Australian Privacy Foundation

email: mail@privacy.org.au

website : www.privacy.org.au

Review of the *Workplace Surveillance Act 2005* (NSW)

Submission to the NSW Attorney-General's Department

January 2011

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Since 1987, the Foundation has led the defence of the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For further information about the Foundation and the Charter, see www.privacy.org.au

Introduction

The *Workplace Surveillance Act 2005* (NSW) ('the Act') replaced the *Workplace Video Surveillance Act 1998* (NSW) ('the WVSA'), which only applied to video camera surveillance. The new Act also applies to additional forms of surveillance including email and internet monitoring and the use of tracking devices.

The NSW Attorney General has described the aim of the Act as being to promote transparency in the workplace and openness about surveillance practices. While the Act does go some way to meeting these objectives, there are several key deficiencies.

The most significant is the failure to regulate the conduct of 'notified' (or 'overt') surveillance. We suggest that both employees and employers would benefit from an Act which provided greater clarity in the area of overt surveillance.

In addition, we are of the view that an independent body, such as the Information and Privacy Commission, should be provided the powers and resources to administer the Act, including the power to institute civil proceedings where necessary. This would ensure employers and employees are educated about their rights and responsibilities, and provisions in the Act are adequately enforced. Further areas for reform are outlined below.

In 2004 we provided a submission to the Attorney-General in response to the exposure draft Workplace Surveillance Bill 2004. In that submission we raised a number of serious deficiencies within the exposure draft, and included a number of recommendations for improvement. The Bill was not changed significantly, and many of these recommendations also apply to the Act. It is our view that unless

modified, the Act represents more a lost opportunity than a serious attempt at law reform in the contentious area of workplace privacy. This submission therefore includes a number of recommendations for how the Act could be modified to provide greater privacy protection to employees, and greater clarity and certainty for employers.

Notified surveillance

The Act defines a category of visible surveillance ('notified surveillance', previously 'overt surveillance' in the WVSA), and defines everything else as its opposite - 'covert surveillance'. Only the conduct of covert surveillance is then further regulated by the Act.

This strict 'overt / covert' dichotomous approach has two major disadvantages:

- operational requirements are incorporated into the definition of notified surveillance, such that a failure to meet an operational requirement moves the conduct into the opposing category, and
- there is no regulation of notified surveillance beyond the requirement to meet the definition (ie to conduct the surveillance with proper notification).

This approach benefits neither employer nor employee.

The risk to employers is that a failure to meet the operational requirements built into the definition of 'notified surveillance', even if simply through forgetfulness, will render the otherwise notified surveillance 'covert', and thus unlawful unless a magistrate's authority is first obtained. In doing so, the employer will commit at least one offence,[1] and they cannot use or disclose any information gathered through the surveillance except in relation to proceedings for an offence.[2]

One example is the employer who accidentally gives only 13 instead of 14 days prior notice to employees that she is taking delivery of new fleet cars which will have their GPS systems switched on.

A second example is the home owner who uses a CCTV system to protect their home against burglary. The system is not 'hidden', in that the camera casings can clearly be seen, and they even have a sign on a front window to indicate there is a security system with CCTV in place. The home owner employs a person to work at the home – a plumber, a cleaner, or a nanny – but forgets to provide them with written notice of the existence of the CCTV before the person commences work. The home owner is an employer,[3] whose conduct does not meet the definition of 'notified surveillance',[4] and thus is now conducting 'covert surveillance' without lawful authority.

The above scenarios illustrate the difficulty in creating an absolute dichotomy between 'covert' and 'notified' surveillance, in which the former is tightly regulated with criminal sanctions and the latter is entirely unregulated, in circumstances where it is easy for the unwary employer to slip from the latter category into the former.

In addition, employees continue to have no privacy protection for the collection, storage, use or disclosure of information gathered through overt surveillance, beyond the notification and signage requirements necessary to meet the definition of 'notified surveillance'. Due to the inadequacies of

[1] See section 19, and possibly also section 16, of the Act.
[2] See section 37(3) of the Act.
[3] See the definition of 'employer' in section 3 of the Act.
[4] See section 10(1) of the Act – the usual requirement of providing 14 days notice prior to commencing surveillance sensibly does not apply in cases where the surveillance existed before the employee commenced working for the employer, but under section 10(3) the employee must still be given notice in writing "before commencing work".

existing information privacy laws in this area,[5] employees are virtually powerless to prevent, or seek redress for, any misuse or unfair handling of their personal information gathered by way of overt surveillance.

