manner. In accordance with its status, employee privacy should be protected as a matter of course, rather than only gaining protection in circumstances of extreme violation.
>
> On a more practical note, the vagaries of the current regulatory system are intolerable for both employer and employee. Employers are often unable to obtain confirmation of the legality of their surveillance procedures and employees have no certain basis upon which to challenge an aspect of their workplace surveillance policy. In the view of the Commission, the requisite certainty can only emerge from a legislative model.[219]

7.4.2 The case for legislation dealing with overt workplace surveillance

The Commission outlined the case for legislative regulation of overt surveillance in *society generally* and after outlining a framework for regulating overt surveillance, it turned to the "employment context" and expressed the view that 'overt surveillance of employees by employers should be regulated according to the general framework proposed for overt surveillance...'[220] Presumably, this view was taken for similar reasons to those outlined in making a case for legislative regulation of overt surveillance in society generally. Those reasons were (in part):

> …The Commission disagrees with the suggestion that existing laws and codes of practice provide sufficient privacy safeguards against technologies which can access huge quantities of personal information…
>
> …The indiscriminate haul of information that can be obtained through using overt surveillance devices means that, even if the surveillance were undertaken for a legitimate purpose, not all the information gleaned necessarily relates to that purpose. What should happen to that information is a serious concern.

[219] Ibid, p 295-97.

[220] Ibid, p 196.

> The Commission further sees a need for statutory regulation of this area in order to provide certainty, consistency and, above all, accountability, elements missing from self-regulatory schemes. Accountability is crucial to providing the necessary incentive to surveillance users to abide by codes of practice. This has benefits for both users and subjects of surveillance. The latter will have the reassurance of rights backed by the force of law. Concomitantly, these rights will be enforceable by means of prescribed sanctions. The former will have set down clear principles of behaviour, to assist them in upholding community expectations regarding privacy. The enactment of statutory provisions mean that no individual participant within an industry or sector can afford to ignore privacy concerns while benefiting from community assumptions that privacy codes of practice apply universally…Furthermore, the Commission believes that those surveillance users who are already voluntarily abiding by codes of practice will not be adversely affected by this recommendation…[221]

[221] Ibid, p 163-64. See also pp 168-72.

8. STAKEHOLDER VIEWS ON DRAFT EXPOSURE BILL

8.1 Introduction

This section of the paper outlines some stakeholder views on the draft exposure *Workplace Surveillance Bill 2004* as contained in submissions made to the Attorney General's Department. Note that around 40 submissions were lodged and only a few are covered here.[222] The focus here is on the key points raised in the submissions covered.

8.2 Unions

Labour Council of NSW

The Labor Council of NSW has not lodged a submission on the *Bill*. However, in about October 2003, the Council made a submission to NSW Government in relation to a review of the *Workplace Video Surveillance Act 1998.* In that submission, the Labor Council strongly recommended that the Act be extended to cover all forms of workplace surveillance to ensure adequate protection of workers' privacy in NSW.[223] The Labor Council was concerned that 'public interest and workplace privacy rights have been neglected as regulation has not kept pace with the rapid advancement of technology.'[224] In particular, the Labor Council referred to 'surveillance of email and internet, biometrics and GSM/GPS [tracking devices]'.[225] Two other concerns which the Council raised were (1) Warrants being awarded to employers without adequate evidence of illegal activity;[226] and (2) The failure of the Act to protect labour-hire workers.[227]

8.3 Privacy bodies

8.3.1 Office of NSW Privacy Commissioner

Privacy NSW 'continues to support the introduction of comprehensive surveillance legislation, as recommended by the NSW Law Reform Commission in 2001…However

[222] The submissions that are discussed in this section were obtained from searches on the internet and through contacting various interest groups. The Attorney General's Department informed the writer on 7 October 2004 that around 40 submissions had been received in relation to the draft Bill, some of which were received in oral form.

[223] Labor Council of NSW, *Submission to the NSW Government on the Workplace Video Surveillance Act 1998,* p 3, 5. The submission is available at: http://www.labor.net.au/campaigns/emailprivacy/background/submissiontoag.html

[224] Ibid, p 3.

[225] Ibid, p 3.

[226] Ibid, p 2.

[227] Ibid, p 3.

until [such] legislation is introduced, Privacy NSW supports specific legislation to protect employees' privacy in the workplace.'[228] Privacy NSW criticises the *Bill* for failing to regulate overt or notified workplace surveillance:

> …the Bill's failure to comprehensively regulate 'notified' surveillance does not provide a sound regulatory framework for the protection of employees' privacy interests. Privacy NSW is concerned that the Bill will leave employees vulnerable to intrusive surveillance practices, particularly given the lack of protection for employees under existing privacy legislation.
>
> Privacy NSW recommends that the Bill be amended to incorporate comprehensive privacy principles for the conduct of 'notified' surveillance. This would ensure that employees have protection for the manner in which information obtained via 'notified' surveillance is collected, stored, used and disclosed by employers.[229]

Other recommendations by Privacy NSW include:

- The Bill should have a broader, technologically neutral definition of surveillance rather than being limited to 3 specific types of surveillance;[230]
- The 'workplace security' defence in the Bill should be removed;[231]
- The Bill should provide that an employer's policy on email and internet use be made by way of *agreement* with employees or their industrial organisation. In the case of unrepresented employees, employers should be required to consult with the Privacy Commissioner as to guidelines;[232]
- The Bill should allow persons aggrieved by the conduct of covert surveillance to have access to a civil remedy – complaints made to Privacy NSW suggest that the criminal prosecutions model in the Workplace Video Surveillance Act 1998 does not provide for effective sanctions.[233]

8.3.2 Australian Privacy Foundation

The Australian Privacy Foundation (APF) states that the Bill is 'a step forward in terms of improving employee privacy while also balancing employers' interests in preventing unlawful behaviour in the workplace.'[234] However, APF submits that 'the Bill has several key deficiencies, the most significant of which is the failure to regulate the conduct of notified (overt) surveillance. We suggest that both employees and employers

---

[228] Privacy NSW, *Submission on the Workplace Surveillance Bill 2004 Exposure Draft,* 20 August 2004, p 2.

[229] Ibid, p 3.

[230] Ibid, p 3.

[231] Ibid, p 4

[232] Ibid, p 5.

[233] Ibid, p 6.

[234] Australian Privacy Foundation, *Submission to the NSW Attorney General's Department Exposure Draft Workplace Surveillance Bill 2004,* August 2004, p 1.

would benefit from a Bill which provided greater clarity in [that] area.'[235] In relation to the non-regulation of overt surveillance, APF states, 'the reality for many employees is that they will continue to have no choice about whether or not they are to be subject to surveillance in the workplace, and how surveillance information may be used.'[236] APF summarises other concerns about the Bill as follows:

> The rigid dichotomy between 'notified' and 'covert' surveillance, and the dichotomy between when an employee is or is not 'at work', are concepts which we do not believe will translate easily into the real world. There is a risk that employers who are trying to 'do the right thing' will nonetheless find themselves in breach of the law and facing criminal sanctions…
>
> We have also identified several key loopholes in the Bill, which would allow employers to conduct covert surveillance of employees while they are not at work, and may also conduct covert surveillance of clients and visitors, even in particularly private areas such as toilets and changerooms. Furthermore, we believe that the Bill provides inadequate protection for employees against the conduct of covert surveillance by an employer who has not obtained the requisite magistrate's authority, and provides little protection against the misuse of any information obtained as a result of such unauthorised and covert surveillance.
>
> We are also disappointed that the enforcement model proposed in this Bill follows that of the existing Workplace Video Surveillance Act, despite evidence of the failure of that Act, with no prosecutions in over five years despite evidence of widespread non-compliance. We propose an alternative model.[237]

The alternative model proposed includes additional powers and funding for the NSW Privacy Commissioner to investigate and prosecute breaches of the covert surveillance provisions; and a civil complaints model for non-compliance with the Act.[238] APF also notes that 'the Bill does not deal with all workplace surveillance issues. For example the difficult issue of alcohol and drug-testing.'[239]

8.4 Employer/business organisations

8.4.1 NSW State Chamber of Commerce

The State Chamber of Commerce states that the Bill 'is an unnecessary and costly impost on business. The Bill…represents an attempt by the NSW Government to impose mandatory and costly regulations on all businesses to limit the actions of a few rogue elements.'[240] The State Chamber argues, 'legislation of this nature is unnecessary,

---

[235] Ibid, p 1.

[236] Ibid, p 12. See also p 3.

[237] Ibid, p 12.

[238] Ibid, p 10-11.

[239] Ibid, p 1. As to alcohol and drug testing in the workplace, see below at paragraph 10.3.3.

[240] NSW State Chamber of Commerce, *Submission on the Workplace Surveillance Bill 2004,* 19 July 2004, p 1.

as electronic monitoring is not as widespread as many might suppose.'[241] The submission also outlines cost consequences for businesses in NSW:

> A number of small and medium businesses may be forced to engage IT professionals to assist them in meeting the notice requirements of the Bill…In addition, technical advice…suggests some systems are incompatible with the 'pop-up' system being suggested as the notification method. This means some businesses will be required to buy new systems. Government restrictions…may simple lead many small businesses to implement a total ban on the personal use of IT facilities in the workplace.[242]

The Chamber also states, 'the compliance requirements of the Bill represent an administrative nightmare for any business that operates outside of NSW. A business will be required to implement a specific policy for NSW, while inter-state staff will be on a different system.'[243] The State Chamber also raises concerns about the prohibition on blocking the accessing and delivery of union material. The submission states that this the Bill goes beyond right of entry provisions in the *Industrial Relations Act*. It also notes that there were very few cases of employers trying to block union emails; and therefore there is 'little logic in implementing another layer of regulation.'[244]

In conclusion, the Chamber submits, 'unfortunately, the impact of the Bill, if implemented, would be far reaching, effecting business operations and may result in the limiting of employee access to IT facilities. We believe that written notice within a staff handbook or employment contract about the monitoring of electronic messages is a far less costly and more practical way of addressing the issue…'[245]

8.4.2 Australian Business Limited[246]/Australian Business Industrial

The joint submission by these organisations states:

> The Exposure Draft does not adequately address the interests of employers and their need to manage and oversee the activities of employees in the workplace. In addition thousands of small businesses would incur additional non-business costs by attempting to comply with the extensive requirements contained in the proposed legislation.
>
> Further, decisions in relation to employee use of email or internet to pursue personal interests or otherwise should be made at the workplace level between the employer and employee. It is not practical or possible to encapsulate within legislation the multitude of arrangements that currently exist between employees and their employers in terms of internet/email usage or the use of other company assets…that may have some form of surveillance device attached.[247]

---

[241] Ibid, p 1.

[242] Ibid, p 2.

[243] Ibid, p 2.

[244] Ibid, p 2.

[245] Ibid, p 2.

[246] Formerly known as the NSW Chamber of Manufacturers.

[247] Australian Business Industrial, *Submission on Exposure Draft Workplace Surveillance Bill*

The submission also argues that state legislation is inappropriate:

> Whereas camera surveillance does not usually raise cross-border issues computer surveillance does, as may tracking surveillance. In both these cases, but particularly in the case of computer surveillance, ABI opposes single state legislation. To the extent that legislation is required it should be nationally consistent. This outcome can be achieved in more than one way.
>
> ABI is also concerned that complying with diverse and potentially overlapping federal and state regulatory requirements concerning the sorts of workplace surveillance contemplated in the draft bill as well as other competing (and sometimes conflicting) workplace legislation results in unproductive efforts, reduces competitiveness and potentially reduces compliance.[248]

In conclusion, the submission suggests that the government should consider a Voluntary Code of Practice rather than introducing legislation. This would provide a way of publicising the question of an appropriate balance between employers' needs and employees' expectations of privacy as well as providing an opportunity to assess the practicability of the measures struck in the code.'[249] The submission also raises a number of specific concerns about the content of the Bill:

- The definitions of tracking and computer surveillance are too broad and catch activities or devices not used for the purpose of surveillance;
- Employers should not be required to obtain authorisation to conduct covert computer and tracking surveillance – unlike video surveillance these other two technologies are utilised for different purposes and means;
- If authorisation is required, employers should be able to obtain it in wider circumstances such as serious misconduct justifying dismissal;
- The requirement that a Nominated Licensed Security Officer oversee the surveillance should not be extended to computer and tracking surveillance. It would be less costly and more practical for an employer to designate an employee in the IT section of the business to oversee such surveillance;
- Employers should only be obliged to take all reasonable steps to provide employees with a general policy (either written or by computer) stating surveillance of email and internet may occur from time to time;
- It is onerous to require employers to place a sign near every computer and/or to ensure the policy appears every time the employee logs on;
- Similarly, it is impractical to require employers to affix signage to every business asset that may contain some form of tracking device;
- There are serious software and resourcing problems associated with accurately identifying emails that fall within the requirements of the Bill in terms of notifying non-delivery to employees.
- The prohibition on blocking delivery of emails containing industrial information should be removed, or amended to allow blocking of emails that could result in (1) an employee being intimidated; (2) a detrimental

---

2004, p 7.

