

## MEDIA RELEASE

### **Australian businesses taking risks with unlawful workplace surveillance practices**

*Sydney, 28 January 2009* – With the increased focus on privacy in the workplace arising from the Australian Law Reform Commission's review of privacy laws released last year and the current submissions to the Senate on the scope of Labor's Fair Work bill, businesses are being told to sharpen up their workplace privacy and surveillance guidelines this year to avoid the risk of possible litigation.

According to Harmers Workplace Lawyers, employers across Australia continue to push the boundaries of what may be considered 'acceptable scrutiny' of their employees without any sufficient form of workplace privacy guidelines in place. Often it is only in hindsight, when an employer becomes aware of an incident after conducting surveillance, that an employer steps up to understand their responsibilities when putting their workforce under the watchful eye.

Bronwyn Maynard, Senior Associate at Harmers Workplace Lawyers, said, "I am constantly surprised at how many businesses choose to monitor their employees' actions without having the necessary workplace surveillance and privacy guidelines in place."

"Employers run the risk of breaching privacy and surveillance legislation and subsequently being penalised. While employers have a legitimate interest in ensuring that their employees are acting appropriately and not misusing company resources, any monitoring of their employees must be conducted in the appropriate manner," she said.

The most common types of workplace surveillance are computer and camera surveillance. In New South Wales, for example, this surveillance is governed by the *Workplace Surveillance Act 2005* that imposes on employers a requirement (among other obligations and subject to very limited exceptions) to provide employees with at least 14 days' written notice before undertaking such surveillance. If an employer obtains evidence of wrong doing via surveillance, without following the requirements in the legislation, they may be unable to use this evidence in a court of law.

Ms Maynard advises businesses to develop workplace surveillance policies and raise awareness of the guidelines within the workplace.

The Federal Privacy Act has recently undergone an extensive inquiry by the Australian Law Reform Commission (ALRC), which published its findings in August last year. Based on these findings and subsequent recommendations, it is anticipated that amendments to the Privacy Act may be released later this year.

Ms Maynard said that of particular interest in the report is the impact of developing and new technologies on privacy, such as Blackberry's and wireless technologies such as 'WiFi' and 'Bluetooth'. She said that the ALRC noted in its report that 'devices that use wireless technologies are vulnerable to theft and subsequent

misuse', raising questions about monitoring by employers of such new and increasingly remote technologies by their staff.

"There should be some interesting and significant changes made to privacy and surveillance legislation based on the ALRC report. Employers should be on the lookout for these changes to understand what they mean for their businesses," Ms Maynard concluded.

Practical advice for businesses:

1. Have a written policy on workplace surveillance that clearly sets out that employees may be monitored at work, including:
  - the method of surveillance (camera, computer or tracking device/GPS), where it will take place and the means (random monitoring of inboxes/outboxes, examining logs of internet use or installation of cameras);
  - who will conduct surveillance (IT staff, human resources or line managers);
  - whether surveillance is continuous or intermittent;
  - whether surveillance is for a specified limited period or ongoing;
  - when and what email or Internet websites will be blocked.
2. Ensure that the policy has been brought to the attention of all employees in such a way that it is reasonable to assume that employees are aware of and understand it. Employers should:
  - distribute the policy to each employee at least 14 days before surveillance commences;
  - ensure the policy (including any consequences of failure to comply) is explained to employees. For a larger employer, this could involve induction and training courses; for a small business, this could involve individual discussion of the employer's policy with each employee;
  - provide employees with regular reminders about the policy (for example, by "all staff" emails, or via the staff noticeboard);
  - ensure all new employees are informed of the policy before they commence work.
3. If employer's block email (other than "spam", email which might damage the computer network, or menacing, harassing or offensive email), employers should ensure there is a system that provides employees with a "prevented delivery notice" each time an email sent to, or by, the employee is blocked.
4. If employers have installed camera surveillance, ensure the camera (or its casing) is clearly visible and the required signs are posted at the entrances of the area under surveillance.
5. If employers have installed GPS or other tracking devices in any vehicle or mechanism used by their employees, ensure the required notice is clearly visible on that vehicle or object.

Ends

**Note to editors:**

***About Harmers Workplace Lawyers***

*Harmers Workplace Lawyers was established in 1996 as a boutique employment law firm. Since then it has become one of Australia's leading employment and industrial law firms, with offices in Sydney, Melbourne and Brisbane. The firm has been awarded Australasian Legal Business's 'employment specialist firm of the year' for the past three years running.*

Issued by Sefiani Communications Group on behalf of Harmers Workplace Lawyers

For further information, please contact:

Lauren White or Dylan Malloch

Tel. (02) 8920 0700

Email: [lwhite@sefiani.com.au](mailto:lwhite@sefiani.com.au) or [dmalloch@sefiani.com.au](mailto:dmalloch@sefiani.com.au)