We are also concerned that third parties – such as clients, customers, students, colleagues and other visitors to the premises – may be subject to surveillance without their knowledge or consent. Most of these people would have no knowledge of any surveillance unless they are warned (eg. by telephone recording) or other public notification (eg. notices about CCTV in buildings).

The NSW Acting Privacy Commissioner has previously drawn the Government's attention to the high rate of telephone enquiries and complaints lodged with his office about the use of overt video surveillance in the workplace.[6] Privacy NSW has noted:

> Uncontrolled overt surveillance can contribute to stress and a sense of powerlessness. It has the potential to be abused, for example, by zooming in on individual employees or subjecting them to an unreasonable level of continuous monitoring. In the absence of privacy protection for employee records there is a capacity for misuse of stored images from video surveillance.[7]

Subsequent Privacy NSW Annual Reports indicate that enquiries continue to frequently relate to surveillance issues.[8]

We submit that an appropriate approach would be to develop privacy principles relating to notified, or overt, surveillance in the workplace, which balance the competing interests of employers and employees, and also takes into account the rights of third parties.

In March 1996 a NSW working party on video surveillance in the workplace convened by the Department of Industrial Relations and representing employers, employees and the NSW Privacy Committee endorsed a voluntary *Code of Practice for the Use of Overt Video Surveillance in the Workplace.* The Code established a series of standards for overt surveillance systems, such as restricting the hours in which surveillance should operate, providing guidance on storage, retention and employees' access to tapes, and providing guidance on the ethical use and disclosure of surveillance material.

The International Labor Office's *Code of Practice on the Protection of Workers' Personal Data* was settled in 1997, and contains principles relevant to overt surveillance of employees such as:

- information collected should be used lawfully and fairly, and only for reasons directly relevant to the employment of the worker
- surveillance information should not be the only factor in evaluating performance
- employers must secure surveillance information against loss, unauthorised access, use, alteration or disclosure, and
- employees should have access to any surveillance information collected about them.

---

[5] There are exemptions for the employee records of private sector employees under the Federal *Privacy Act 1988* and the NSW *Health Records and Information Privacy Act 2002,* and for any information about the suitability of public sector employees under the NSW *Privacy and Personal Information Protection Act 1998* and the NSW *Health Records and Information Privacy Act* 2002.

[6] See Attachment 1 to *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003, available from www.lawlink.nsw.gov.au/privacynsw

[7] See pp 5-6 of the *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003.

[8] See p 21 of the Privacy NSW 2002-03 Annual Report, and p 10 of the 2008-09 Annual Report.

In 2001, the NSW Law Reform Commission's recommendations from their Report 98, *Surveillance: An Interim Report,* included the introduction of a set of binding principles governing overt surveillance. The proposed principles included core standards such as that the surveillance must not breach reasonable expectations of privacy, must only be undertaken for acceptable purposes, and that use must be consistent with its purpose. The Law Reform Commission's recommendations have in turn been comprehensively reviewed by the NSW Privacy Commissioner.[9]

In 2005 in their *Workplace Privacy: Final Report*, the Victorian Law Reform Commission recommended that workplace surveillance legislation include principles to assist employers in complying with their proposed legislative obligation not to unreasonably breach the privacy of workers. The Commission determined that an employer would unreasonably breach the privacy of workers if it engages in acts or practices:

- for a purpose that is not directly connected to the employer's business
- in a manner that is not proportionate to the purpose for which those acts and practices are being used
- without first taking reasonable steps to inform and consult workers about the relevant act or practice
- without providing adequate safeguards to ensure the act or practice is conducted appropriately, having regard to the obligation not to unreasonably breach the privacy of the worker.[10]

We recommend that in addition to visibility and signage requirements for conducting notified surveillance, there also be principles which set out requirements relating to the operation of notified surveillance, and the collection, use, storage and disclosure of surveillance information obtained through notified surveillance.