[248] Ibid, p 8.

[249] Ibid, p 9.

impact on the operations, profitability or efficiency of the employer or of a supplier or customer; (3) a breach of the employer's email policy;

- The increase in penalties for contraventions from those currently in the Workplace Video Surveillance Act has not been justified and is opposed.

In support of its objection to the prohibition against blocking emails containing industrial information, ABI's submission states:

> ABI members have reported instances of employees utilising work email to incite industrial action against their own employers and/or suppliers or customers of the employer. This action can have an adverse impact on the operations of employers, their customers and suppliers. It would not be appropriate for business to be obligated to allow employees to use company time and assets to incite industrial action or industrial problems that adversely impact on the employer's operations.[250]

8.4.3 Australian Retailers Association NSW

The Australian Retailers Association NSW (ARA), which is primarily concerned about restrictions on video surveillance, states:

> The ARA maintains the position it held when the Workplace Video Surveillance Act 1998 was first introduced – that is, utilisation of surveillance should not be controlled by legislation and that a system of self-regulation, whether through an industry Code of Practice or an agreed set of Principles or Guidelines, is the most appropriate method of regulation.[251]

The ARA's primary objection relates to the requirement to seek approval from a magistrate in order to conduct covert surveillance, which it says is 'unduly onerous.' It says that before the introduction of this legislation, the retail industry responsibly used covert video surveillance – in accordance with a Code of Practice – and it was only used as a last resort.[252] In relation to applications for authorisation, the ARA states:

> The Bill requires retailers to justify why they are seeking a covert surveillance authority. The problem retailers have…is that in many cases while they are aware that there is some form of illegal activity…going on in their business, they are not entirely sure what is happening, who is doing it, or what the extent of the problem is. This makes it very hard for an employer to justify why they should be issued with an authority.[253]

The ARA asks, 'if a retailer is unable to get an authority, and the Police will not or cannot help them where does this leave them? At what point has the employer lost enough, whether it is stock or money, to justify the issuing of an authority?'[254] The ARA

---

[250] Ibid, p 15.

[251] Australian Retailers Association, *Submission to the Attorney General's Department on the exposure draft Workplace Surveillance Bill 2004,* p 1.

[252] Ibid, p 3 and see also p 1.

[253] Ibid, p 5.

[254] Ibid, p 6.

also refers to extensive time delays associated with getting a permit.[255] In addition, the ARA also submits that the Act does not make 'adequate provision for the use of covert video surveillance to detect theft or other crimes by parties external to the business.'[256] In conclusion, the ARA submits:

> Retailers recognise that workplace surveillance is potentially intrusive and that for this reason it needs to be regulated in some way. Retailers are not seeking to be able to use surveillance, whether overt or covert, carte blanche. What they are seeking is that the fundamental right of retailers to protect their property is recognised and that any regulation of surveillance reflect the realities of these matters.
>
> Any reform in this area should focus on monitoring rather than approval. Instead of requiring the prior judicial approval before undertaking covert surveillance activity the court could institute a process whereby it monitors the incidence of covert surveillance to ensure that such surveillance is conducted in accordance with an agreed set of principles.[257]

8.5 Other stakeholders

8.5.1 Institute of Mercantile Agents

The IMA submits that the 'wrong party is being nominated under the…Bill to act in the oversighting of a covert surveillance operation.'[258] The IMA believes that oversight should be undertaken by a Private Inquiry Agent, licensed under the Commercial & Private Inquiry Agents Act, as amended – instead of by the holder of a Class 2C licence under the *Security Industry Act 1997*.[259] The 'oversight and conduct of the surveillance operation would then be in the care and control of an experienced, qualified and competent investigator rather than with a technician who knows the intracies of power, voltage, inductance…etc' but who is not competent to act as an investigator.[260] The IMA also argues that the maximum penalties for breaches of the proposed Act are not sufficient to deter unscrupulous employers (and licensed security operators) from installing covert cameras in the workplace without obtaining an authority - the IMA states 'anecdotal accounts within the industry suggest that…these practices are currently rife.'[261] The IMA is also concerned that the Bill would restrict surveillance of employees for the purpose of investigating sick leave and workers compensation claims.[262]

---

[255] Ibid, p 3.

[256] Ibid, p 4.

[257] Ibid, p 6.

[258] IMA, *Response to NSW Workplace Surveillance Bill 2004,* July 2004, p 6.

[259] Ibid, p 5.

[260] Ibid, p 6.

[261] Ibid, p 7.

[262] Ibid, p 8-9. See p 10-14 for comments on specific provisions of the Bill.

9. WORKPLACE SURVEILLANCE LAWS ELSEWHERE

9.1 Introduction

This section outlines legislative or other regulatory measures, specifically relating to workplace surveillance, which have been introduced or proposed in other jurisdictions. It will also refer briefly to privacy legislation in other jurisdictions. No attempt is made to present a summary of legal position vis-à-vis workplace surveillance in each jurisdiction as that would necessitate looking at any constitutional rights, common law, technology specific regulation and industrial relations laws.[263]

9.2 Australia

9.2.1 Victoria's recent law reform proposal

As noted in the introduction, on 23 September 2004, the Victorian Law Reform Commission published an *Options Paper* on *Workplace Privacy*, which proposed two alternate options for reform. In putting the case for reform, the Commission said:

> This [paper] has revealed important concerns employers have in running and managing their businesses. It has also revealed the significant gaps that exist in the protection of workers' privacy in Victoria and the difficulties of taking third-party issues into account. It seems clear that the status quo is not adequate in either protecting workers' privacy or addressing employer concerns.
>
> …The current regulatory regime is unable to account for the particular environment within the workplace and fails to provide practical assistance to employers and workers in the onerous task of adequately balancing these issues.
>
> We believe reform of this area is essential to provide the necessary regulatory guidance to both employers and workers, through mechanisms that allow for a proper evaluation and balancing of these complex interests. That is why reform to the status quo is required and why we advocate a new regulatory regime.[264]

In considering options for reform, the Commission stated three goals:

- To ensure minimum standards of privacy protection for workers without unduly limiting the ability of employers to run their business;
- To protect worker privacy in a way that is sufficiently flexible to accommodate the needs of different workplaces;
- To put in place mechanisms that ensure compliance with the selected regime.[265]

---

[263] Other publications discussing workplace surveillance in other jurisdictions include: Privacy International, *Privacy and Human Rights 2003: An International Survey of Privacy Laws and Developments*, September 2003. See specific sub-section on "workplace privacy" in the section entitled "Threats to Privacy" (see also Country reports)`. In addition, see the NSW Privacy Committee report, Note 22, p 81ff but note that that it outlines the position as at 1995. See also International Labour Organisation, 'Workers' Privacy: Part II Monitoring and surveillance in the workplace (1993), *Conditions of Work Digest,* Vol 12, No. 1.

[264] VLRC Options Paper, Note 88, p 93.

[265] Ibid, p xiii.

The Commission dismissed a number of lighter regulatory options including: (1) self-regulation involving publication of best practice guidelines by a body such as the Victorian Privacy Commission, complemented by education; (2) incentive based schemes, eg making workplace privacy 'best practice' a requirement for tendering for government work; (3) Sanctions involving reputation, eg disclosing names of employers that have not adopted good workplace privacy practices.[266] The Commission ultimately proposed the following two options for regulating workplace surveillance and testing:

Option 1: Legislation would require employers to seek authorisation in advance from a regulator before undertaking either some or all surveillance or testing.[267] This would apply to both overt and covert surveillance. Features of this option could include:

- A process for notifying workers that an application for authorisation has been submitted to the regulator (with the exception of certain covert practice applications);
- A process for workers to be properly consulted about the application (either by the regulator or the employer);
- Powers for the regulator to conciliate or hear disputes about the application between the employer and workers;
- A complaints-based mechanism;
- Powers for the regulator to conciliate or investigate worker complaints, and to enforce the Act and authorisation conditions by having an ability to audit employers and issue compliance notices;
- An educative role to be fulfilled by the regulator.[268]

Option 2: Legislation would require employers to comply with a set of principles on how they implement and conduct surveillance and testing. The 'principles would be general in nature and address matters such as the purpose a practice is used for and communication with workers about the practice. This is similar to the information privacy legislation approach...' Other features of this option could include:

- A code or codes produced by the regulator (or an equivalent developed by industry and approved by the regulator) to provide practical details on how employers can comply with the principles in relation to particular practices – the codes would not be binding, but compliance with a code could be used by employers to defend themselves against worker complaints;
- A complaints-based mechanism with powers for the regulator to conciliate or investigate complaints about breaches of the principles;
- Powers for the regulator to issue compliance notices for serious breaches of the Act;
- An educative role to be fulfilled by the regulator.[269]

---

[266] Ibid, p 98-102. Note, the Commission did not look at reforms that directly regulate the providers of surveillance technologies, as this was outside the terms of reference. (p 102)

[267] As to the matters that the employer would need to address in an application for authorisation, see ibid, p 104. Note also 'Employers could either submit applications themselves or, if a practice is an industry-wide one, an employer association or industry body could submit the application on behalf of its members.' (p 104).

[268] Ibid, p xiv.

[269] Ibid, p xiv.

The Options compared: The Commission states, 'Option 1 would require the authorisation of all or some workplace surveillance…and testing practices before they are implemented, whereas Option 2…is reliant on a complaints trigger. Option 1 would have some resource implications for the government and, depending on the extent and use of practices, for employers. But it would provide greater certainty about acceptable and unacceptable practices for employers and workers than Option 2. It also has a more stringent enforcement regime than Option 2. Option 2 would put more direct responsibility on employers and may require less resources.'[270]

9.2.2 Other states and territories in Australia

No other state or territory has specific workplace surveillance legislation. However, note that an October 2002 *Report on the Review of the South Australian Industrial Relations System* recommended that workplace surveillance legislation be developed in that state.[271] In addition, Western Australia and the Northern Territory (and Victoria), have introduced general surveillance devices legislation, which regulates the use of listening devices, optical surveillance devices and tracking devices, including in the workplace.[272] In all three jurisdictions, the prohibition against using listening and optical devices only applies to the monitoring of 'private conversations' or 'private activities.'[273] The Victorian Law Reform Commission states that 'the definitions of [these phrases] are restrictive. As a result, in most situations, workers will be unable to rely on the [legislation] to protect them against surveillance in the workplace.'[274] Also, the prohibition against using a surveillance device does not apply if a person under surveillance has consented to it, expressly or impliedly.[275]

---

[270] Ibid, p xv.

[271] Stevens G, *Report of the Review of the South Australian Industrial Relations System,* report prepared for the Hon MJ Wright, South Australian Minister for Industrial Relations, October 2002, p 69-70. In a private communication with SA Attorney General's Department on 12/10/04, the writer was informed that the Attorney General was monitoring the situation in NSW.

[272] *Surveillance Devices Act 1998 (WA), Surveillance Devices Act 1999 (VIC), Surveillance Devices Act 2000 (NT).* The Northern Territory Act regulates the use of data surveillance but the application of the Act to computer surveillance in the workplace is unclear.

[273] See for example *Surveillance Devices Act 1998 (WA)*, s 5(1), s 6(1).

[274] VLRC *Options Paper,* Note 88, p 23. For example the Western Australian *Surveillance Devices Act 1998* defines "private activity" to mean any activity carried on in circumstances that may reasonably be taken to indicate that any of the parties to the activity desires it to be observed only by themselves, but does not include an activity carried on in any circumstances in which the parties to the activity ought reasonably to expect that the activity may be observed.'

