



Net and email abuse is no cyber myth

By **Tony Wood**, Partner and **Millen Lo**, Solicitor, Freehills

🌀 Risk awareness

🌀 Relevant case law

🌀 Equal opportunity issues

It is a business tool, isn't it?

Employers who think that they are risk free from the cyber activities of their staff are best to look at developments in the last twelve months or so in the legal arena.

Recent developments in the law point out the importance of implementing and communicating company policies which deal with the accessing, transmission and storage of inappropriate material on the company's IT infrastructure.

A failure by employers to maintain vigilance in this area can leave them exposed to claims such as unfair dismissals and discrimination or harassment claims in the equal opportunity jurisdiction.

In the legal world

Over the last year we have seen some notable decisions handed down by the Australian Industrial Relations Commission (AIRC) in applications brought by employees who have been dismissed for inappropriate use of the internet and email. These cases are now generating an increasing interest amongst employers who had never thought about these types of issues before.

While the legal risks associated with misuse of the internet and email are not necessarily confined to issues arising in the equal opportunity area, recent decisions in this area show that it is a key area of liability for companies.

What is also particularly interesting is how industrial tribunals are delving into areas perhaps traditionally thought to belong to the

equal opportunity jurisdiction. Surprisingly enough, the equal opportunity tribunals themselves are yet to really consider this issue of internet and email use.

How is internet and email usage an equal opportunity issue?

For those who may not be convinced or are unsure how an email or accessing a web site may fall foul of the equal opportunity laws, the Human Rights and Equal Opportunity Commission (HREOC) has provided some guidance to employers in their publication *Sexual Harassment A Code of Conduct*. The *Code* provides that sexual harassment not only includes unwelcome physical touching but also includes offensive communications such as email messages and inappropriate screen savers and arguably any other inappropriate and offensive material of a sexual nature obtained in an electronic form from the internet. It also means that offensive jokes circulated by email may also fall foul of the equal opportunity laws including the race and disability discrimination laws if the jokes are derogatory. And there is certainly no doubt that pornography in the workplace in whatever form can be unlawful conduct.

What are the cases saying?

The recent spate of cases dealing with misuse of company IT technology have primarily dealt with the inappropriate access, storage and distribution of pornographic material.

In these cases the relevant industrial tribunals have sought to identify whether the employer had any relevant policies which dealt with the conduct in question, before proceeding to review their content and implementation in the workplace.

There is a general acceptance by the industrial tribunals that inappropriate internet and email use in this way is a valid reason for termination of employment (and in some cases summary dismissal).

In *Ueckert v Australian Water Technologies Pty Ltd* (25 July 2000), the NSW Industrial Relations Commission accepted that the applicant had been engaged in serious sexual harassment, conduct which included the accessing of pornographic sites and intimidation of co-workers. The Commission noted in particular:

It is trite for the Commission to observe that there is absolutely no place, or reason for, the harassment of one employee by another employee, be it sexual or otherwise, in, or outside the workplace. Indeed, such behaviour is unlawful. Where proven, it will, in

Employers should review their policies from time to time. Policies do outdate and if they are not regularly revised and kept relevant, they may not necessarily protect a company from liability.

my view, be a sound basis for disciplinary action and, if the behaviour continues, or is of a serious nature, it may constitute grounds for summary dismissal.

The Commission subsequently decided that there was no ground to intervene in the dismissal.

In two decisions handed by Senior Deputy President Watson of the AIRC late last year, the Commission also found in favour of the employer where in both cases the dismissed employees had accessed

pornographic material in the workplace.

In *Klopsteins and Holden Ltd*, SDP Watson in finding for the employer noted that the employee's conduct:

was in breach of the company diversity policy, the content and the implications of which were made clear to the applicant. A company presentation explained the policy to employees and was attended by the applicant on 9 December 1999. The applicant recalls a video presentation which formed part of the broader

continued over

Code of Professional Ethics and Conduct

- Chartered Secretaries Australia (CSA) requires its members to observe the highest standards of professional conduct and ethical behaviour in all of their activities. By maintaining such standards, members enhance their own standing as corporate managers and increase public confidence in the management and administration of corporations.
- Members shall uphold the Objectives of CSA and abide by the Regulations.
- As the conduct of an individual member can reflect upon the wider profession of corporate management and upon CSA's membership as a whole, the Code sets out what are deemed to be appropriate standards of professional conduct.
- Members shall refrain from conduct or action which detracts from the reputation of CSA.
- Members are required to exercise complete probity, honesty and diligence in carrying out their duties and responsibilities.
- Members shall at all times safeguard the interests of their employers or clients provided that members shall not knowingly be party to any illegal or unethical activity.
- Members shall not enter into any agreement or undertake any activity which may be in conflict with the interests of their employers or clients or which would prejudice the performance of their professional duties.
- Members shall not use confidential information gained in the performance of their duties for any personal gain nor in a manner which would be detrimental to their employer or client.
- Members shall exercise due care and diligence in performing their duties and ensure the currency of their knowledge, skills and technical competencies.
- Members acknowledge that this Code is to be adhered to both in spirit and to the letter, so that members' conduct is governed by the highest standards of professionalism and ethical behaviour.