This review of the Act would appear to be an opportune time to implement comprehensive privacy principles governing notified surveillance of employees, as previously recommended by the NSW Law Reform Commission. In the absence of regulation relating to notified surveillance, this Act adds very little of the privacy protection promised for employees or the sensible guidance promised for employers.

We therefore recommend that the Act be amended to incorporate provisions similar to the 1996 voluntary *Code of Practice for the Use of Overt Video Surveillance in the Workplace* and/or the privacy principles as proposed by the NSW Law Reform Commission and the Victorian Law Reform Commission, such that the conduct of overt surveillance is directly regulated. Such provisions could also address the situation where overt surveillance incidentally or deliberately monitors or records information about third parties, such as clients, customers, students, visitors to the premises, and so on.

'Notified' surveillance that is not actually notified

The definition of notified surveillance also incorporates surveillance conducted for a purpose 'other than surveillance of employees', where the employee (or a body representing a substantial number of employees) has agreed to that use, and the surveillance is 'carried out in accordance with that agreement'.[11] This category would appear to require none of the notification, visibility or signage requirements.

---

[9] See pp 6-18 of the Privacy NSW *Submission on the NSW Law Reform Commission Report 98, Surveillance: An Interim Report*, June 2002.
[10] See p 54 of the Victorian Law Reform Commission *Workplace Privacy: Final Report,* October 2005.
[11] See section 14 of the Act.

Thus it would appear that the Act would allow for example hidden CCTV cameras in the foyer of a building, with no signage whatsoever. This is a significant departure from existing Government policy on the use of CCTV cameras in public places.[12]

This provision nonetheless suggests that any use of the surveillance material must conform to the 'agreement' with the employees. It would appear that any other use will tip the conduct from being 'notified' surveillance into the category of 'covert' surveillance and thus be prohibited, but only if employees are subject to the surveillance. There are no penalties or remedies for non-agreed uses of surveillance material, so long as employees are not the target. Thus while the employees or their representative body may negotiate an agreement which incorporates privacy protection for third parties such as clients or members of the public, the employer may breach the agreement with impunity.

Furthermore this approach exposes all parties to considerable risks. The status of the surveillance at law will depend on interpretation of the 'agreement'. How will disputes about the 'agreement' be resolved? The Act provides no guidance on how or whether surveillance established for one non-employment purpose (such as security of premises) could legitimately be used for another purpose (such as disciplining of employees or tracking their punctuality).

We therefore recommend that section 14 be deleted.

Covert surveillance

Section 19 of the Act prohibits covert surveillance of an employee at work without a magistrate's authority.

While this is a commendable protection, we are disappointed that it could potentially be undermined by the provision in section 22, which provides a defence to prosecution in some circumstances. It is our submission that this particular section undermines the basic rule in section 19, by allowing an employer to conduct covert surveillance of employees without a magistrate's authority, and then if caught and prosecuted simply justify their actions as necessary for 'the security of the workplace or persons in it'. The employer can thus avoid both the up-front justification before a magistrate, and the post-hoc reporting requirements, for covert surveillance of employees that the Act is predicated upon. We recommend the necessity of section 22 be considered.

Prohibition on surveillance using work surveillance device while employee not at work

Section 16 of the Act prohibits the use of a device (other than a computer), normally used for notified surveillance of the employee at work, if it is also used for surveillance of the employee when the employee is not at work. However this does not cover the scenario where the employer uses a device only switched on when the employee is not at work.[13] For example, it is our reading that the Act will not prohibit an employer from using a tracking device to determine the location of an employee's work-provided mobile phone or fleet vehicle while the employee is off duty, so long as they don't use the same tracking device when the employee is also on duty. Potentially such conduct could be more privacy-invasive that any surveillance conducted while the employee is 'at work'.

In addition, inadvertent surveillance may become criminal conduct under section 16. For example, an employer who installs a location-tracking device (eg. in a fleet vehicle) to lawfully track their vehicle or staff are during work time will be in breach of the Act if they accidentally leave the surveillance 'on'

[12] See part 14 of the NSW Government *Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television in Public Places*, which also recommends the relevant Australian Standard, AS 2342 – 1992. The policy is available at http://www.lawlink.nsw.gov.au/cpd.nsf/pages/cctv_index .