[275] See for example *Surveillance Devices Act 1998 (WA)* s 5(3)(c), 6(3)(a), 7(1). In the case of tracking devices used to locate an object, it is sufficient to obtain the consent of the person in lawful control of the object. There is some debate about the interpretation of this provision – ie whether it means that the employer's consent is sufficient in the case of a tracking device installed in a vehicle which is owned by the employer. See 'Patrick Corp defends GPS technology', Thompson Privacy Alert, Issue 41 19/3/03, Note 189 above.

9.3 United States

9.3.1 Federal level

There is no specific workplace surveillance legislation at the federal level in the United States but there have been at least two legislative proposals. The first was a Bill entitled *Privacy for Consumers Act,* which was originally introduced in 1991 and then reintroduced in 1993.[276] This Bill has been summarised as follows:

> …the Act would require an employer to provide general notice to employees and prospective employees that the employer engages in workplace monitoring. An employer could randomly monitor new employees without any advance notice of the specific surveillance during the first sixty days of employment. For other employees, the employer would be required to provide individualized notice prior to actual surveillance. This notice would have to state the days and hours when the monitoring would occur and the uses for the data collected. Moreover, if the monitoring involved employee exchanges with customers, the customers would have to be notified of the monitoring…In general employers would be prohibited from randomly monitoring any long-term employee. [The notice requirements would not apply] if the employer "has a reasonable suspicion" that the employee's action "violates criminal or civil law or constitutes wilful gross misconduct." Employers could also monitor employee activity if the basis of the investigation was possible employee abuse of workers' compensation.
>
> Electronic monitoring of bathrooms, locker rooms and dressing rooms would be generally prohibited. In addition, the Act would limit access to monitoring records, and would afford an employee the opportunity to review her records. Moreover, an employer would not be able to evaluate work performance or set production goals or quotas solely on the basis of information acquired by monitoring employees.[277]

Each violation of the Act would be punishable by a $10,000 civil fine and employees could pursue private actions to seek equitable relief.[278] A wide variety of business organisations opposed the Bill and it did not proceed from the committee stage.[279]

A more recent proposal entitled *The Notice of Electronic Monitoring Act* (NEMA) was introduced into the House of Representatives and the Senate in 2000.[280] NEMA would 'not ban or even limit electronic monitoring in the workplace…Instead [it would] merely requir[e] that employers give notice to employees that electronic monitoring will take place.'[281] Employers would need to give employees notice prior to monitoring an

---

[276] Lane, Note 81, p 255.

[277] Flanagan J, 'Restricting Electronic Monitoring in the Private Workplace', (1993-94) 43 *Duke Law Journal* 1256 at1271-72.

[278] Ibid, p 1272 (footnote 124).

[279] Lane, Note 81, p 255.

[280] Watson N, 'The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?', 54 (2001-02) *Federal Communications Law Journal* 79 at 80.

[281] Ibid, p 92.

electronic communication or computer usage.[282] Notice would also need be given on an annual basis and if there were any material changes to monitoring practices.[283] Failure to comply with the Act would not be an offence but would give rise to a civil action.[284] Damages would be limited to $20,000 per employee; and an employer's maximum liability for a violation of the Act would be $500,000.[285] There would be an exception to the notice requirements if an employer had reasonable grounds to believe that (i) an employee is engaged in conduct that violates the legal rights of the employer or another person; (ii) the conduct involves significant harm to the employer or such other person and (iii) monitoring may produce evidence of such conduct.[286]

The House Judiciary Committee's Subcommittee on the Constitution held hearings on the Bill in September 2000 but the NEMA Bill did not proceed.[287] According to one commentator, 'employer groups succeeded in getting the Judiciary Committee to pull the bill from further consideration. They cited a potential increase in litigation and more work for human resources professionals in complying with NEMA.'[288]

9.3.2 State level

It is beyond the scope of this paper to undertake a comprehensive survey of US states. However, as at 2000, a *non*-exhaustive survey of states in the US found that only one state, Connecticut, had 'an employee monitoring statute on its books.'[289] Several other states 'had considered electronic monitoring legislation during the 1999-2000 legislative sessions, but none of the bills were enacted into law.'[290] The legislation in Connecticut and legislation recently passed in California are outlined below.

---

[282] The notice would need to be 'clear and conspicuous…in a manner reasonably calculated to provide actual notice. The notice would need to describe (1) the form of communication or computer usage that will be monitored; (2) the means by which such monitoring will be accomplished and the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored; (3) the frequency of such monitoring; and (4) how information obtained by such monitoring will be stored, used or disclosed: clause 2711(b).

[283] Clause 2711(a)(2), (3).

[284] Clause 2711(a), (d)

[285] Clause 2711(d)(3)(A),(B).

[286] Clause 2711(c).

[287] See *Thomas Legislative Information on the Internet* (a service of the Library of Congress) at: http://thomas.loc.gov/home/thomas.html

[288] Watson N, Note 281, p 80.

[289] See Morrissey C.M, 'Electronic Monitoring in the Workplace', *CongressLine*, 4 September 2000. Accessed at: http://www.llrx.com/congress/090400.htm. See also Gray Carey, 'Electronic Communications Privacy Issues', online information resource accessed at: http://www.gcwf.com/gcc/GrayCary-C/Practice-A/Privacy/ecompriv.doc_cvt.htm?COM=P

[290] Ibid.

Connecticut: The legislation[291] requires that 'each employer who engages in any type of electronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur.'[292] The employer may conduct monitoring without prior notice if the employer has reasonable grounds to believe that employees are engaged in conduct which (a) violates the law, (b) violates the legal rights of the employer or other employees, or (c) creates a hostile workplace environment; and if electronic monitoring may produce evidence of this misconduct.[293] The Labor Commissioner may levy a civil penalty for a breach of the Act.[294]

California: In August 2004, the Californian legislature passed a Bill on electronic monitoring in the workplace.[295] The *Electronic Privacy Bill* 'requires employers to give employees a one-time written notice if they plan to read e-mail, track Internet use, or use other electronic devices to monitor employees on or off the job. The bill requires employers to explain what will be monitored -- for example employee e-mail content or location based on a GPS-chipped cell phone or car -- but doesn't require employers to tell employees each time they're about to read an e-mail or check an employee's whereabouts.'[296] Governor Schwarzenegger has until September 30th to sign or veto the Bill, or let it become law without his signature.[297] Three similar e-mail privacy bills in 1999, 2000, and 2001, were vetoed by former-Governor Gray Davis.[298]

[291] Public Act No 98-142, which has the long title 'An Act requiring notice to employees of electronic monitoring by employers.'

[292] Section (b)(1). This section also provides that 'each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employee may engage in. Such posting shall constitute prior written notice.'

[293] Section b(2).

[294] Section (c).

[295] California E-Mail Privacy Bill Passes Legislature, Heads to Governor's Desk', *Government Technology*, 27/8/04. The Bill passed the Senate by a 23-11 vote.

[296] Ibid.

[297] Ibid.

[298] Ibid.

9.4 United Kingdom

The UK *Data Protection Act 1998* implements the 1995 European Union *Data Protection Directive*[299] and 'places responsibilities on any organisation to process personal information that it holds in a fair and proper way.'[300] In June 2003, the UK Information Commissioner, who oversees the Act, published Part 3 of the *Employment Practices Data Protection Code*, entitled *"Monitoring at Work*" together with *Supplementary Guidance,* and *Guidance for Small Businesses.*[301] The stated purpose of Part 3 of the Code on "Monitoring at Work" is:

> …to help employers comply with the Data Protection Act and to encourage them to adopt good practice. The Code aims to strike a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. It does not impose new legal obligations.[302]

The Information Commissioner explains that the Data Protection Act 'does not *prevent* monitoring. Indeed in some cases monitoring might be necessary to satisfy its requirements. However, [the Act requires that] any adverse impact of monitoring on individuals must be justified by the benefits to the employer and others.'[303] Part 3 of the Code is 'designed to help employers determine when this might be the case.'[304]

Part 3 of the Code contains 'Good Practice Recommendations' which 'may be relevant to either larger or small employers, but they primarily address activities that are likely to be undertaken by those involved with systematic monitoring. As such they are most likely to be relevant to larger organisations.'[305] The recommendations are organised under the following headings: (1) Managing data protection; (2) General approach to monitoring; (3) Monitoring electronic communications; (4) Video and audio monitoring; (5) Covert monitoring; (6) In-vehicle monitoring; (7) Monitoring through information from third parties. A summary of the recommendations for each topic is

---

[299] See below at paragraph 9.5.1

[300] UK Information Commissioner, *The Employment Practices Data Protection Code, Part 3 Monitoring at Work,* June 2003, p 4.

[301] The Code was issued in accordance with a provision in the *Data Protection Act* which 'requires [the Commissioner] to promote the following of good practice, including compliance with the Act's requirements…and empowers him, after consultation, to prepare Codes of Practice giving guidance on good practice.' There are four parts to the Code. Part 1 deals with "Recruitment and Selection" and Part 2 deals with "Employment Records". Part 4 will deal with "Information about Workers' Health". The Code and the Guidance documents are available from the Information Commissioner's website: http://www.informationcommissioner.gov.uk/eventual.aspx?id=437

[302] Part 3 of the Code, supra, p 3 (emphasis added). See also benefits of the Code at p 4-5.

[303] Ibid, p 15.

[304] Ibid, p 12.

[305] Ibid, p 20.

presented in **Appendix 3** to this paper. Outlined below are the five core principles upon which the general approach to monitoring (point 2) is based:

- It will usually be intrusive to monitor your workers;
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment;
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered;
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified;
- In any event, workers' awareness will influence their expectations.[306]

9.5 Europe

9.5.1 European Union (EU)

Existing EU legislation: Data Protection Directive 95/46/EC

There is currently in force a 1995 *Data Protection Directive 95/46/EC* of the European Parliament and Council, which is concerned with 'the protection of individuals with regard to the processing of personal data.'[307] Member States were required to implement this directive by 1998. In 2001, a EU Data Protection Working Party published an Opinion on the *Processing of Personal Data in the Employment Context*.[308] In relation to workplace surveillance, the Working Party expressed the following opinion:

> Data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, Internet access, video cameras or location data.
> …
> - **Any monitoring…must be a proportionate** response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers.
> - **Any personal data** held or used in the course of monitoring must be **adequate, relevant and not excessive for the purpose for which the monitoring is justified.** Any monitoring must be carried out in the least intrusive way possible…
> - **Monitoring…must comply with transparency requirements of Article 10.** Workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair proceedings…[309]

[306] Ibid, p 24.

[307] The Directive is located on the European Commission website at: http://europa.eu.int/comm/internal_market/privacy/law_en.htm

[308] Article 29 – Data Protection Working Party, *Opinion 8/2001 on the processing of personal data in the employment context,* adopted on 13 September 2001.

[309] Ibid, p 24-25 (original emphasis).

In May 2002, the Working Party published a *Working Document on the Surveillance of Electronic Communications in the Workplace*.[310] In that document the Working Party states, 'compliance with all [of] the following principles [derived from the *Data Protection Directive*] is necessary for any monitoring activity to be lawful and justified.'[311] Those principles are: (1) Necessity; (2) Finality; (3) Transparency; (4) Legitimacy; (5) Proportionality; (6) Accuracy and Retention of data; and (7) Security. The Working Document discusses each of these principles in the context of monitoring electronic communications, eg in relation to the transparency principle, it states:

> This principle means that an employer must be clear and open about his activities. It means that no covert e-mail monitoring is allowed by employers except in those cases where a law in the Member State under Article 13 of the Directive allows for that. This is most likely to be the case where specific criminal activity has been identified…or in those cases where national laws providing the necessary safeguards, authorise the employer to take certain actions to detect infractions in the workplace.[312]

EU initiative on protection of workers' personal data[313]

In August 2001 the European Commission launched a first stage consultation of the EU-level social partners[314] on the protection of workers' personal data. Social partners were asked to consider whether the existing Directive adequately addressed the protection of workers' personal data and whether it was advisable that the EU take an initiative in this field, including in relation to monitoring and surveillance in the workplace.

The responses to the first stage indicated that there was 'widespread consensus among the social partners as regards the importance of the question of personal data in the employment context taking into account notably the socio-economic and technological developments of recent years.'[315] However there was a clear divergence between the responses of employers' organisations and those of workers' organisations. Employers

[310] Article 29 – Data Protection Working Party, *Working Document on the surveillance of electronic communications in the workplace*, adopted 29 May 2002.

