THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: EmploymentLawCommittee/VK/431437

27 January 2011

Director
Policy, Legislation and Criminal Law Review
NSW Department of Justice and Attorney General
GPO Box 6,
SYDNEY NSW 2001

By email: lpd.enquiries@agd.nsw.gov.au

Dear Sir/Madam,

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

The Employment Law Committee (the "Committee") of the Law Society of New South Wales is pleased to provide the following submission in respect of the Review of the operation of the *Workplace Surveillance Act 2005* (NSW) (the "Act"); whether its objects remain valid; and, whether the terms of the legislation remain appropriate for securing that objective.

The Committee members, who practice extensively in the employment law area, have considered the objects of the Act, the second reading speech and their own professional experience in relation to the operation of the Act.

The second reading speech reveals that the Act had been the subject of consultation for over 12 months from June 2004. The primary concern was a view that the *Workplace Video Surveillance Act 1998* (NSW) was not wide enough to protect employees from obtrusive acts of covert surveillance. The particular concern was that essentially private communications may end up being intercepted and read by employers. Concern also existed around the advance on GPS tracking devices.

Technology moves quickly and advances since 2005 now see large numbers of employees with private access to email and the internet through home computers and personal mobile devices. In addition internet cafés are in abundance providing access away from work. Employees are no longer totally reliant on work computers for purely personal and private use. Further email communications and internet use has become a primary means for business communication. Social networking sites were once generally banned by employers but now businesses are using them as business tools. Experience also shows that email communications and internet use are not truly private. Internet search engines and other applications trace movements and the daily newspapers show how emails can be widely published.

The Committee is aware of only three instances in which the Act has come before the court. In 2006, a potential prosecution involving Centrelink was not pursued by prosecuting authorities. In 2010, Australia Post brought Federal Court proceedings seeking a declaration that the Act did not apply to it. Those proceedings do not appear to have been continued beyond an initial application to stay the proceedings.

It was reported in July 2010 that a mine worker commenced proceedings in Newcastle against Austar Coal Mining Pty Limited in respect of covert camera surveillance, the alleged camera being hidden in a lever arch folder. The outcome of these proceedings is unknown.

The limited judicial consideration of the Act may suggest that it is working effectively, or alternatively, that any non-compliance has not raised real issues for employees. However, the ability to review emails for legitimate business purposes has, in the Committee's experience, arisen on many occasions for employers where there were doubts about compliance with the notice requirements. This has raised legitimate business concerns about the ability to track and use business communication.

The Committee believes that it is time to draw a distinction between computer and internet use and improper surveillance. The Act's current structure essentially provides that the failure to give a notice makes any surveillance covert and the absence of an authority creates an offence. While the Committee supports the concept of transparency and fair dealing with employees, it does not consider that the failure to give a notice in respect of computer and internet use should give rise to an offence or give rise to an argument that computer records cannot be used in criminal or civil proceedings, including discipline proceedings.

In balancing the rights of employers and employees, consideration needs to be given to the privacy regimes and the protections that they provide to employees in respect of truly personal information. The privacy regimes provide a strong protection to employees.

The Committee draws a distinction between the tracking and reviewing of emails and internet use and surveillance that may be in the form of "spyware". It is now commonplace for employees to use work computers for internet banking and other secure transactions. It would not be appropriate for an employer to be able to track computer use to capture account details and passwords and thereby effectively "steal" secure information from employees. The use of any such device should be included in Part 4 as part of the covert surveillance provisions as in our view the only legitimate use of any such device is if an employee is suspected of being engaged in an unlawful activity.

The Committee endorses prohibitions on vision surveillance as they currently stand within the Act and as apparently alleged in the proceedings against Austar Coal Mining Pty Limited. The need for cameras to be overt and for appropriate notices to be installed is now a standard expectation.

The Committee's experience on tracking surveillance indicates that it has become a more common business tool to assist in better consumer service. However, its use is by no means as widespread as computer use. The Committee considers that it may remain appropriate to require that vehicles fitted with tracking surveillance equipment carry a notice in that respect.

Thank you for the opportunity to comment.

Yours sincerely,

Stuart Westgarth
President