[13] That is, a device which is not part of a 'notified surveillance' system used 'at work'.

when the employee is not 'at work' (eg. using the vehicle for personal use after hours). However, unless the employee's work and commute hours are strictly controlled, and the surveillance device likewise, how is the employer to know when to turn the surveillance on and off?

Therefore, under section 16, deliberate misconduct may not amount to an offence, and inadvertent conduct may be criminalised. We therefore recommend the wording of this section be carefully reviewed.

Use of covert surveillance material

The Act provides at section 37(2) the circumstances in which surveillance material, obtained covertly with a magistrate's authority, may be used or disclosed. Categories (b)-(d) each require a test in which the use or disclosure is for a purpose that is 'directly or indirectly related to …'. We suggest that an appropriate additional threshold be that the purpose also be 'reasonably necessary for …'.

The Act provides at section 37(3) that illegally obtained surveillance material (that is, material gathered through covert surveillance that was not authorised) may still be used or disclosed in some circumstances.

There are two circumstances in which material could potentially be gathered through covert surveillance that was not authorised:

- the employer who intended to conduct visible surveillance, but whose actions accidentally tipped them into the definition of 'covert' surveillance, and
- the employer whose intention was to conduct hidden surveillance, and who does so without obtaining the appropriate authorisation, whether through ignorance of the law or by intention.

That the Act does not distinguish between these two categories is of concern, as previously dealt with above. Furthermore there should be a distinction between the covert surveillance which could have been carried out with a magistrate's authority but wasn't, versus that which could never have been authorised in the first place.

We suggest that any use or disclosure of illegally obtained surveillance material is inappropriate in circumstances where an authority to conduct the covert surveillance could not have been lawfully obtained in the first place. That is, where the purpose of the surveillance was outside the terms of section 20(1) in the Act (eg. if the covert surveillance is conducted with the purpose of monitoring an employee's work performance, or is conducted in a toilet facility), it is our argument that any use or disclosure of the surveillance material obtained must be prohibited.

We submit that if Parliament has set rules about when covert surveillance can not be authorised in the first place, a person who contravenes those rules should not be able to benefit from their unlawful conduct in any way. To prevent the use, disclosure, or admission into evidence of illegally obtained surveillance material, where its collection could never have been lawfully authorised in the first place, would also provide greater certainty and relief for the subjects of illegal covert surveillance. Such an approach would be consistent with the Legislative Council's recommendations in relation to illegally or improperly obtained forensic material.[14]

Blocking email and internet access

Section 17 provides an important privacy protection by preventing an employer from blocking emails without notifying the employee. Yet the exemptions to the general rule, in section 17(2), are too wide. In

[14] Legislative Council Standing Committee on Law and Justice, *Review of the Crimes (Forensic Procedures) Act 2000*, Report 18, February 2002. See recommendation 51.

particular, section 17(2)(c) represents a significant restriction on free speech and the privacy of communications. This places the employer in the position of censoring speech in a covert way. There may be various legitimate reasons that material that reasonable persons would find offensive should nonetheless be communicated by electronic means. An example would be a person who has received an offensive document, which incites racial hatred. The person seeks to forward a copy on to the Anti-Discrimination Board to lay a complaint, or perhaps to the local newspaper as part of a protesting letter to the editor. For these reasons we recommend deletion of section 17(2), such that any blocking of website or emails must always be notified to the employee.

Administration of the Act

Currently, no regulator has specific responsibility for administering the Act - providing education about the Act, monitoring the use of surveillance in workplaces, or enforcing its provisions. While Privacy NSW is responsible for administering the *Privacy and Personal Information Protection Act 1998,* it has no responsibilities in relation to the Workplace Surveillance Act. We recommend the newly created Information and Privacy Commission be made responsible for administering the Act, including educating employers and employees or their rights and responsibilities under it, and enforcing its provisions.