[311] Ibid, p 13 (emphasis added).

[312] Ibid, p 14.

[313] Except where otherwise indicated the information in this section is taken from Delbar C et al, *New Technology and Respect for Privacy at the Workplace*, Institut des Sciences du Travail, 12 August 2003. This document can be accessed at the European Industrial Relations Observatory online: http://www.eiro.eurofound.eu.int/2003/07/study/tn0307101s.html

[314] The European Commission website provides the following description of "social partners" (in part): 'The Commission is required to consult various social partners when it wants to submit proposals in this field. This social dialogue occurs via the three main organisations representing the social partners at European level:

- the European Trade Union Confederation (ETUC),
- the Union of Industries of the European Community (UNICE),
- the European Centre for Public Enterprise (CEEP).'

[315] Institut des Sciences du Travail, supra, p 7 of 25.

did not see any need for another Directive. In their view, the existing Directive was adequate and sufficient to ensure a high quality protection of workers' personal data. On the other hand, employees' organisations supported an EU Directive.

In October 2002, the Commission 'launched a second stage consultation, this time on the content of an envisaged proposal in this area - having concluded that it is advisable that a framework of employment-specific rules on data protection should established at EU level - giving the social partners the opportunity to negotiate an agreement on the issue and thus forestall a proposed Directive. The second-stage consultation was more concrete and detailed, suggesting a new framework of principles and rules on data protection at the workplace.'[316] The Commission proposed a framework that would build on the principles of the *Data Protection Directive* and would particularise and complement this Directive as regards protection of personal data in the employment context.[317] In relation to workplace surveillance, the Commission suggested that the following principles form part of the European framework under discussion:

- The workers' representatives should be informed and consulted before the introduction, modification or evaluation of any system likely to be used for monitoring/surveillance of workers;
- Prior check by a national data protection supervisory authority should be considered;
- Continuous monitoring should be permitted only if necessary for health, safety, security or the protection of property;
- Secret monitoring should be permitted only in conformity with the safeguards laid down by national legislation or if there is reasonable suspicion of criminal activity or other serious wrongdoing;
- Personal data collected in order to ensure the security, control or proper operation of processing systems should not be processed to control the behaviour of individual workers except where the latter is linked to the operation of these systems;
- Personal data collected by electronic monitoring should not be the only factors in evaluating workers' performance and taking decisions in their regard;
- Notwithstanding particular cases, such as automated monitoring for purposes of security and proper operation of the system (eg viruses), routine monitoring of each individual worker's e-mail or internet use should be prohibited. Individual monitoring may be carried out where there is reasonable suspicion of criminal activity or serious wrongdoing or misconduct, provided that there are no other less intrusive means to achieve the desired purpose (eg objective monitoring of traffic data rather than of the content of e-mails, or preventive use of technology);
- Prohibition in principle on employers opening private e-mail and/or other private files, notably those explicitly indicated as such, irrespective of whether use of the work tools for private purposes was allowed or not by the employer. In particular, private e-mails/files

[316] Ibid, p 7 of 25.

[317] See European Commission, *Second Stage Consultation of Social Partners on the Protection of Workers' Personal Data,* p 9. Accessed at http://europa.eu.int/comm/employment_social/news/2002/oct/data_prot_en.pdf

> should be treated as private correspondence. Secrecy of correspondence should not be able to be waived with a general consent by the worker, in particular upon conclusion of the contract of employment; and
>
> - Communication to occupational health professionals and representatives of workers should receive particular protection.[318]

An August 2003 report on the progress of the EU consultation states, 'following the responses of the social partners to the second round of consultations, it appears that [the] opportunity [to reach an agreement] has been rejected, and the Commission is planning a draft Directive in 2004 or 2005 (according to its June 2003 mid-term review of social policy agenda).'[319] A draft Directive has not yet been released.

9.5.2 European States

A September 2003 publication entitled *New technology and respect for privacy at the workplace*, by the Institut des Sciences du Travail, looks in particular at the relationship between internet/email use at work and respect for privacy.[320] The comparative study examines 'the European and national legal framework on privacy at work, data protection, and workplace internet/mail use; guidelines and codes of conduct in this area; the views and activities of the social partners; and the extent to which collective bargaining deals with such topics.'[321] The publication summarises the legal and regulatory framework amongst European States as follows:

> Measures that…regulate the monitoring and surveillance of workers' use of new technology are primarily based on a body of law in each country, made up of: general (often constitutional) provisions relating to respect for privacy and the secrecy of correspondence; personal data protection provisions; and, less extensively, workplace-specific privacy provisions. While general privacy and secrecy provisions may often be assumed to cover internet/e-mail use, this is rarely explicit. With regard to personal data protection, most national measures implement the EU Directive (95/46/EC) on the issue and thus have implications for the employment relationship. However, specific legislation applying data protection rules to the employment context is rare, with the main example being Finland (plus France, Greece and, to some extent, Portugal).
>
> Beyond data protection, some general protection of workers' privacy is provided by law in countries such as France, Belgium (a national collective agreement), Italy and Portugal. The specific issue of video surveillance and monitoring at the workplace is regulated by legislation in countries such as Belgium (national collective agreement), Denmark and France**.** In some cases, works councils or other workplace employee representatives have powers over the introduction and/or use of monitoring equipment. Agreement or co-determination is required in Austria, Germany, Luxembourg, the Netherlands and Sweden while information and/or consultation is required in Belgium, Denmark, Finland, Norway and Spain. Specific legislation on the

[318] Ibid, p 17

[319] Institut des Sciences du Travail, Note 314, p 7 of 25.

[320] Ibid, p 1 (abstract).

[321] Ibid, p 1 (abstract).

monitoring of employees' e-mail and internet use exists only in Belgian (national collective agreement) and, to a lesser extent, Denmark and Germany. New legislation in this area is under debate in countries such as Finland, Germany, Norway and Sweden.

Outside the field of legislation, employer surveillance and monitoring of employees' e-mail and internet use has been the subject of guidance or codes from regulatory authorities in countries such as Denmark, Greece, Portugal and the UK. It is also dealt with in codes of practice and policies drawn up by various employers' organisations or individual employers or proposed by trade unions (eg the UNI code). This is also an issue regulated by the little multi-employer bargaining which relates to employee e-mail and internet use (eg in Belgium, Denmark and Norway) and in company agreements on the matter.[322]

9.6 Hong Kong

In March 2002, the Office of the Privacy Commissioner for Personal Data (PCO) released a *Draft Code of Practice on Monitoring and Personal Privacy Data at Work* for consultation.[323] The development of the draft Code was a response to several factors: (1) it was a recommendation of the Privacy Sub-Committee of the Law Reform Commission in its consultation paper entitled *Civil Liability for Invasion of Privacy* published in August 1999; (2) independent opinion surveys commissioned by the PCO clearly indicated the prevalence of workplace monitoring in Hong Kong; (3) technological developments and reduced costs, notably of monitoring software, made employee monitoring systems affordable to almost all employers.[324]

The Draft Code deals with telephone monitoring, email monitoring, computer usage (Internet access) monitoring and video monitoring.[325] The aim of a Code of Practice would be 'to give practical guidance to the application of the requirements of the [*Personal Data (Privacy) Ordinance*[326]] to employee monitoring involving personal data.[327] The public consultation ended in June 2002 and a report on that consultation was published in December 2003. The result of the report was that the Commissioner

[322] Ibid, p 24 of 25. See also p 25 of this document as to employer and union activity in relation to monitoring of emails and internet in the workplace. As to legislation on workplace surveillance in Finland, see *Act on the Protection of Privacy in Working Life* (2001), which is located at http://www.finlex.fi/pdf/saadkaan/E0010477.PDF.

[323] Office of the Privacy Commissioner for Personal Data, Hong Kong, *Report on the Public Consultation in relation to Draft Code of Practice on Monitoring and Personal Data Privacy at Work*, December 2003, p 4. Note also the Hong Kong *Code of Practice on Human Resource Management*, which was issued in September 2000 and came into effect on 1 April 2001. The latter Code is discussed in Roth P, 'Workplace Privacy, New HK and UK Codes', (2000) 7(6) *Privacy Law and Policy Reporter* 111.

[324] Ibid, p 3.

[325] Office of the Privacy Commissioner for Personal Data, Hong Kong, *A Draft Code of Practice on Monitoring and Personal Data Privacy at Work,* Consultation Document, March 2002, p 8-9.

[326] This Ordinance 'provides for comprehensive control of the collection, holding, processing and use of personal data, including processing personal data used for employment related activities.' (See ibid, p 4).

[327] Ibid, p 4.

would issue a set of "best practice" guidelines on employee monitoring practices' rather than a Code of Practice. This approach was explained as follows:

> The issuing of a set of "best practice" guidelines…is a reasoned approach towards building a self-regulatory framework conducive to the development of best personal data management practices in the workplace. In electing to issue guidelines, the PCO are respecting the views expressed in a majority of submissions. Guidelines offer two possibilities. First, employers may elect to adopt them in the form in which they appear…Secondly, the guidelines offer a model around which employers may tailor an employee monitoring policy that is specific to the needs of the organization. This flexibility provides an incentive for employers to respond voluntarily to the appeal of the guidelines rather than have to submit to the more robust demands of a code of practice. [328]

If the guidelines did not encourage 'a regime that strikes a fair balance between the respective interests of employers and employees', the 'PCO would…initiate a comprehensive review [which] may result in a revision of the guidelines and their issuance as a binding code of practice.'[329] According to the report, the guidelines would be published in 2004.[330] In relation to drafting the guidelines, the report states:

> …the PCO will give particular emphasis on best practice guidance requiring employers to be "transparent" about, and "accountable" for, monitoring practices they engage in the workplace. It is intended that the guidelines should address the data privacy issues arising from the capture of an employee's personal data in the course of workplace monitoring over the duration of an employee's employment. Where employees are subject to workplace monitoring the employer should, at a very minimum, be transparent in terms of workplace monitoring practices. Employees need to be unambiguously informed about the practices and intentions of the employer insofar as the purposes to which their personal data, collected in the process of monitoring, will be used during the period of employment and possibly once employment has ceased.

9.7 New Zealand[331]

There is no legislation or codes of practice specifically regulating workplace surveillance in New Zealand. However, the *Privacy Act 1993* applies to both the public and private sectors and applies in employment contexts. Like the privacy legislation in Australia, the *Privacy Act 1993* sets out a number of Information Privacy Principles that deal with the collection, holding, use and disclosure of personal information. The Privacy Commissioner, which oversees the *Privacy Act*, has issued opinions in relation to specific complaints about the use of *video* surveillance in the workplace.[332]

---

[328] Report on the public consultation (2003), Note 324, p 39.

[329] Ibid, p 40.

[330] Ibid, p 40. Guidelines have not yet been published.

[331] The information in this paragraph was obtained from the Office of the Privacy Commissioner (NZ) as at 26 August 2004.

[332] See case-notes 632 of 1995 and 18302 of 2001. Located on the Privacy Commissioner's website: http://www.privacy.org.nz/top.html. The Privacy Commissioner has also outlined some general pointers on video surveillance. See 'Extract from a letter by the Privacy Commissioner concerning Video Surveillance', obtained from the Privacy Commissioner's office.

9.8 Canada[333]

There is no specific workplace surveillance legislation at the federal level.[334] There are, however, privacy laws that are relevant to workplace surveillance. The *Privacy Act*, which took effect in 1983, applies to employee information in federal government institutions. Since 2001, the *Personal Information Protection and Electronic Documents Act* has applied to personal information about customers or employees that is collected by certain (federally regulated) private sector organisations; and since January 2004, the Act has regulated the collection of personal information by all private sector organisations within a province.[335] Oversight of both Acts rests with the Privacy Commissioner of Canada. The Privacy Commissioner has published on its website a fact sheet on *Privacy in the Workplace*.[336] This document outlines some basic rules for organisations to follow although it is not suggested that failure to follow these rules will result in a breach of the privacy legislation. The rules are:

- The employer should say what personal information it collects from employees, why it collects it, and what it does with it.
- Collection, use, or disclosure of personal information should normally be done only with an employee's knowledge and consent.
- The employer should only collect personal information that's necessary for its stated purpose, and collect it by fair and lawful means.
- The employer should normally use or disclose personal information only for the purposes that it collected it for, and keep it only as long as it's needed for those purposes, unless it has the employee's consent to do something else with it, or is legally required to use or disclose it for other purposes.
- Employees' personal information needs to be accurate, complete, and up-to-date.
- Employees should be able to access their personal information, and be able to challenge the accuracy and completeness of it.[337]

In November 2001 the Privacy Commissioner delivered a speech on *Workplace Privacy in the Age of the Internet*.[338] In relation to monitoring of internet communications, the

---

[333] The information in the following paragraph is taken from three fact sheets on the Canadian Privacy Commissioner's website http://www.privcom.gc.ca/. Those fact sheets are entitled 'Privacy Legislation in Canada', 'Application of the *Personal Information Protection and Electronic Documents Act* to Employee Records' and 'Privacy in the Workplace.'

