

PRIVACY LAWS

Eye on the spy

Privacy laws are finally catching up with technology in the workplace writes *Charles Power*.

There are many ways an employer can intrude on the privacy of people at work: they may retain personal data about their employees, may use closed circuit television or global positioning devices (GPS) to observe or track employees or may monitor work emails and telephone communications.

New technologies have made this easier. Biometric systems, such as facial recognition and iris and retinal scanning, threaten to replace the security card or the time clock. Psychological testing has become the preferred means for selecting and assessing job candidates.

The idea that Australian domestic law should set limits on the extent to which employers can intrude on worker privacy is consistent with Australia's ratification of the International Covenant on Civil and Political Rights. Despite this, the laws that regulate workplace privacy in Australia are inconsistent, far from comprehensive and in most cases lacking any significant mechanisms for enforcement.

The next five years should see dramatic changes in the regulation of workplace privacy in Australia. However, governments at all levels appear to be committed to introducing these changes at a pace that should give employers ample opportunity to revise their practices in line with the new requirements.

IS THERE A RIGHT TO PERSONAL PRIVACY?

Common law protection for personal information has long been available in the form of an action for breach of confidence. Yet it cannot be said, despite some bold judicial pronouncements, that Australian law has recognised a cause of action based on breach of privacy. The High Court left the door open for the development of such a cause of action in *ABC v Lenah Game Meats*. The opportunity was taken up by Hampel J in *Doe v ABC*. Her Honour found that the broadcaster, in identifying a victim of sexual assault, had committed an invasion or breach of privacy being "an actionable wrong which gives rise to a right to recover dam-

ages according to the ordinary principles governing damages in tort".

In its May 2008 report, Australian Privacy Law and Practice (ALRC Report 108), the Australian Law Reform Commission (ALRC) recommended that federal legislation should provide for a statutory cause of action for a serious invasion of privacy. This action would be available in such situations as where an individual has been subjected to unauthorised surveillance, or his or her emails have been interfered with, misused or disclosed, or sensitive facts relating to his or her private life have been disclosed.

Following the release of ALRC Report 108 in August 2008, the Federal Government announced that it would consider the ALRC's recommendation in early 2010. This means that Australians are unlikely to have a statutory cause of action for breach of privacy before the next federal election.

INFORMATION PRIVACY – STILL NOT A REALITY IN MOST AUSTRALIAN WORKPLACES

Australian information privacy legislation requires employers to handle records of personal information about people in their workplace in a manner that is consistent with certain principles.

The primary legislation governing the private sector is the Privacy Act 1988 (Cth) (Privacy Act). However, the application of the Privacy Act to employment relationships in the private sector is largely non-existent because businesses with an annual turnover of not more than \$3 million are exempt – around 94 per cent of all Australian businesses. Furthermore, the Privacy Act does not regulate private sector employers in their handling of employee records directly related to a current or former employment relationship.

There is significant inconsistency in the privacy principles adopted by the various states and territories where laws generally recognise one of two sets of principles – the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs), both of which

are contained in the Privacy Act. Generally, the NPPs set a higher standard for privacy regulation.

THREADBARE REGULATION OF WORKPLACE SURVEILLANCE

State and territory statutes regulating use of video, audio and tracking devices in the workplace is variable and patchy. Employee consent is required for their GPS monitoring and video surveillance in Victoria, NSW, South Australia, Western Australia and the Northern Territory. However, video surveillance in workplace toilets and washrooms is prohibited only in Victorian and NSW. Additional notification requirements for surveillance apply in NSW. Consent is required to record private conversations to which employees are party in all states and territories. However, regulation of computer or internet usage monitoring in the workplace applies in NSW only.

Employee consent is required for their GPS monitoring and video surveillance in Victoria, NSW, South Australia, Western Australia and the Northern Territory. However, video surveillance in workplace toilets and washrooms is prohibited only in Victorian and NSW.

NSW is also the only state in which there is statutory regulation of email monitoring by employers. There is no statutory regulation anywhere of the extent to which employers can engage in practices that involve physical intrusion on individual workers such as genetic testing, drug testing and bodily searches.

Some workplace agreements made under the Workplace Relations Act 1996 (Cth) (WR Act) limit the extent to which employers can rely on the results of surveillance or drug or alcohol testing to discipline or dismiss employees. Moreover, if an employer uses this information to dismiss an employee and the employee challenges that step in the Australian Industrial Relations Commission (AIRC) under unfair or unlawful termination laws provided in the WR Act, the AIRC will usually scrutinise the employer's practices to determine whether they have been fair.

THE WAY FORWARD FOR PRIVACY REGULATION

The most significant development on the horizon for workplace privacy is the possibility that the Federal Government will amend the Privacy Act to remove both the small business and the employee records exemptions. On this basis, then, we could expect that in the next five years all Australian employers will be required to observe the following rules when handling records about their employees and contractors:

- The records must only contain personal information about employees that is relevant to their employment, accurate, complete, up to date and relevant. The records must be kept secure.
- An employee is entitled to access those records (subject to certain exceptions). If the employee disputes the accuracy or completeness of records, the employee is entitled to include a note to this effect in the records.
- The information contained in the records must be collected by lawful and fair means and not in an unreasonably intrusive way. Where reasonably practicable, it must be collected from the employee. If collected from someone else, the employee must be informed.
- Employee consent will be required before collecting certain classes of 'sensitive information' about an employee (for example, medical information).
- Employee consent will also be required to use or disclose personal information retained in a record for a purpose not related to employment (unless this is necessary to investigate a reasonable suspicion that unlawful activity is occurring, or the use or disclosure is required or authorised by or under law).

In the meantime, states and territories are considering a national approach that would regulate workplace surveillance (including email and internet monitoring), covert surveillance practices, surveillance and monitoring of employees outside of work and genetic testing in the workplace, including taking bodily samples. This is likely to be based on the model recommended by the Victorian Law Reform Commission in October 2005 (contained in a report which, to date, has largely been ignored by the Victorian Government).

Charles Power is a partner in the law firm Holding Redlich and an accredited workplace relations specialist. He is a graduate of Monash University with Bachelor degrees in Economics (Honours) and Law.

To view this academic paper in full, see www.mbr.monash.edu.au.