In today’s workplace, it is not uncommon for employers to utilise a mix of the following types of surveillance and monitoring:

- Email and internet monitoring;
- Video surveillance in customer areas or where valuable stock is held;
- Audio surveillance of staff, particularly in call centres (and even monitoring conversations with customers at the point of sale in retail outlets);
- Use of swipe card technology to monitor staff movements; and
- Drug and alcohol testing, particularly for employees who use vehicles or dangerous machinery.

Recent and proposed developments in the regulation of these areas are creating a brave new world of employee rights which, if managed incorrectly by organisations, will have costly economic and non-economic consequences.

**Current state of the law**

**New South Wales**

Employers in New South Wales have specific legislation to consider. On 7 October 2005, the *Workplace Surveillance Act 2005 (NSW)* came into force. The act regulates overt and covert workplace surveillance.

Essentially, surveillance will be ‘overt’ and lawful if employers notify their employees if surveillance in the workplace is to occur, and advise them of how the surveillance will occur (ie by what means) and whether the surveillance is limited or ongoing.
Importantly, employers in New South Wales must not prevent the delivery or sending of emails or access to certain websites unless such actions are done in accordance with a workplace policy (which the employees are aware of) and employees are given notification whenever blocking occurs.

Any surveillance which is not ‘overt’ (eg where employers do not notify employees that it is occurring) will be classified as ‘covert’. Covert surveillance is unlawful unless an employer obtains a ‘covert surveillance authority’ from a magistrate. Failure to comply with the act can result in penalties of up to $5,500 for each breach. Further, for corporations, directors and persons concerned in the management of the corporation may be held liable.

**Victoria**

On 1 July 2007 the *Surveillance Devices (Workplace Privacy) Act 2006 (Vic)* came into force. This act amended the *Surveillance Devices Act 1999 (Vic)*.

Prior to the amendment, employers were only entitled to use optical or listening devices to monitor private activities or conversations if consent was obtained. Consent was also required to use tracking devices to determine the geographical location of an employee. The amendments introduced specific offences. Employers in Victoria are now also prohibited from using listening or optical devices in workplace toilets, washrooms, change rooms and lactation rooms, although limited exceptions apply. Penalties for a breach include imprisonment and significant fines. It is worth noting that the act does not regulate the monitoring of computer or email usage like the New South Wales equivalent.

**Other States**

Although not specifically regulating workplace surveillance, most States and Territories (with the exception of Queensland) have laws which prohibit using devices to listen to private conversations and/or intercept telecommunications. Employers should also be aware that these prohibitions extend to such surveillance in the workplace.

**Emerging issues – National statutory right to privacy?**

On 12 September 2007, the Australian Law Reform Commission issued *Discussion Paper 72 – Review of Australian Privacy Law*. In all, there were approximately 300 proposals of which one in particular should make employers carefully consider the extent to which they monitor their employees. The ALRC is currently seeking feedback on its recommendations and any concerned employers should make a submission by **7 December 2007**.

**Statutory cause of action**

The ALRC recommended that the *Privacy Act 1988 (Cth)* be amended to provide for a statutory cause of action for the invasion of privacy. The cause of action should cover situations such as:

- unauthorised surveillance; and
- interference, misuse or disclosure of an individual’s correspondence or private written, oral or electronic communications.

If the ALRC recommendations are adopted, an employee would need to prove the following elements:

- that they had a reasonable expectation of privacy; and
- the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities.

On any view, these recommendations involve a significant step towards prescribing the appropriate boundaries for any form of surveillance in the workplace.

Any surveillance not covered by a company policy, or which exceeds
What should employers do?

It is recommended that employers review and, if necessary amend their current policies in light of the recent and proposed changes. During this process employers need to consider both the legal and operational implications. In the current economic climate, with an extremely tight labour market, being over-zealous and untrusting of employees can have a negative impact on staff retention and morale. Therefore employers need to strike a balance between protecting their interests on the one hand and managing employee expectations on the other.

In addition, concerned employers should review the ALRC recommendations, and if necessary make submissions on the potential business impact of the proposed statutory cause of action. Submissions must be made by 7 December 2007.

Lincoln Smith, Senior Associate
+61 8 8236 1139

the parameters of a company policy could be caught within this action. Further, employers will need to develop ways of differentiating between private and work related communications. As the recommendations stand, an interference with private email may be grounds for an action.

Possible defences

The ALRC proposes a range of defences to the statutory cause of action namely:

> if the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

> if the act or conduct was required or specifically authorised by or under law;

> if the information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

> if the information was under the law of defamation, privileged.

It is unlikely that any of these defences could be raised by employers in the workplace surveillance context. Rather, employers will need to claim that there was no reasonable expectation of privacy or the act was not sufficiently serious to cause offence to a person or ordinary sensibilities. As already discussed, the use of well drafted and implemented company policies may be the most appropriate method of minimising the risk of employees commencing an action.

Remedies for a breach of privacy

The ALRC also recommends that a Court hearing the case should have a full suite of remedies available to it to remedy a breach, including:

> damages, including aggravated damages;

> an injunction; and

> an order requiring the defendant to apologise to the plaintiff.

If and when the proposals become law, employees will have a powerful weapon to counter any undisclosed or invasive surveillance and monitoring techniques. Any employers who do not fully disclose the level of surveillance used in a workplace will leave themselves open to claims which could have significant economic consequences.

Possible defences

The ALRC proposes a range of defences to the statutory cause of action namely:

> if the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

> if the act or conduct was required or specifically authorised by or under law;

> if the information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

> if the information was under the law of defamation, privileged.

It is unlikely that any of these defences could be raised by employers in the workplace surveillance context. Rather, employers will need to claim that there was no reasonable expectation of privacy or the act was not sufficiently serious to cause offence to a person or ordinary sensibilities. As already discussed, the use of well drafted and implemented company policies may be the most appropriate method of minimising the risk of employees commencing an action.

Possible defences

The ALRC proposes a range of defences to the statutory cause of action namely:

> if the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

> if the act or conduct was required or specifically authorised by or under law;

> if the information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

> if the information was under the law of defamation, privileged.

It is unlikely that any of these defences could be raised by employers in the workplace surveillance context. Rather, employers will need to claim that there was no reasonable expectation of privacy or the act was not sufficiently serious to cause offence to a person or ordinary sensibilities. As already discussed, the use of well drafted and implemented company policies may be the most appropriate method of minimising the risk of employees commencing an action.

Possible defences

The ALRC proposes a range of defences to the statutory cause of action namely:

> if the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

> if the act or conduct was required or specifically authorised by or under law;

> if the information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

> if the information was under the law of defamation, privileged.

It is unlikely that any of these defences could be raised by employers in the workplace surveillance context. Rather, employers will need to claim that there was no reasonable expectation of privacy or the act was not sufficiently serious to cause offence to a person or ordinary sensibilities. As already discussed, the use of well drafted and implemented company policies may be the most appropriate method of minimising the risk of employees commencing an action.

Possible defences

The ALRC proposes a range of defences to the statutory cause of action namely:

> if the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

> if the act or conduct was required or specifically authorised by or under law;

> if the information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

> if the information was under the law of defamation, privileged.

It is unlikely that any of these defences could be raised by employers in the workplace surveillance context. Rather, employers will need to claim that there was no reasonable expectation of privacy or the act was not sufficiently serious to cause offence to a person or ordinary sensibilities. As already discussed, the use of well drafted and implemented company policies may be the most appropriate method of minimising the risk of employees commencing an action.