[334] Research has not been undertaken to determine if there is any provincial legislation specifically regulating workplace surveillance. Note however that the Information and Privacy Commissioner of Ontario published a report in November 1993 entitled *Workplace Privacy, The Need for a Safety Net*, which discussed employee monitoring, testing and employment records and recommended the introduction of workplace privacy legislation. As far as the writer is aware no such legislation was enacted. The report is located on the Ontario Privacy Commissioner's website: http://www.ipc.on.ca/scripts/home.asp?action=31&N_ID=1&P_ID=1&U_ID=0

[335] For a brief discussion of the Act in the context of workplace surveillance, see Geist, Note 68, p 21-25.

[336] See Privacy Commissioner's website at: http://www.privcom.gc.ca/fs-fi/02_05_d_17_e.asp

[337] Ibid.

[338] Radwanski G, *Workplace Privacy in the Age of the Internet*, Excerpt of address to University of Toronto Centre for Industrial Relations and Lancaster House Publishing, 5th Annual Labour

Privacy Commissioner noted that reasons advanced by employers for monitoring and expressed the view that 'directed suspicion-based inquiry is preferable to wholesale monitoring and violation of privacy. A targeted investigation based on reasonable suspicion is not only less privacy-invasive, it's more effective.'[339]

9.9 International Labour Organisation Code of Practice

In 1997, the International Labour Organisation (ILO) published a *Code of Practice on the Protection of Workers' Personal Data.*[340] The Code was adopted by 'a Meeting of Experts on Workers' Privacy of the ILO, convened in October 1996.[341] The Code 'has no binding force, but rather makes recommendations. The Code does not replace national laws, regulations, international labour standards or other accepted standards. It can be used in the development of legislation, regulations, collective agreements, work rules, policies and practical measures at an enterprise level.'[342] The Code contains general principles as well as specific guidelines on the collection, security, storage, use and communication of personal data. The ILO's commentary on the Code summarises the way in which the Code deals with the practice of electronic monitoring:

> While the Code does not exclude monitoring of workers, it clearly restricts it. Monitoring is subject to two conditions. First, it can only be conducted if the workers concerned are informed in advance of the employer's intentions. Consequently, before the monitoring is put into operation, the workers must know the purposes of the monitoring and have a clear idea of the time schedule. Secondly, employers are not at liberty to choose the method and means of monitoring that they consider to be the most suitable for their aims. Rather, employers should take into consideration the consequences for the privacy of workers and give preference to the least intrusive means of surveillance.
>
> In the case of secret or continuous monitoring, the code chooses a definitely more restrictive approach. Continuous monitoring…should be limited to cases in which the surveillance is necessary to deal with specific problems related to health and safety or to the protection of property. As to secret monitoring, it is accepted as long as it is foreseen by specific provisions of national law. It might also be unavoidable in connection with investigations concerning criminal activities or other serious wrongdoings. But the Code stresses that the mere suspicion of such an activity or wrongdoing is not sufficient. Only if, and to the extent that reasonable grounds exist for suspecting such activities or wrongdoings may the employer resort to secret monitoring. An example of serious wrongdoing is sexual harassment…[343]

Arbitration Conference, 2 November 2001.

[339] Ibid.

[340] International Labour Organisation, *Protection of Workers' Personal Data,* Geneva, 1997. This can be accessed online at the ILO website: http://www.ilo.org/

[341] Ibid, p v (preface).

[342] Ibid, p v (preface).

[343] Ibid, p 19. See also Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder flows of personal data.*

10. OTHER WORKPLACE PRIVACY ISSUES

10.1 Introduction

This paper has so far dealt with workplace surveillance but it is relevant to briefly discuss some other current workplace privacy issues.[344] They include biometric identification of employees and testing of current and prospective employees. The latter includes medical and psychological testing, drug and alcohol testing, and genetic testing.

10.2 Biometric identification[345]

Biometrics is the science of identifying people on the basis of physical or behavioural characteristics. Examples of biometric identifiers include DNA, fingerprints, irises, facial characteristics, voice and hand geometry. Biometric identifiers works by comparing the characteristics of a person which are stored in a database to a new sample provided by that person. Biometrics are seen by supporters as a good way of controlling access to buildings, airports and computer networks. They are also seen as a way of reducing 'buddy-punching' in the workplace, i.e. the ability of workers to clock on and off for each other.

According to the Victorian Law Reform Commission (2004), the use of biometrics in the workplace is still rare but it is likely to become more common as the technology becomes more reliable and decreases in cost, particularly with the prevalence of security concerns in the community. The Commission refers to a recent example of a trial of biometrics system by Qantas, which attempted to introduce a finger-scanning system to log baggage handlers clock-on and clock-off times. The trial was opposed by the Transport Workers Union as an invasion of privacy. After negotiations, Qantas agreed to introduce an electronic swipe card time and attendance system. The Labor Council of NSW has submitted that the *Workplace Video Surveillance Act* be extended to cover biometrics, stating:

> This technology is increasingly being used by employers in a range of industries. For example, registered clubs in NSW are utilising finger scanning equipment (also known as a "Bundy Clock") for the purpose of recording employee's start and finishing times, to provide payslip information by computer and for other methods of employee monitoring such as recording which areas of the club premises are being accessed by employees and when they are accessing those areas. Biometrics is another form of surveillance that is completely unregulated…and there is no mechanism to protect the privacy of employees. A number of disputes have already arisen in the club industry with no legal recourse available due to lack of legislation.[346]

The Biometrics Institute has recently issued a draft Code for the Biometrics Industry, which is awaiting approval from the Federal Privacy Commissioner.[347] However, the Code would only bind members of the Institute and membership is voluntary.

---

[344] These issues are sometimes also referred to as workplace *surveillance* issues.

[345] This section is based on VLRC *Options Paper,* Note 88, p 27ff, unless otherwise stated.

[346] Labor Council of NSW Submission, Note 223, p 5.

[347] See Biometrics Institute website: http://www.biometricsinstitute.org/bi/. Accessed on 30 July

10.3 Testing employees

10.3.1 Medical testing

The Victorian Law reform Commission discusses this practice in its 2004 *Options Paper* on *Workplace Privacy*. It notes, 'there is scant statistical evidence available indicating the levels of medical testing within the Australian community.'[348] The paper outlines the circumstances in which an employer could require an existing employee to undertake a medical test; it discusses the content of the test, the relationship between doctor and worker, consent/confidentiality, and the current regulatory framework. The Commission has proposed legislative regulation of workplace surveillance and testing.[349]

10.3.2 Psychological testing

VLRC Report: The Victorian Law Reform Commission also discusses this issue. The Commission states that 'testing in personnel selection and assessment usually involves the employer identifying "relevant knowledge, skill, abilities and other attributes"... Having identified the criteria, selection techniques are adopted that will help "predict" how individuals will perform/behave against the criteria.'[350] The Commission refers to different types of tests including aptitude or ability tests and personality or attribute tests. The Commission also outlines the process of testing including consent/confidentiality, the availability, administration and interpretation of tests, and storage and disclosure of test results. The current regulatory framework is also discussed. As noted above, the Commission has proposed regulation of workplace surveillance and testing.

Media: Some fairly recent articles discuss the use of psychological testing in the workplace and some of the issues involved. For example, an article in the *Sydney Morning Herald* on 27 February 2003 reports on the growth of psychological testing:

> While psychometric testing has been used on a small scale in Australia for decades, its use has spread in recent years, primarily for recruitment but also to aid team-building programs or company restructures.
>
> A range of tests are available to measure a person's potential performance on the job, through an analysis of aptitude, manual dexterity, behavioural style and motivational drivers.
>
> Up to 30 percent of companies in Australia are estimated to use the tests, particularly for white-collar management but increasingly for factory and other blue-collar work.[351]

2004. See also the *Discussion Paper* (September 2003) by the same organisation, which raises some of the issues associated with biometrics, including privacy issues.

[348] VLRC *Options Paper,* Note 88, p 31.

[349] See above at paragraph 9.2.1.

[350] VLRC *Options Paper*, supra, p 38.

[351] 'AWU wants psych test crackdown', *Sydney Morning Herald,* 27/2/03.

The article reports that, according to the managing director of a psychometric testing company, the tests could 'help a company to improve productivity, lower turnover and lessen the risk of accidents by putting the best people into positions.' However, the AWU criticised such testing and was considering a resolution for 'a national policy to protect workers from discrimination and misuse of psychometric testing.'

Another article in *The Age* on 18 March 2004 reported on how psychological testing of candidates for white-collar jobs was moving into blue-collar industries.[352] According to the same managing director as in the previous article, 'testing among the blue collar industry is crucial in assessing an applicant's potential to work safely and produce high-quality work, as well as predicting their reliability and commitment to the role and the organisation.' The article reports that the ACTU was sceptical about the tests, its health and safety coordinator suspecting that 'testing was more about companies selecting people with compliant personalities and preferred social values rather than any real concern for safety.'

10.3.3 Drug and alcohol testing

Nature of Testing and arguments: The nature of testing and the arguments for and against have been summarised very briefly as follows:

> The term 'drug testing' refers to the analysis of biological material to detect drugs or their metabolites in the body. Urine tests are most common…but saliva, sweat and hair can be tested. For alcohol, breath tests are most common.
>
> Drug testing at work takes a variety of forms, including pre-employment testing, random testing of employees and post-accident testing.
>
> The arguments *for* drug testing at work are that there are benefits for safety, efficiency, an organisation's reputation and employee welfare. The arguments are strongest with respect to safety-critical occupations, where drug-induced intoxication can increase the risk of accident.
>
> The arguments *against* drug testing are that it does not have the benefits that are claimed for it, is excessively invasive, may damage relations between employers and employees, and could hamper the recruitment and retention of good staff.[353]

Recent media: An article in the *Sydney Morning Herald* on 26 March 2004 reported that 'Qantas, State Rail and some mining companies face stiff resistance from unions as they press campaigns to have staff screened.' Qantas had planned to 'extend random drug and alcohol testing from pilots and cabin crew to all staff' but after worker complaints had 'delayed the introduction until after presenting unions with new research on different types of breath and urine testing.' Unions were concerned that:

> …testing would lead to a "regime of fear" and breach the privacy of people on prescribed medications.

---

[352] 'Workplace psych tests widen', *The Age*, 18/4/04.

[353] Drugscope et al, *Drug Testing in the workplace: The report of the Independent Inquiry into Drug Testing at Work,* published by the Joseph Rowntree Association, 2004, at p x.

> Unions say companies should not have a right to know that staff are taking prescription drugs, such as heart tablets or anti-depressants, because the information would be recorded and used against them later.
>
> They also have serious doubts about how random the testing would be, and the extent to which tests would be applied across a company to executives.[354]

NSW Privacy Committee report: The NSW Privacy Committee published a report in October 1992, which recommended that 'workplace drug testing should be prohibited by legislation other than when (i) a person's impairment by drugs would pose a substantial and demonstrable safety risk to that person or to other people; and (ii) there is reasonable cause to believe that the person to be tested may be impaired by drugs; and (iii) the form of drug testing to be used is capable of identifying the presence of a drug at concentrations which may be capable of causing impairment.'[355] The report also recommended that 'workplace drug testing that is permitted should be subject to procedural standards, set out in legislation, to protect the privacy interests of those who are tested.'[356]

Victorian Law Reform Commission: The Victorian Law Reform Commission's *Options Paper* (2004) discusses drug and alcohol testing in the workplace[357] and proposes legislative regulation of workplace surveillance and testing.

