ThomsonsLawyers

Employment and Safety Alert February 2011

Privacy and Policies - After Hours

The Federal Court has upheld the decision to dismiss an employee for viewing pornography on a work-supplied laptop while at home, outside of working hours.

In this case, *Griffiths v Rose* [2011] FCA 30 (31 January 2011), the employer's Information Communication Technology Policy (**Policy**) prohibited the use of facilities to access pornography. The employer, the Commonwealth Department of Resources, Energy and Tourism (**Department**), installed monitoring software on all laptops which recorded searches for programmed keywords and also took screen shots at 30 second intervals. A routine search revealed that Mr Griffiths had accessed prohibited websites on a number of occasions.

To make matters worse, during the Department's investigation of his conduct, Mr Griffiths offered implausible excuses to justify his conduct. It was this factor, rather than the act of viewing the pornography that ultimately led to the Department's decision to terminate his employment.

The Case

Mr Griffiths sought to challenge the termination decision in a number of ways, including asserting that:

- the laptop was not covered by the Policy;
- the monitoring of his use of the laptop in his home was in breach of the *Privacy Act 1988* (**Privacy Act**) and his common law right to privacy; and
- the decision to terminate his employment was an unreasonable exercise of the Department's powers.

Findings

The Court held that:

- the laptop was a 'facility' as specified in the Policy;
- the Department's collection of information was lawful and reasonable, because the Department had a legitimate interest in monitoring the use of its property. The collection of information was also fair, because Mr Griffiths had read and signed the Policy, and was aware that his use of the laptop could be monitored. The Department had not breached the Privacy Act or common law rights to privacy;
- the decision to dismiss Mr Griffiths' employment was not only based on the viewing of the websites, but also the employee's implausible explanation for accessing the sites; and
- the decision was therefore reasonable.

Despite the outcome, the Court noted that monitoring software used by employers to collect personal information (such as banking details) could possibly breach privacy rights.

Implications

This is an important case emphasising the need for clear policies and communication of obligations, rights and consequences.

continued over page

Employers should take care to ensure that all policies dealing with company property and IT:

- stipulate how property and facilities can be used, and explicitly extend the prohibitions on improper use to uses away from the workplace and outside work hours;
- comply with appropriate legislation regarding workplace surveillance and privacy;
- are current and regularly updated;
- are readily accessible; and
- have been acknowledged by all staff, particularly where staff are provided with employer owed equipment.

Employers should also ensure that they set up monitoring software in ways that minimise the risk of breaches of privacy legislation.

Any workplace investigation must be conducted with due process, and disciplinary action which is to be taken must be proportionate to the conduct. An employer who is misled by an employee during an investigation may be able to rely on that deception, as well as the issue of improper conduct, to justify a dismissal.

For further information, please contact:

Mark Branagan
Partner
+61 3 8080 3638
mbranagan@thomsonslawyers.com.au

Karl Luke
Partner
+61 8 8236 1280
kluke@thomsonslawyers.com.au

Paul Ronfeldt
Partner
+61 3 8080 3533
pronfeldt@thomsonslawyers.com.au

Jacquie Seemann
Partner
+61 2 9020 5757
jseemann@thomsonslawyers.com.au