



STAY ON SOLID GROUND

June 2002

When the tectonic plates of assumed employee privacy and enterprise security begin to grate, friction can be relieved only with clear understanding and a fair touch.

Scores of Australian organisations, including Telstra, Holden, Colonial and the NSW Police Service, have sacked and disciplined workers in the past three years for personal use of the Internet at work.

Last year, the analyst Red Sheriff found that Australian workers who did not have Internet access at home spent 3.6 hours a week surfing the Web at work, at a cost of \$312 million. In the United States, Computer Security Institute, which conducts an annual cyber crime audit with the FBI, found that 91% of respondents detected employee abuse of access privileges.

A US study by the Society for Human Resource Management found that 74% of corporation monitor their workers for cyber crimes. There are no firm figures for Australian organisations.

US workplace academic Bradley Alge advocates clearly defined acceptable-use policies devised in consultation with workers that include:

- Reasonable personal use of the Internet, for instance for Internet banking and dealing with government.
- Identifying specific behaviour, such as downloading pornography, that is not allowed.
- Explaining when monitoring is likely to occur.

There are compelling reasons for monitoring: complying with legislation on equal opportunity, protecting intellectual property, and ensuring that the network does not get bogged down. Chevron paid out \$US2.2 million three years ago to workers who brought a sexual harassment case over a dirty joke sent by e-mail.

But Bradley Alge of the Krannert Graduate School of Management at Purdue University in the US has found that surveillance can be counterproductive. "Electronic monitoring can create an environment of mistrust between managers and employees, particularly when monitoring systems are primarily designed to catch or punish employees." Alge says that, instead, employers should give employees freedom to search serendipitously on the Web, thereby retaining a creative workforce.

SafeWeb co-founder and chief executive Stephen Hsu says: "The attitude generally in Silicon Valley is that workers work long hours, and the way employers make that more beatable is to allow personal activities in the workplace."

SurfControl Australia managing director Charles Heunemann says employers should be realistic about workers using corporate resources for personal matters. SurfControl makes content-filtering software.

A recent study by CSIRO discovered that filtering software let through up to 80% of pornography and other objectionable material.

Jim Tyre, a US lawyer and co-founder of the Censorware Project, says: "The use of censorware technology in the workplace is, at best, counterproductive. Unless the employer strictly prohibits employees from using the telephone to make personal calls, why should Internet usage be treated any differently?"

Jack Andrys, chief executive of the Perth-based WebSpy, which makes software for monitoring online activities, says lunch breaks could be “free for alls”, allowing workers to surf unfettered with the exception of objectionable sites. “If misuse is detected, the employer should not over-react and should review the person’s overall effectiveness.”

Digital-Age philosopher and former IBM executive Jonas Nader says he has no problems with banning private use of the Internet; just don’t ask workers to be creative. And he says that if you become aware of something in the course of monitoring, you could be liable, especially if that information is later misused by the staff conducting the scan.

Policeman turned KPMG computer security consultant Rod McKernmish says most IT departments do not have the forensic skills to stand up in court.

The Officer of the Federal Privacy Commissioner advises that to comply with the Privacy Act, workers should be warned if their activities or e-mail are being monitored.

Sam Greengard, who has written on privacy in the workplace for *Workforce* magazine over several years, says: “If committing espionage or theft, sorting through e-mail and voicemail might be acceptable. But it’s not acceptable on a routine basis just to listen in. If a worker gets the work done, that is what really matters.”

Management Magazine