United Kingdom: In July 2003, an All-Party Parliamentary Drug Misuse Group published a report entitled *Drug Testing on Trial,* which looked at the use of drug testing both in the workplace and at the roadside.[358] The report noted that 'there is no real consensus or clarity about what the aim of drug testing in the workplace is or should be.' The report made a number of recommendations. Most of the recommendations were directed at providing employers and employees with guidance on the issue but the report also suggested that the government consider ways to better control and regulate workplace drug testing. Also, in May 2004, an independent inquiry, initiated by Drugscope with the support from the Joseph Rowntree Association, published a report on *Drug Testing in the Workplace.*[359]

---

[354] 'Random drug tests at frontline of workplace battleground', *Sydney Morning Herald,* 26/3/04. CSee also 'Drugs, grog not the only problems, bosses told', *SMH,* 5/8/03.

[355] The Privacy Committee of NSW, *Drug Testing in the Workplace,* Report No. 64, October 1992, p 2.

[356] Ibid, p 2. It seems that these recommendations were not been implemented. There is currently no general legislative regulation in NSW of drug and alcohol testing in the workplace. But see specific legislation such as *Rail Safety Act 1993 (NSW),* s 61. As to the introduction of drug and alcohol policies in the workplace see NSW Department of Industrial Relations website: http://www.industrialrelations.nsw.gov.au/workplace/practice/pol_proc.html#drug

[357] See VLRC *Options Paper,* Note 88, p 45-53.

[358] This report is located on the drugscope website at: http://www.drugscope.org.uk/uploads/news/documents/FINAL%20Drugtestinginquiry.pdf

[359] Drugscope et al, Note 354 The working party comprised representatives from the following organisations: the Australian Liquor, Hospitality and Miscellaneous Workers Union, the Labor Council of New South Wales, the National Union of Workers, the Employers Federation of New South Wales, the Australian Chamber of Manufactures, New South Wales Branch, the Retail Traders Association of New South Wales, the Registered Clubs Association of New South

10.3.4 Genetic screening and monitoring

In March 2003, the Australian Law Reform Commission published a report entitled *Essentially Yours: The protection of Human Genetic Information in Australia,* which made a number of recommendations for reform, including in relation to the use by employers of genetic information of prospective and current employees.[360] Before outlining those recommendations it is relevant to provide a very brief overview of the topic.

Use of genetic information[361]: Genetic information may be used for genetic screening or genetic monitoring. The former refers to examining the health status of an employee or job applicant for certain inherited traits, disorders or susceptibilities for the purpose of excluding 'high risk' persons from the workplace or providing alternative work that may present fewer risks. Genetic monitoring involves the periodic testing of employees to evaluate genetic damage caused by exposure to a workplace hazard.

Extent to which genetic information is used by employers: The Commission states:

> There is little evidence that Australian employers are currently seeking access to genetic information about job applicants or employees, although there is some evidence of this occurring overseas. However, other forms of workplace testing (such as drug and alcohol testing and psychometric testing) that were unknown some years ago are now becoming relatively commonplace. There is little doubt that the pressures to use genetic information will increase as the reliability and availability of genetic tests increases, and as the cost of testing decreases.[362]

Competing interests[363]: Employers want to ensure that an applicant or employee is able to perform the inherent requirements of the job. Employers also have an interest in ensuring a productive workforce and in limiting unnecessary overheads. Employers may also come under pressure from insurers to conduct genetic testing to minimise compensation claims. Employers may also seek to collect and use genetic information to comply with their duties under occupational health and safety legislation, i.e. to protect the health and safety of employees and third parties. On the other hand, the collection of genetic information raises a number of issues for job applicants and employees, including privacy and discrimination concerns. The public also has an interest in this area, in particular reducing the incidence of workplace injury and disease; ensuring that individuals are not unfairly excluded from work, in public health outcomes, and in protecting privacy in society.

Wales, the Public Employment Office, the Privacy Committee of New South Wales, the Attorney General's Department, and the Department of Industrial Relations (per second reading speech).

[360] Australian Law Reform Commission, *Essentially Yours: The protection of Human Genetic Information in Australia,* Report 96, March 2003.

[361] The following is a very brief summary of the ALRC report, ibid, at p 760-761.

[362] Ibid, p 45-46.

[363] The following is a brief summary of the ALRC report, ibid, p 767-770.

Recommendations in brief[364]*:* The Commission recommended that employers should not collect or use genetic information in relation to job applicants or employees, except in the limited circumstances where this is consistent with anti-discrimination, OH&S and privacy legislation, as amended. Specifically, the ALRC recommended:

- *Anti-discrimination:* federal anti-discrimination legislation should be amended to limit an employer's ability to request and use genetic information;
- *OH&S:* guidelines (and potentially a code of practice) should be developed (a) for the conduct of genetic screening for susceptibility to work-related conditions, (b) for the conduct of genetic monitoring of employees exposed to hazardous substances, (c) for the collection and use of genetic information for the protection of third party safety;
- *Privacy legislation:* the *Privacy Act 1988* should be amended to ensure that employee records are subject to the protections of the Act, to the extent that they contain genetic information;
- *Workers compensation:* a policy should be developed regarding the appropriate use of genetic information in the assessment of claims.[365]

[364] See ALRC Report, ibid, p 67-69.

[365] The Federal Government is considering these recommendations (Private communication with ALRC on 6 October 2004).

11. CONCLUSION

While surveillance at work is as old as work itself[366], the increasing propensity of employers to resort to new forms of electronic surveillance in the workplace has become an important industrial relations issue and a matter of public concern.[367] Employers argue that the use of electronic surveillance has been necessary to protect their legitimate business interests. On the other hand, unions, privacy groups and others argue that regulation is needed to prevent employers using electronic surveillance in a way that denies workers their reasonable expectation of privacy. Some writers in the media and in academia have raised fears of workplaces becoming "Big Brother" like[368] or developing into "electronic sweatshops".[369]

In 1998, the NSW government introduced the legislation to respond to concerns about the use of video surveillance in the workplace. The recent draft Bill proposes to extend that regulatory scheme to computer and tracking surveillance. By requiring employers to give employees notice of surveillance, this scheme addresses the primary concerns of unions and privacy advocates – ie the use of *covert* surveillance - but some argue that the *Bill* should go further and regulate *overt surveillance.* Employers criticised the 1998 legislation for restricting their ability to detect theft and protect their property. They argued that self-regulation was adequate. The draft Bill has attracted similar criticism and strong objections have been raised regarding the substantial costs for businesses of complying with the Bill's notice requirements. Employers also argue that the draft Bill's prohibition on blocking union emails is unreasonable.

The NSW Law Reform Commission's final report on *Surveillance* is due in December. The Victorian Law Reform Commission's recent proposal may also influence the development of laws in NSW. Another important development in this area is the federal government's review of the "employee records" exemption in privacy legislation, which could lead to increased privacy protection for private sector employees.[370] National privacy legislation applies to the workplace in a number of overseas jurisdictions; and in the UK, for example, a Code of Practice has been issued on workplace surveillance to facilitate compliance with privacy laws. Specific workplace surveillance legislation has been introduced in at least two US states and in some European countries.

---

[366] Eivazi K, 'Employees' email privacy and the challenge of advancing technology', (2003) 10(5) *Privacy Law and Policy Reporter* 95 at 98.

[367] Sempill J, 'Under the Lens: Electronic Workplace Surveillance', (2001) 14(2) *Australian Journal of Labour Law* 111 at 111-12.

[368] See for example 'Bigger Brother', *The Weekend Australian*, 7-8/8/99.

[369] See for example Flanagan J, 'Restricting Electronic Monitoring in the Private Workplace, (1993-94) 43 *Duke Law Journal* 1256 at 1257.

[370] See above paragraph 6.4.1.

APPENDIX 1 – COVERT SURVEILLANCE AUTHORISATION

Introduction

This appendix presents a summary of the provisions in Part 3 of the draft *Bill* relating to covert surveillance authorisations. These provisions regulate:

- The issuing of covert surveillance authorities (CSAs) and the carrying out of surveillance under such authorities;
- Access to and destruction of covert surveillance records;
- Restrictions on use and disclosure of such records.

The issuing of CSAs and carrying out of surveillance pursuant to CSAs

Covert surveillance authorities (CSAs): A CSA issued to an employer authorises the covert surveillance generally of any of the employer's employees for the purpose of establishing whether or not one or more particular employees are involved in any unlawful activity at work.[371] A CSA does not authorise the carrying out of covert surveillance (a) for the purpose of monitoring the employee's work performance; or (b) in any change room, toilet facility etc.[372] A CSA is subject to the condition that a nominated licensed security operator (LSO) oversees the authorised covert surveillance[373]; and any other conditions imposed by or under the Act.[374]

Applications for CSAs: An employer or employer's representative[375] may apply to a magistrate for the issue of a CSA.[376] The application must include information about a number of matters including (a) grounds for suspecting that a particular employee is or employees are involved in unlawful activity at work (b) whether other procedures have been undertaken to detect the unlawful activity and the outcome; (c) who and what will regularly be subject of the covert surveillance; (d) the dates and times during which the covert surveillance is proposed to be conducted; (e) the LSO who has been nominated to oversee the covert surveillance.[377] The information in the application must be verified before the magistrate by affidavit or on oath or affirmation.[378]

---

[371] Clause13(1), (2).

[372] Clause 13(3).

[373] Clause 13(2). *Licensed security operator* means 'a person holding a class 2C licence issued under the *Security Industry Act* or a licence of a corresponding kind issued under any Act that replaces that Act (cl 3).

[374] Clause 13(2).

[375] An employer's representative means a person authorised to act on behalf of the employer for the purposes of this Act: cl. 3

[376] Clause 14(1).

[377] Clause 14(2), (4)

[378] Clause 14(5).

Determining applications for CSAs: The magistrate may only issue a CSA if satisfied that the application shows that reasonable grounds exist to justify its issue.[379] The magistrate must have regard to the seriousness of the unlawful activity with which the application is concerned[380]; and must also have regard to whether covert surveillance of the employee(s) concerned might unduly intrude on their privacy or the privacy of any other person.[381] If the CSA would authorise covert surveillance of a recreation room, meal room or any other area at a workplace where employees are not directly engaged in work, the magistrate must also (a) have regard to the affected employees' heightened expectation of privacy when in such an area; and (b) be satisfied that each nominated LSO is competent and fit to oversee the conduct of surveillance in such an area and is capable of adequately accommodating this heightened expectation of privacy.[382]

Form and contents of CSA: A CSA is to be in the prescribed form[383] and must specify a number of matters including:

(a) The purpose for which it authorises covert surveillance;
(b) The kind of covert surveillance (camera, computer or tracking) it authorises;
(c) Where practicable, the name of any person who is likely to be subject to the covert surveillance;
(d) The premises, place, computer, vehicle or thing that is to be the subject of the covert surveillance;
(e) Each nominated licensed security operator who is to oversee the conduct of the covert surveillance;
(f) The period for which the authority remains in force (see below);
(g) The Act's requirements of reporting and restrictions on use and disclosure of surveillance records (see below);
(h) The conditions to which the authority is subject (see below).[384]

Conditions of CSA: Aside from the condition that the covert surveillance be oversighted by a nominated LSO, a CSA would be subject to conditions restricting access to surveillance records made as a consequence of covert surveillance[385]; and a condition requiring the nominated LSO to destroy surveillance records.[386] It would also be subject to such other conditions as prescribed by the regulations or specified in the CSA.[387]

---

[379] Clause 16(1).

[380] Clause 16(2).

[381] Clause 17.

[382] Clause 16(3).

[383] Clause 18(1).

[384] Clause 18(2).

[385] Clause 20(1).

[386] Clause 20(1).

[387] Clause 20(1)(e).

