

# TAMING BIG BROTHER



*Jean-Paul Pelosi runs the magnifying glass over the new Workplace Surveillance Bill in NSW*

**S**ince the arrival of the internet, we've been better placed than ever to satisfy one of our main drives - our curiosity. Before the internet, there was little chance of finding photos of Angelina Jolie or checking the weekend footy results via your computer.

The flip side was that our employers' curiosity was also stifled. As the saying goes, 'no news is good news' and in terms of news penetrating the office walls, it must have been all good as far as the boss was concerned.

Nowadays, the 'news' is coming thick and fast. Many employers feel a need to monitor the activity of their employees, thereby running the risk of encroaching on privacy. Perhaps the new Workplace Surveillance Bill will at least provide some counterbalance to ensure things don't get out of hand.

## Protection or problems

The idea behind the new Bill, passed on 24 May, is both to help protect employee privacy and to better define when workplace surveillance is acceptable. But there seems to be some confusion as to how the law will be practically implemented. For example, computer surveillance (which is perhaps most important to the average employee) has an ambiguous definition.

According to the Second Reading speech delivered by NSW Attorney-General Bob Debus, computer surveillance is "surveillance by means of software or other equipment that monitors or records the information

input or output, or other use, of a computer. It includes the sending and receipt of e-mails and the accessing of internet websites."

Sophie Dawson and Arthur Artinian, lawyers from Blake Dawson Waldron, suggest the definition has a "potentially broad application" and that its interpretation will depend on the courts. Dawson and Artinian warn that employers should aim to have suitable measures in place before the Bill becomes an Act, such as outlining an employee agreement and appropriate compliance policies. These basic steps should ensure that any potential confusion is minimised.

Another problem may occur in the interpretation of "justified surveillance" or "reasonable suspicion" of wrongdoing. The Bill provides that employers are allowed to conduct surveillance as long as they meet a general notice requirement of 14 days and specific requirements for each surveillance type. So computer surveillance can be used in conjunction with this notice and, when the employer's computer surveillance policy is properly established, with the employee. But the surveillance must be carried out within the boundaries of this policy.

National retail practice manager Geoff Whytcross of Talent 2 sees some inherent flaws in the Bill's design. "If they [the employer] thought Geoff Whytcross was sending confidential information to a competitor, then they would have the right to check my e-mails," he says. "But how much information do they have to have?"

Whytcross believes the lines of reasonable suspicion are murky. "Because I'm very

good friends with one of my competitors and that competitor starts doing quite a bit of business - is that reasonable suspicion that I'm passing information on?" he asks. "Or if Geoff Whytcross resigns does that give you the opportunity to check every e-mail I've sent in the last six months?"

Recent research undertaken by Talent 2 shows that 91% of employees believe they have the right to privacy, but conversely, 82% say there are mitigating circumstances where employers should have the right to spy on staff. Whytcross says of the contradiction: "A lot of people feel it's ok for companies [to spy], as long as it's not on them."

## Employer perspective

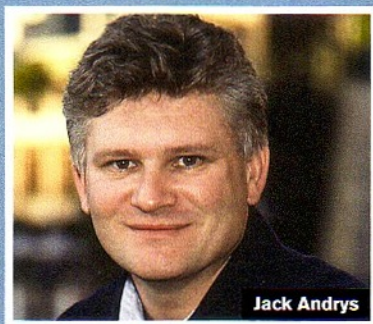
The proposed legislation seeks to make surveillance transparent in the workplace, encouraging employers to be open about their practises. While this should reduce much of the anxiety on the subject, Chair of the Australian Privacy Foundation Anna Johnston says the Bill is actually quite harsh on the employer.

"One of our concerns with the Bill is the way it's been drafted," Johnston says. "It means that even if an employer is trying to do the right thing and comply with the rules about overt surveillance, if they only give 13 days written notice instead of 14, for example, the law will punish the employer.

"So we think the very structure of the Bill and the way it operates is problematic. For employers it's a high risk situation," she says.

Johnston also says the Bill offers nothing new in the way of protection for the employee: all that changes is that they are given official notice. "They're not necessarily going to have any power to stop the surveillance and the Bill doesn't provide any protection against the employer misusing anything they gain from surveillance," she argues.

Jack Andrys, CEO of electronic surveillance company Webspy, agrees the Bill offers nothing new. "I don't see how it will change anything that we've put out before internally," says Andrys. "What they're



Jack Andrys



Fab Zincone

saying in the Bill is what we've been saying from day one: that it's perfectly alright to monitor employees as long as they know about it and they sign off on that. In all honesty I think the Bill is there to prevent that blatant, personal attack on people as far as privacy is concerned."

Andrys says Webspy, which predominantly sells products that monitor and report internet traffic flow, will not be affected by the new legislation one way or the other.

## **A LOT OF PEOPLE FEEL IT'S OK FOR COMPANIES [TO SPY], AS LONG AS IT'S NOT ON THEM**

He adds that Webspy has always advocated being open about 'spying' as the products protect both employers and employees. "Quite a few people have been falsely accused of doing the wrong thing with PCs and our product has proven that they haven't - it works both ways."

### **The debate continues**

As technology grows, so too will curiosity. Hopefully a balance between both can be struck. "I think the NSW government should be congratulated for trying to achieve

a balance in the workplace on a rapidly-expanding technology that has the potential to be exploited," says the national secretary of the Australian Workers Union, Bill Shorten.

Andrys says that in the end, monitoring staff does not have to be an invasive activity. He suggests monitoring traffic flow is all that is needed in workplace computer surveillance. "When you look at the spying aspect of it, all the product's doing is actually reporting the normal transactions within an organisation, that in ninety-odd per cent

of the cases have already been logged and already exist," he says.

IT manager for Kogarah Council, Fab Zincone, says he has found the presence of Webspy makes all the difference. "People know I can do reports on internet usage and that alone is usually enough to deter them," he says. He explains that the extent to which a company implements surveillance depends on their need to protect information. "In our line of business, I guess information isn't that crucial."

"I think the best thing this Bill does is create a debate," says Shorten. "A debate which says there are limits to unfettered discretion of employees or employers is good." **HC**