corporate lawyer

spring 2005 issue

ISSN 1176-7081

Corporate Lawyers Association of New Zealand

Michael Wigley

on-line porn and other **workplace vices**

Earlier this year porn on Police computers hit the news and caused a media frenzy. However, for all organisations, porn is just one aspect of on-line risk (and that risk is legal, reputational, etc). Technology and process solutions such as traffic filters, audits and firewalls are the first line of defence, however, more is needed and in-house lawyers can play a role in limiting the risks.

It would be dangerous to focus on a single risk (such as porn) to the exclusion of others like security, defamation, copyright and privacy. In fact security/privacy risk is a much greater risk anyway.

An Acceptable Use Policy (AUP) is key, yet it is common for AUP's to be inadequately drafted. Often they don't properly form part of the contract with an employee or contractor, which can create problems if issues arise (for example, in a personal grievance situation where the employer struggles to prove its case).

On-line use by employees and contractors can be problematic for organisations in various ways. For example:

Copyright: Use and distribution, via a work computer, of pirated or unlicensed proprietary software can expose the organisation legally

Defamation: An organisation might be liable for its employees' defamatory statements via email, just as a library or a bookshop can be liable for a defamatory book on its bookshelves (subject to certain defences).

Pornography: Although unlikely, an organisation might be prosecuted based on the strict liability aspects of the porn legislation

Security: Risk is wide-ranging, from potential liability to third parties where a virus is spread, through to liability for loss of information (contract and tort risk)

Privacy: The Privacy Act and the law of confidentiality raise a number of issues, including concerns overlapping with security (such as protection of on-line information). Risk is not limited to New Zealand of course, so overseas laws can become relevant.

Dealing with these issues in an AUP can be awkward. To take porn as an example, it is quite common for AUP's to define unacceptable pornography based upon the prosecution-related definitions in the Films, Videos, and Publications Classification Act 1993. Only particularly bad porn is included such as child porn, violent sex etc. However, context may be relevant. For example, an email sent by a male to a male colleague could have a different impact than the same email sent to a female colleague, highlighting the difficulty of defining what is 'unacceptable'.

Thus, while things will fall between the cracks either way, it's probably better to take a flexible approach in outlining what is or is not acceptable, rather than being too prescriptive (and to avoid using the statutory definition). Typically, AUP's are stand-alone documents cross-referenced in the employment contract. This is the way it should be, in particular because AUP's will need to be updated to take into account, among other things, corporation-wide policy changes (for example in any relevant collective employment agreement), new risks and security threats etc. Both contract and employment law allow for such post-contract changes in AUP's. We set out more detail on this and other issues in an article at www.wigleylaw.com : 'Police On-line Porn Blitz: Implications for other organisations'.

There is an important practical and legal question: 'How should the employee acknowledge acceptance of the AUP?'

The safest way is to have it signed. However, it's common for the AUP to lurk in a personnel manual or simply to be located on-line somewhere. There is a problem with this: when and if the AUP becomes an issue, the employee may be able to say (as has

continued on page 5

inside... finding the right balance
... weighing up individual risk ... preparing for mediation
... protection of tax advice from disclosure
... Law Awards ... the winners

continued from page 1

happened in court cases) that he or she had no notice of the AUP and therefore it is not binding.

Even on-line 'click accept' requirements (both of the original AUP and any change) can have problems as we explain in the article referred to above. In large organisations, it is often thought that having on-line 'click-accept' of a new or changed AUP strikes the right balance between risk and practicality. However, that assumption will not apply in every case.

We believe that the way in which the AUP is required to be accepted is just as important as the contents of the AUP itself.

In practice, new employees should sign the AUP (the employer shouldn't just rely on a cross-reference to the AUP in the employment agreement). That's easy enough - as they are signing the employment agreement anyway. When introducing new AUP's for existing staff, or changing the existing AUP, smaller organisations might still get acceptance in handwriting whilst larger organisations should look at a 'click accept' solution.

The AUP needs to be practical and to reflect reality. For example, if reasonable personal use of the Internet is accepted by the organisation, it would be counter productive to state in the AUP that it is not permitted.

Finally, having put an AUP in place, the AUP and its contents should be reinforced consistently and in various ways, such as during on-line security training sessions.

In summary, legal and reputational problems in relation to on-line use in organisations have been simmering away for some time. Many organisations have inadequate AUPs, and fail to make sure they are properly signed up to by employees and contractors. However, by taking some simple steps, improvements are relatively easy to implement. **CL**

Michael Wigley is the principal of Wigley & Company. He specialises in IT telecommunications and procurement, ranging from contracts and strategic advice through to litigation. He is president of the Technology Law Society.