Duration of CSA: A CSA remains in force for the period - not exceeding 30 days or such other period as may be prescribed by regulations - specified in the authority.[388]

Variation or cancellation of CSA: A magistrate may at any time cancel a CSA, either on the magistrate's own initiative or on application made by any employee, employer, or other person affected by the authority.[389]

Review of magistrate's decision: An applicant for a CSA who is aggrieved by a magistrate's decision to refuse to issue or to vary or cancel a CSA may apply to a judicial member of the Industrial Relations Commission to issue, vary or cancel the authority.[390] An employee affected by a CSA who is aggrieved by a magistrate's decision to refuse to vary or cancel a CSA may apply to a judicial member to vary or cancel the authority.[391] These applications must be made within 30 days after the decision is given or such further period as allowed.[392]

Employer's reporting requirements: The employer or representative to whom a CSA is issued must furnish a report to the magistrate who issued the authority within 30 days after the expiry of the authority.[393] The report is to set out briefly the result of the surveillance carried out and give details of a number of specified matters. Some of these relate to the matters which the CSA was required to specify on being issued (eg the name of an employee who was subject of the surveillance, and the period during which the surveillance was conducted). Other specified matters include details of any surveillance record made, any action proposed to be taken in light of the information obtained, and any reason why an employee who was subject of the surveillance should not be informed of the surveillance.[394]

Orders that magistrate can make after receiving report: The magistrate may make such orders as he or she thinks appropriate with respect to the use or disclosure of any surveillance record made as a consequence of surveillance conducted in accordance with the authority including either or both of the following orders: (a) an order that the surveillance record be delivered up to the magistrate to be kept in the custody of the magistrate or otherwise dealt with; (b) an order that a specified person or body be informed of the surveillance and given access to, or to part of, any surveillance record made as a consequence of the surveillance.[395]

---

[388] Clause 19.

[389] Clause 22(1), (2).

[390] Clause 31(1).

[391] Clause 31(2).

[392] Clause 31(3).

[393] Clause 26(1), (4). Contravention of this provision is an offence.

[394] Clause 26(2).

[395] Clause 26(6).

Access to and destruction of covert surveillance records

Restrictions on access to covert surveillance records: The CSA is subject to a condition that the nominated LSO and their supervisees[396] must not give any other person access to surveillance records[397] made as a consequence of covert surveillance.[398] The only exception to this condition is that they may supply the employer or the employer's representative with any portions of such surveillance records that are relevant to establishing the involvement of any employee in an unlawful activity at work in accordance with the authority conferred by the CSA or for identifying or detecting any other unlawful activity at work.[399] And, if an employer or employer's representative takes detrimental action against the employee[400], the employer or representative must give the employee access to the surveillance record within a reasonable period of being requested to do so by the employee.[401]

Destruction of records and protection against unauthorised use: The nominated LSO must erase or destroy within 3 months of the expiry of the CSA all parts of surveillance records not required for evidentiary purposes.[402] Any LSO who oversees the conduct of covert surveillance under the authority of a CSA must take such security safeguards as are reasonable in the circumstances to ensure that any covert surveillance record that is in its possession is protected against loss or unauthorised access or use.[403] An employer or employer's representative to whom a CSA has been issued has the same obligation in relation to any portion of a covert surveillance record in its possession.[404]

Restrictions on use and disclosure of covert surveillance records

Prohibition on use or disclosure of covert surveillance information: A person must not make use of or disclose to another person surveillance information or a surveillance record knowing or having reasonable cause to suspect that the information has been

---

[396] Supervisees are any person conducting covert surveillance under the oversight of a nominated LSO: cl. 20(2).

[397] A *surveillance record* means a record or report of *surveillance information***,** and that term means information determined, recorded, monitored or observed as consequence of surveillance of an employee: clause 3.

[398] Clause 20(1)(a).

[399] Clause 20(1)(b).

[400] This means action causing, comprising or involving (a) discrimination, disadvantage, or adverse treatment in relation to employment; or (b) dismissal from, or prejudice in, employment; or (c) a disciplinary proceeding: clause 20(2).

[401] Clause 20(1)(d). Contravention of a conditions is an offence.

[402] Clause 20(1). Contravention of this condition is an offence.

[403] Clause 27(1). Contravention of this provision is an offence.

[404] Clause 27(2). Contravention of this provision is an offence.

obtained or the record has been made as a result of *covert surveillance* of an employee at work.[405] There are exceptions to this prohibition as outlined below.

Exceptions where covert surveillance authorised by CSA: If the covert surveillance of an employee was authorised by a CSA, the following use or disclosure is permitted:

- That which is authorised or required by conditions of CSA or an order of a magistrate to whom report on the use of CSA has been furnished;
- For a purpose related to establishing whether or not an employee is involved in unlawful activity at work pursuant to the authority conferred by the CSA;
- For a purpose related to taking disciplinary action or legal proceedings against an employee as a consequence of any alleged unlawful activity at work;
- For a purpose related to establishing security arrangements or taking other measures to prevent or minimise the opportunity for unlawful activity at work of a kind identified by the surveillance record to occur at work;
- To a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- For a purpose related to the taking of proceedings for an offence;
- For a purpose related to taking any other action authorised or required by the Act.[406]

Exceptions where covert surveillance not authorised by CSA: If covert surveillance of an employee was not authorised by a CSA, the following use or disclosure is permitted:

- To a member or officer of a law enforcement agency for use in connection with the detection, investigation or prosecution of an offence;
- For a purpose related to taking proceedings for an offence.[407]

Information obtained inadvertently pursuant to CSA: Information that has inadvertently or unexpectedly come to the knowledge of person as result of carrying out of covert surveillance authorised by a CSA is, for the purpose of any determination by a court as to the admissibility of evidence in criminal proceedings, not considered to have been obtained in contravention of the Act[408] – except if the court is of the opinion that the application on the basis of which the CSA was granted was not made in good faith.[409]

[405] Clause 28(1). Contravention of this provision is an offence.

[406] Clause 28(2).

[407] Clause 28(3).

[408] Clause 29(1).

[409] Clause 29(2).

APPENDIX 2 – DRAFT BILL COMPARED TO NSWLRC PROPOSAL

Introduction

As outlined above, the NSW Law Reform Commission's Interim Report on Surveillance (2001) recommended enacting comprehensive surveillance regulation, including regulation of workplace surveillance.[410] The main differences between the draft *Bill* and the Commission's recommendations, as they relate to workplace surveillance, are summarised below.[411]

Types of surveillance regulated

The draft *Bill's* coverage of workplace surveillance would be limited to camera surveillance, computer surveillance and tracking surveillance, whereas the Commission proposes a broader definition of "surveillance" that is not device specific.[412] This would include internet and email monitoring[413] – but note that the Commission has not proposed to regulate the *blocking* of employees' emails or access to websites.

Manner in which employees must be notified of surveillance

Like the draft *Bill,* the Commission's proposal would require employers to give employees written notice of the intended surveillance at least 14 days prior to its commencement.[414] However, the Commission's proposal also outlines what the written notice should specify, namely, the location of the surveillance, the nature and capacity of the surveillance devices, whether the surveillance will be continuous and, if not, the hours of operation, the purpose of the surveillance, and the person responsible for the conduct of the surveillance.[415] For surveillance outside the employment context, the Commission recommended that adequate notice of surveillance could be given by clearly visible signs, or other warnings such as audio announcements or written notification, and surveillance equipment which is clearly visible.[416] It is not clear whether these requirements would also apply to workplace surveillance.

---

[410] See section 7 of this paper, above.

[411] All references to clauses in these footnotes refers to clauses in the draft *Bill* and all references to recommendations refer to the NSWLRC Interim Report, Note 61, above.

[412] See Recommendations 1-3. Note, the *Listening Devices Act 1984 (NSW)* (which regulates audio surveillance would continue to apply if the draft Bill was enacted.

[413] Interim Report, p 60-66.

[414] Recommendation 11.

[415] Recommendation 12.

[416] Recommendation 10.

Regulation of covert surveillance

The Commission proposed the same scheme for regulating covert surveillance as the draft *Bill* (ie covert surveillance would be prohibited without authorisation) but some of the Commission's recommendations differ from the Bill, as outlined below.

Grounds for obtaining covert surveillance authorisation: The draft Bill only allows covert surveillance authorisation to be obtained "for the purpose of establishing whether or not the employee is involved in any unlawful activity at work."[417] The Commission recommended that an employer should *also* be entitled to obtain an authorisation for covert surveillance if "serious misconduct justifying summary dismissal is reasonably suspected".[418] The Commission said that this additional justification would encompass behaviour such as falsifying time records and other forms of serious misconduct.[419] Its availability would depend on both the particular employment relationship involved and the relevant conduct.[420]

The issuing authority: The draft *Bill* would require covert surveillance authority applications to be made to and decided by a magistrate, whereas the Commission's proposal would vest the responsibility in Industrial Magistrates and Judicial Members of the Industrial Relations Commission.[421] The Commission explained this approach as follows, "as the fundamental basis of providing a separate authorisation regime for surveillance by employers is the industrial dimension, it seems appropriate that Industrial Magistrates and Judicial Members of the Industrial Relations Commission are the issuing authority."[422]

Retrospective authorisation: The Commission recommended that while authorisation for covert surveillance should be obtained prior to its commencement, provision should also be made for retrospective authorisation in exceptional circumstances.[423] The Commission gives an example of a situation where "an employer may reasonably suspect misconduct such as tampering with machinery, which could pose a health risk to other employees and/or third parties. In such a situation, it would be justifiable to commence surveillance as soon as possible."[424] The draft *Bill* does not provide for retrospective authorisation.

---

[417] Cause 8.

[418] Recommendation 58, p 303.

[419] Interim Report, p 303.

[420] Ibid.

[421] Recommendation 62.

[422] Interim Report, p 306-7.

[423] Recommendation 66.

[424] Interim Report, p 312.

Accountability for covert surveillance: The draft *Bill* would require employers to furnish a report to the magistrate who issued the covert surveillance authority, giving details of a number of matters (eg the result of the surveillance, period of surveillance, details of any surveillance record made).[425] The draft Bill would also require the Minister to prepare an annual report on operations carried out pursuant to covert surveillance authorities and table the report in both Houses of Parliament. The Commission's recommendations contain more stringent accountability requirements:

- Employers would be required to report to the Attorney-General (AG) as to the use of a surveillance device (in addition to reporting to the industrial magistrate);[426]
- The issuing authority (ie Industrial Magistrate) would be required to forward to the AG, annually, information about applications for authorisations;[427]
- Employers would be required to keep records containing particulars as to the use of surveillance devices.[428]
- An inspecting authority (either the Privacy Commissioner or Ombudsman) would be required to inspect those records to ascertain the accuracy of entries in the records, the extent of compliance with the legislation, and also to determine whether notice should be given to the subject of surveillance;
- The inspecting authority would be required to report to the AG about the result of those inspections.[429]
- The AG's annual report to parliament with respect to the use of surveillance devices would be required to contain certain information (such information is not specified in the draft *Bill*).[430]

Proceedings for offences and penalties: The draft *Bill* provides for offences to be dealt with summarily.[431] The maximum penalty for an offence would be a fine of 50 penalty units ($5,500). The Commission recommends that offences generally be prosecuted summarily but that there be provision for prescribed offences to be prosecuted either summarily or on indictment.[432] It recommends penalties in line with the *Listening Devices Act*.[433] In that Act, the maximum penalties for offences are: for a summary conviction – a fine of 40 penalty units ($4,000) and/or imprisonment for 2 years; and,

[425] Clause 26.

[426] Recommendation 68.

[427] Recommendation 70.

[428] Recommendation 72.

[429] Recommendation 73. See also Recs 74-78 (re: inspecting authority).

[430] Recommendation 79, p 344ff

[431] Clause 35.

[432] Recommendation 104

[433] Recommendation 121.

for a conviction on indictment– a fine of 100 penalty units ($11,000) and/or imprisonment for 5 years.[434] Where a corporation committed the offence and the proceedings are taken in the Supreme Court in its summary jurisdiction, the maximum penalty is a fine of 500 penalty units ($55,000).[435] The Commission envisages that a fine would be the appropriate penalty in most cases but that, in more serious circumstances, a custodial sentence may be appropriate.[436]

Civil action available in addition to prosecution: Consistently with the Commission's recommendation that breaches of *overt* surveillance provisions should give rise to a civil action (see below), it recommends that employees be entitled to bring a civil action for breach of a covert surveillance provision.[437] This civil action would be available concurrently with a prosecution for a criminal offence under the Act.[438] The draft *Bill* makes no provision for employees to bring civil actions.

Regulation of overt surveillance

The draft *Bill* does not impose any limits on surveillance which has been notified to employees in the manner specified, except for the prohibition on the use of notified surveillance in toilets and change rooms etc[439]; and the prohibition on surveillance of an employee while he or she is not at work.[440] On the other hand, the Commission proposes to regulate notified surveillance. Employers would need to comply with the following eight legislative principles when undertaking overt surveillance:

1. Overt surveillance should not be used in such a way that it breaches an individual's reasonable expectation of privacy.
2. Overt surveillance must only be undertaken for an acceptable purpose.
3. Overt surveillance must be conducted in a manner which is appropriate for purpose.
4. Notice provisions shall identify the surveillance user.
5. Surveillance users must be accountable for their surveillance devices and the consequences of their use.
6. Surveillance users must ensure all aspects of their surveillance system are secure.
7. Material obtained through surveillance to be used in a fair manner and only for the purpose obtained.
8. Material obtained through surveillance must be destroyed within a specified period.[441]

---

[434] See Interim Report, p 449.