Employers should be aware of ... emerging issues dealing with the provision of IT infrastructure to persons wishing to work from home.

policy presentation. In the video the company clearly explained the rights of employees and the responsibilities of employees under its diversity policies.

SDP Watson also noted that the consequences of the breach of the policy were clear in that discipline and dismissal could result, as well as the individually being personally subject to litigation themselves.

The other decision is that of *Toyota Motor Corporation and Automotive, Food, Metals, Engineering, Printing and Kindred Industries Union*. It involved the dismissal of two employees who had breached the company's Equal Opportunity/Diversity Policy. It is interesting to note that the dismissals came about from the investigation of a complaint about a sexually explicit joke sent by email which lead to broader investigations subsequently involving these two employees.

In the course of the decision the Commission commented that the two employees should have been aware of the policy which prohibited the storage, receipt or transmission of pornographic material electronically, that one of them had attended a three hour training session on the company's EO policy and both were aware of the 'pop up' screen which provided they read and adhere to the policy.

The Commission subsequently

found that despite the long and otherwise satisfactory service of the employees their summary dismissals were not harsh, unjust or unreasonable. The Commission held that the nature of the conduct, the communication of the policy and the consequences of its breach and general awareness made this type of conduct inappropriate in the workplace.

Notably, SDP Watson also rejected the applicants' argument that the email communications were private. His Honour concluded that they 'occurred on company equipment, at company premises, within working time, in breach of a clear policy'.

Minimising the associated risks of staff internet and email usage

The overall lessons from the recent cases can be summarised as follows:

- employers should have an equal opportunity policy that is comprehensive so as to cover misuse of the internet and email by staff
- such a policy should point out the consequences of breach (discipline and dismissal if appropriate)
- the policy should be promulgated routinely and staff trained.

In the Toyota and Holden cases, the AIRC was clearly satisfied that they had addressed these issues successfully.

Given the growing concern of regulation of internet and email use by staff, the office of the federal Privacy Commissioner has also been prompted to release a set of guidelines when formulating or improving on existing policies. The *Guidelines on Workplace Email, Web Browsing and Privacy* go beyond

addressing equal opportunity and look at associated privacy and security issues. The guidelines can be found on the Commissioner's website www.privacy.gov.au.

Briefly the guidelines contain six points:

- The policy should be well communicated and understood by staff.
- The policy should articulate what is permitted use and inappropriate use. Notably, the Guidelines provided by the Privacy Commissioner indicate that a policy which simply provides that sanctioned use is limited to 'work-related' use may be inadequate.
- The policy should provide what information is logged (for example, sites visited and time spent on those sites) and who can legitimately access staff emails and browsing logs.
- The policy should refer to the company's computer security policy.
- The policy should provide how the company will monitor staff compliance with respect to email and internet usage.
- The policy should be regularly reviewed in line with technological developments. The policy should be reissued when significant changes are made to it.

What's in store: emerging issues

The year 2000 has seen some of the ramifications of allowing staff access to IT technology come to the surface. However, it would be naive to conclude that the only issues which can arise relate to incidents of sexual harassment.

One interesting issue which employers should be aware of concerns dealing with the provision of IT infrastructure to persons wishing to work from home. In a

decision handed down by the Victorian Civil and Administrative Tribunal in April last year the Tribunal found that a failure to provide a modem line to an employee's home to enable them to continue to work full time amounted to discrimination based on the employee's child-raising responsibilities. The applicant had requested that her work arrangements be altered to allow her to look after her child at home. Notably, the Tribunal determined that the provision of modem line was a reasonable accommodation and awarded the applicant \$161,307.40 as compensation (*Schou v State of Victoria*).

We anticipate that another emerging issue will be the accessibility of IT technology by staff with disabilities. HREOC has recently released its report entitled

Accessibility of electronic commerce and new service and information technologies for older Australians and people with a disability. While the report primarily deals with the accessing of e-technology by people with disabilities as customers, the issues raised in the paper raises some interesting questions for employers as well. The Commission's report can be found at www.privacy.gov.au.

Final comments: 'I have a policy. I'm protected?'

There is no doubt that the internet and email are powerful business tools. If employers allow their staff access to these tools, then it makes sense to regulate their use.

The measures which employers should at least consider are:

- Reviewing their internet and email usage policy and equal

opportunity policy to see if they are consistent. Some employers may find that while their internet policy is comprehensive their equal opportunity policy is not or vice versa.

- Ensuring staff are made aware of the relevant policies (both EO and IT/security policies).
- Reviewing their training program on relevant policies.
- Regular review of the relevant policies and training programs.

Wherever you start the process it is clear that simply having a policy may not be necessarily providing adequate protection. Employers should review their policies from time to time. Policies do outdate and if they are not regularly revised and kept relevant, they may not necessarily protect a company from liability.

And you thought you couldn't give an analyst briefing in several places at once.

Some of Australia's top 100 companies have discovered the benefits of using **announcetv's** web casting expertise.

For live or on-demand annual general meetings, result announcements and analyst briefings, being in more than one place is now a simple exercise. Let us show you just how simple and cost effective our solutions are. Call Jacqui Begbie on 02 8232 9067.