Education

It is vital to the success of the Act that employers and employees are aware a) that the Act exists, and b) of their rights and responsibilities under it. Consider the example cited above – the homeowner who uses surveillance to protect their home and also employs a cleaner or nanny – it is plausible such a person is not even aware of the existence of the Act. Education about a legislative regime is fundamental to its success, and has been frequently acknowledged. The Department of Treasury and Finance for example, cited education as 'an essential non-legislative measure to ensure compliance with statutory obligations'.[15] In addition the former federal Privacy Commissioner noted that 'promotion and education are key tools used by the Office in meeting our responsibility to encourage adoption of privacy standards more broadly in the community'.[16] We recommend additional powers and funding for the Information and Privacy Commission to undertake this role.

Enforcement

Notified surveillance

Rather than the criminal offence approach to non-compliance with the 'covert surveillance' provisions of the Act, we recommend there be a system of civil remedies available for any non-compliance with the notified surveillance provisions, more in line with existing information privacy laws.

For example, there should be the ability for any person affected by the conduct of notified surveillance to lay a complaint with the Information and Privacy Commission in the case of refused access to the surveillance material, unethical use or unauthorised disclosure of surveillance material. As with existing information privacy laws in NSW, the Information and Privacy Commission could attempt to conciliate the complaint, or the complainant could seek an enforceable remedy in the Administrative Decisions Tribunal.[17]

Covert surveillance

[15] See 1-7 of Department of Treasury and Finance, *Victorian Guide to Regulation* (2005).
[16] See p 44 of the Office of the Privacy Commissioner *The Operation of the Privacy Act Annual Report* (2001).
[17] The ability for a complaint to proceed from the NSW Privacy Commissioner to the Administrative Decisions Tribunal, and for the Tribunal to deal with privacy complaints against private sector as well as public sector respondents, will commence on 1 September 2004 when the NSW *Health Records and Information Privacy Act 2002* commences.

We are not aware of any prosecutions under the Act, although there are two matters currently before the courts.[18] This is despite Privacy NSW receiving a large number of complaints relating to workplace surveillance.[19] We are also not aware of any prosecutions under the Act's predecessor, the WVSA, despite evidence of widespread non-compliance with that Act.[20] This may be because no single agency is responsible for administering the Act, and therefore does not have both the willingness and capacity to investigate and prosecute for breaches under it. Further, because of the lack of public record of how the law is being enforced, the Act has little deterrent or educative effect on employers. We recommend additional powers and funding for the newly created Information and Privacy Commission to undertake this role, to cater for situations where there is no union who can represent the employee, or where the employee is not a member of the relevant union.

The Victorian Law Reform Commission in its 2005 review of workplace privacy recommended that civil penalties should be imposed for some breaches of proposed workplace privacy legislation.[21] Similarly, the NSW Law Reform Commission in its 2001 review of surveillance recommended that subjects of unlawful covert surveillance should have the right to gain a civil remedy.[22] We support this recommendation, and do not believe that it is unreasonable that the covert surveillance operator is potentially subject to both a criminal and civil penalty. We also support the recommendation of the NSW Privacy Commissioner that a person subject to covert surveillance should be able to seek a civil remedy if it can be subsequently established that an application for covert surveillance was not made in good faith.[23] We therefore recommend a civil complaints model for non-compliance with the covert surveillance provisions, as per that proposed above with respect to overt surveillance.

Accountability

The Act provides, at section 35, a system by which employers with a covert surveillance authority must provide a 'report back' to the magistrate on various matters, including 'any action taken or proposed to be taken in light of the information obtained'. Under section 35(6), the magistrate may then order that the employee who was the subject of the surveillance be informed of and/or given access to the surveillance material. We approve of these provisions.

We also commend the requirement, at section 42, for a report to be tabled each year by the Attorney General on the number of covert surveillance authorities sought, and the number issued during the reporting year. However we suggest that the report should also include details of:

- the type of surveillance requested / authorised (ie. camera, computer or tracking), and
- what actions were taken after the period of surveillance (as reported back to the magistrate under section 35), and
- whether or not the magistrate made any subsequent orders in relation to the employee subject being informed of or receiving access to the surveillance material (under section 35(6)).