[435] Ibid.

[436] Ibid.

[437] Recommendations 105, 106.

[438] Interim Report, p 433

[439] Clause 9.

[440] Clause 10.

[441] Recommendations 17-21. See also Interim Report at p 196 (para 4.74)

These principles would need to be supplemented with codes of practice for "significant users" of overt surveillance. The Commission states that, having regard to the highly controversial nature of performance monitoring, substantial consideration must be given to the overt surveillance principles when performance monitoring is an issue."[442] The Commission suggests that principles 2 and 3 will be of particular relevance to performance monitoring.[443] Overt surveillance by an employer in contravention of the overt surveillance principles would give rise to civil liability (see below).[444]

Civil actions for breaches of overt and covert surveillance provisions

Bringing an action: The Commission proposes a complaints and review process whereby an employee who is aggrieved by surveillance (or an organisation representing employees) could elect to have the complaint dealt with in one of two ways (i) conciliation by the Privacy Commissioner, and if unresolved, a hearing by a specialist division of the Administrative Decisions Tribunal (ADT); or (ii) conciliation by the Industrial Relations Commission (IRC), and if unresolved, arbitration by the IRC.[445]

Remedies: The remedies available would depend on the election as to venue. The ADT would have the power to make an award of damages of up to $150,000 (or up to $750,000 if a District Court Judge is the presidential member on the panel). Damages would not be limited to financial loss but could include damages for psychological or physical harm resulting from the unlawful surveillance. The ADT could also grant other relief such as an injunction, a mandatory order, a declaration, or an order that the employer implement a program to eliminate unlawful surveillance in the workplace.[446] The IRC would have at its disposal the full range of remedies available in the case of an unfair dismissal, namely reinstatement, re-employment, lost remuneration in either of these cases, or compensation if the employee is not reinstated or re-employed.[447] Compensation would be limited to the amount of remuneration during six months prior to being dismissed.

[442] Interim Report, p 198.

[443] Ibid.

[444] Recommendation 88.

[445] See Recommendations 91-102 (p 428-432)

[446] Recommendation 112, p 446.

[447] Interim Report, p 451.

APPENDIX 3 – UK CODE OF PRACTICE: MONITORING AT WORK

Introduction

This appendix presents a summary of *Employment Practices Data Protection Code – Part 3: Monitoring at Work,* published by the UK Information Commissioner.[448] As outlined above Part 3 of the Code contains 'Good Practice Recommendations', which are organised under the following headings:

(1) Managing data protection;
(2) General approach to monitoring;
(3) Monitoring electronic communications;
(4) Video and audio monitoring;
(5) Covert monitoring;
(6) In-vehicle monitoring;
(7) Monitoring through information from third parties.

The following is a summary of the main points raised under headings (2) to (6). See also the *Supplementary Guidance* referred to in paragraph 9.4, above.

General approach to monitoring

As noted above the core principles are as follows:

- It will usually be intrusive to monitor your workers;
- Workers have legitimate expectations that they can keep their personal lives private and that they are also entitled to a degree of privacy in the work environment;
- If employers wish to monitor their workers, they should be clear about the purpose and satisfied that the particular monitoring arrangement is justified by real benefits that will be delivered;
- Workers should be aware of the nature, extent and reasons for any monitoring, unless (exceptionally) covert monitoring is justified;
- In any event, workers' awareness will influence their expectations.[449]

In relation to the third dot point, it will be seen below that the Code recommends, in relation to all forms of monitoring, that employers consider –preferably *using an impact assessment* – whether the benefits of monitoring justify the adverse impact. An impact assessment involves: (a) Identifying clearly the purpose behind the monitoring arrangement and the benefits it is likely to deliver; (b) Identifying any likely adverse impact of the monitoring arrangement; (c) Considering alternatives to monitoring/or different ways in which it might be carried out; (d) Taking into account the obligations that arise from monitoring; (e) Judging whether monitoring is justified.[450]

[448] See paragraph 9.4, above.

[449] Part 3 of the Code, p 24.

[450] Ibid, p 16.

Monitoring electronic communications[451]

Generally:

- *Establish a policy* - Employers who wish to monitor electronic communications at work, should establish a policy on their use and communicate it to workers.[452] The Code refers to a number of matters which employers should consider including in such a policy.[453]

- *Regulatory of Investigatory Powers Act 2000:* Ensure that where monitoring involves the interception of a communication it is not outlawed by this Act.

- *Security of system* – Consider – preferably using an impact assessment – whether any monitoring of electronic communications can be limited to that necessary to ensure the security of the system and whether it can be automated (automated systems may be less intrusive).[454]

Email and internet monitoring:

- If emails and/or internet access are, or are likely to be, monitored, consider - preferably using an impact assessment – whether the benefits justify the adverse impact. If so, inform workers about the nature and extent of all e-mail and internet access monitoring.[455]

- Wherever possible avoid opening emails, especially ones that clearly show they are private or personal.[456]

- Where practicable ensure that those sending emails to workers, as well as workers themselves, are aware of any monitoring and the purpose behind it.[457]

---

[451] This includes monitoring of 'telephone, fax, e-mail, voice-mail, internet access, and other forms of electronic communication.' Part 3 of the Code, p 29

[452] Ibid, p 29.

[453] See Part 3 of Code, p 30.

[454] Ibid, p 31.

[455] Ibid, p 30.

[456] Ibid, p 33. In this regard, the Code recommends that (a) email monitoring be confined to address/heading unless essential for a valid reason to examine content; (b) workers be encouraged to mark any personal emails as such and tell those who write to them to do the same; (c) if workers are allowed to access personal email accounts from the workplace, such e-mails should only be monitored in exceptional circumstances.

[457] Ibid, p 34.

- If it is necessary to check the email accounts of workers in their absence, make sure that they are aware that this will happen.[458]

- Inform workers of the extent to which information about their internet access and emails is retained in the system and for how long.[459]

Video and audio monitoring:

- If video or audio monitoring is (or is likely) to be used, consider – preferably using an impact assessment – whether the benefits justify the adverse impact.[460]

- Give workers a clear notification that video or audio monitoring is being carried out and where and why it is being carried out.[461]

- Ensure that people other than workers, such as visitors or customers, who may inadvertently be caught by monitoring, are aware of its operation and why it is being carried out.[462]

Covert monitoring

Covert monitoring means 'monitoring carried out in a manner calculated to ensure that those subject to it are unaware that it is taking place.'[463]

The recommendations in the Code are mainly directed at covert video or audio monitoring – but are also relevant where electronic communications are monitored when workers would not expect it. Recommendations include:

- Covert monitoring should not normally be considered. It will be rare for covert monitoring of workers to be justified. It should therefore only be used in exceptional circumstances.[464]

- Senior management should normally authorise any covert monitoring. They should satisfy themselves that there grounds for suspecting criminal activity

[458] Ibid, p 34.

[459] Ibid, p 34.

[460] Ibid, p 35.

[461] Ibid, p 35.

[462] Ibid, p 36.

[463] Ibid, p 37.

[464] Ibid, p 37.

or equivalent malpractice and where notifying individuals about the monitoring would prejudice its prevention or detection.[465]

- Ensure that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that it does not continue after the investigation is complete.[466]

- Do not use covert audio or video monitoring in areas where workers would genuinely and reasonably expect to be private.[467]

- If a private investigator is employed to collect information on workers covertly make sure there is a contract in place that requires the private investigator to only collect information in a way that satisfies the employer's obligations under the Act.[468]

- Ensure that information obtained through covert monitoring is used only for the prevention or detection of criminal activity or equivalent malpractice. Disregard and where feasible, delete other information collected in the course of monitoring unless it reveals information that no employer could reasonably be expected to ignore. Prior to the investigation, set up clear rules limiting the disclosure and access to information obtained.[469]

In-vehicle monitoring

The Code states that 'monitoring of vehicle movements, where the vehicle is allocated to a specific driver, and information about the performance of the vehicle can therefore be linked to a specific individual, will fall within the scope of the Data Protection Act.'[470] Recommendations include:

- If in-vehicle monitoring is or will be used, consider – preferably using an impact assessment – whether the benefits justify the adverse impact.[471]

- Where private use of a vehicle is allowed, monitoring its movements when used privately, without the freely given consent of the user, will rarely be

[465] Ibid, p 37.

[466] Ibid, p 37.

[467] Ibid, p 37.

[468] Ibid, p 38.

[469] Ibid, p 38.

[470] Ibid, p 39.

[471] Ibid, p 39.

justified. If the vehicle is for both private and business use, it ought to be possible to provide a 'privacy button' to enable monitoring to be disabled.[472]

- Set out a policy that states what private use can be made of vehicles provided by, or on behalf of, the employer, and any conditions attached to use.[473]

[472] Ibid, p 39.

[473] Ibid, p 39.

Recent Research Service Publications

To anticipate and fulfil the information needs of Members of Parliament and the Parliamentary Institution.

[Library Mission Statement]

Note: **For a complete listing of all Research Service Publications contact the Research Service on 9230 2093. The complete list is also on the Internet at:**

http://www.parliament.nsw.gov.au/prod/web/PHWebContent.nsf/PHPages/LibraryPublist

(A) BACKGROUND PAPERS

Implications of the 2001 Federal Election for the 2003 New South Wales Election by Antony Green 1/02

New South Wales State Electoral Districts Ranked by 2001 Census Characteristics by Mark D'Arney 1/03

New South Wales State Election 2003: Electorate Profiles by Mark D'Arney 2/03

Prospects for the 2003 Legislative Council Election by Antony Green 3/03

2003 New South Wales Elections – Preliminary Analysis by Antony Green 4/03

Alcohol Abuse by Talina Drabsch 5/03

2003 New South Wales Elections – Final Analysis by Antony Green 6/03

New South Wales Legislative Assembly Elections 2003: Two-Candidate preferred results by polling place by Antony Green 7/03

New South Wales Legislative Council Elections 2003 by Antony Green 8/03

The Economic and Social Implications of Gambling by Talina Drabsch 9/03

Principles, Personalities, Politics: Parliamentary Privilege Cases in NSW by Gareth Griffith 1/04

Indigenous Issues in NSW by Talina Drabsch 2/04

Privatisation of Prisons by Lenny Roth 3/04

2004 NSW Redistribution: Analysis of Draft Boundaries by Antony Green 4/04

(B) BRIEFING PAPERS

Court Delays in NSW: Issues and Developments by Rachel Callinan 1/02

Sentencing Law: A Review of Developments in 1998-2001 by Rowena Johns 2/02

Outworkers by Roza Lozusic 3/02

Censorship in Australia: Regulating the Internet and other Recent Developments by Gareth Griffith 4/02

Bushfires by Stewart Smith 5/02

Information Privacy and Health Records by Gareth Griffith 6/02

Public Liability by Roza Lozusic 7/02

Dealing with Graffiti in New South Wales by Rachel Callinan 8/02

Human Cloning and Stem Cell Research by Stewart Smith 9/02

Victims of Crime: Plea Bargains, Compensation, Victim Impact Statements and Support Services by Rowena Johns 10/02

Public Liability: An Update by Roza Lozusic 11/02

Water Reforms in New South Wales by Stewart Smith 12/02

Defamation Law Reform Revisited by Gareth Griffith 13/02

Drought by Stewart Smith 14/02

Bail Law and Practice: Recent Developments by Rowena Johns 15/02

Gangs in NSW by Roza Lozusic 16/02

Native Vegetation: Recent Developments by Stewart Smith 1/03

Arson by Talina Drabsch 2/03

Rural Sector: Agriculture to Agribusiness by John Wilkinson 3/03

A Suburb Too Far? Urban Consolidation in Sydney by Jackie Ohlin 4/03

Population Growth: Implications for Australia and Sydney by Stewart Smith 5/03

Law and Order Legislation in the Australian States and Territories, 1999-2002: a Comparative Survey by Talina Drabsch 6/03

Young Offenders and Diversionary Options by Rowena Johns 7/03

Fraud and Identity Theft by Roza Lozusic 8/03