Surveillance in the workplace

JOE MURPHY
DIRECTOR AUSTRALIAN BUSINESS LAWYERS & ADVISORS

Technology in the workplace is rapidly changing and becoming increasingly mobile. As a result, the law has been forced to evolve to ensure it keeps up with developments in this field.

A number of recent employment-related cases have highlighted the need for employers to ensure they have a comprehensive policy in place. The policy needs to address the issues of technology use at work, in connection with employment (which may extend to out-of-hours use), and the surveillance of those activities by an employer.

It is easy to understand why employers tend to view the use of their technology as a licence to monitor and dictate what their employees do with that technology. However, in order to avoid breaches in privacy or workplace surveillance laws, it is important for employers to have a policy that is compliant with privacy and surveillance laws. Here are 10 tips to help you formulate a policy:

TOP TIPS

1. Ensure your business has a workplace surveillance/information technology policy that accommodates your video surveillance, global positioning systems (GPS) technology, and computer/data surveillance (including access and storage processes).
2. Ensure employees know about the existence of the policy, understand the policy and acknowledge their understanding of it.
3. Ensure the policy covers all forms of surveillance (computer, GPS and video/camera).
4. Understand your legal obligations regarding all forms of surveillance (laws vary between states and territories).
5. Ensure the policy clearly states that all use (including personal) of company equipment is monitored and that employees should not expect privacy.
6. If the policy allows for personal use, include the restrictions and obligations that apply to that use; e.g. outline expectations about the quantity of personal use allowed.
7. The policy should notify employees of the types of company property that are monitored.
8. When emails are blocked, employees should be notified that an email addressed to them has been blocked and from whom it was sent.
9. Ensure employee passwords and login details are kept confidential.
10. Make sure you also comply with your policy. Schedule annual policy reviews and update the policy in response to changes in legislation.