[18] See http://www.smh.com.au/technology/australia-post-spying-on-workers-20100203-ndj0.html?skin=text-only; http://www.smh.com.au/nsw/claims-firm-spied-on-mine-staff-20100726-10st1.html.
[19] See for example p 21 of the Privacy NSW 2002-03 Annual Report, and p10 of the 2008-09 Annual Report.
[20] See p6 of the *Submission by Privacy NSW to the Director General, NSW Attorney General's Department on the Workplace Video Surveillance Act Review*, October 2003.
[21] See recommendation 55 of the Victorian Law Reform Commission *Workplace Privacy: Final Report,* October 2005.
[22] See recommendation 105 and the discussion at 10.38 of the Report.
[23] See p 24 of the Privacy NSW *Submission on the NSW Law Reform Commission Report 98, Surveillance: An Interim Report*, June 2002.

An additional accountability measure would be to allow for the random or periodic audit of local court files by the Information and Privacy Commission to assess the operation of the scheme, including compliance with the report-back requirements.

Definitions

In addition, we make the following recommendations:

- 'Camera surveillance' is defined in the Act as the 'monitoring or recording, by electronic means, of visual images'. This limits the coverage of the Act, such that the recording of a single image (as opposed to two or more images) is not included in the definition. We recommend that the singular as well as plural form be used.
- Our reading of the definition of 'computer surveillance' is that it will incorporate the use of a work-provided email or internet account, even when the computer being used by the employee is the employee's own computer (for example, when the employee uses their home computer to access their work email account). In fact our reading is that any use of any computer by a person will meet the definition of 'computer surveillance', so long as that person's employer is monitoring or recording that use. We recommend this be interpreted broadly to ensure the Act prohibits the surveillance of an employee when not at work.

Conclusion

While advancing the reasonable protection of employees' privacy by prohibiting covert surveillance in most cases, the Act fails to actually regulate the conduct of notified surveillance beyond signage and notification requirements. 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.

This is particularly disappointing, given the amount of work already conducted in the past decade by NSW government agencies in the industrial relations, privacy and law reform fields to develop a workable model of regulation for overt surveillance.

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 to 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, yet at the same time a wronged employee has no ability to obtain a civil remedy for an invasion of their privacy.

We have also identified several key loopholes in the Act, which would allow employers to conduct covert surveillance of employees while they are not at work, and also may conduct covert surveillance of clients and visitors. Furthermore we believe that the Act 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 concerned that the Act does not adequately address situations where overt surveillance incidentally or deliberately monitors or records information about third parties, such as clients, customers, students, visitors to the premises, and so on.

We are of the view that the Act should include principles which aim to balance the interests of employers and employees, and take into account the rights of third parties. These principles should set out requirements relating to the operation of notified surveillance, and the collection, use, storage and disclosure of information obtained through notified surveillance.

Finally, we are of the view that an independent body, such as the Information and Privacy Commission, should be provided the powers and resources to administer the Act, including educating employers and employee about their rights and responsibilities, and instituting civil proceedings where necessary. This would help to ensure that workplace surveillance practices are conducted openly and transparently, the competing interests of employers and employees are effectively balanced, and the rights of third parties are respected.

Summary of recommendations

- That the *Workplace Surveillance Act 2005* (NSW) ('the Act') include principles which set out requirements relating to the operation of notified surveillance, and the collection, use, storage and disclosure of information obtained through notified surveillance.
- That an independent body, such as the Information and Privacy Commission, be provided the powers and resources to administer the Act, including providing education about the Act; enforcing its provisions; and to institute civil proceedings where necessary.
- That section 14 of the Act be deleted.
- That the necessity of section 22 of the Act be considered.
- That the wording of section 16 be carefully reviewed.
- That the report tabled annually by the Attorney General under section 42 also include details of:
    - the type of surveillance requested / authorised (ie. camera, computer or tracking), and
    - what actions were taken after the period of surveillance (as reported back to the magistrate under section 35), and
    - whether or not the magistrate made any subsequent orders in relation to the employee subject being informed of or receiving access to the surveillance material (under section 35(6)).
- That the singular as well as plural form be used in the definition of 'camera surveillance' in section 3 of the Act.
- That the definition of 'computer surveillance' in section 3 of the Act be interpreted broadly to ensure the Act prohibits the surveillance of an employee when not at work.

End.

For further information please contact:

Emily Minter, Board Member
Australian Privacy Foundation
Phone: 0431 729828
E-mail: Board8@privacy.com.au
APF Web site: http://www.privacy.org.au