Wigley & Company

BARRISTERS and SOLICITORS

On-line Employee Privacy versus Employer Protection

How far can organisations intrude into employees' online activity? What's the optimal approach? This is Wigley & Company's presentation at the 12th Annual IT Security Summit in Auckland: April 2007.

IT security in organisations is an ever-growing problem. Employees and others[1] have greater access within expanding IT and telecommunication system boundaries such as mobiles, PDAs, wireless access, internet access and so on.

When so much is at stake, it is remarkable how organisations still take a great deal of risk in the critical "people" aspect of IT security. For example, increasingly, an organisation's intellectual property is a major asset, which is at risk of being hacked or taken (often via employee actions) in this computer and internet-oriented world.

Here we outline some of the issues in handling online security and access, first by dealing with the successful appeal of two employees in a recent case[2]. The challenges faced by the employer in that case are typical of those faced by many organisations.

Then we address how far an organisation can intrude into an employees' privacy.

We also note some best practice tips for implementation of online policies.

What happened in the case?

In 2003, Air New Zealand looked at the issue of excessive personal use of the internet and online porn, in its engineering division.

Having selected what the employer said were its top 13 culprits, there were dismissals. Two dismissals were appealed to the Employment Court. The Court said the two employees were unjustifiably dismissed.

The judgment demonstrates potential problems when going through a disciplinary process around computer and internet use. The employer had brought in a contractor to handle this. Observations range from the way in which the various meetings were handled during the dismissal process, through to use of unreliable internet access data, a fact that was not communicated to the employees.

Anyone relying on evidence from computers in a court case (whether or not in an employment disciplinary context) will find the judgment to be useful reading.

However here we focus on the case to the extent it covers internet and computer use policies, and whether employees are sufficiently aware of those policies.

In observations that apply to all organisations, the Judge said[3]:

> *"As misuse of the Internet can lead to dismissal, [the employer's] responsibility was to ensure by specified means that its policy was known to those who had access to the Internet. It could reasonably have been expected that at the time any new user is given access to the Internet, they be provided with a specific reference to the policy either by a direction to the appropriate place on the Intranet or in a written document. That was not done for either [of the two employees].*

[1] Contractors and others that use the organisation's computer systems.

[2] *Cliff and Groom v. Air New Zealand Auckland*, 23 August 2006, ARC 50/05; ARC 51/05; AC 47/06, EC, Shaw J.

[3] At paras 136, 137 and 141.

> *It was also unhelpful for [the employer's] Internet policies to be in several different locations and unwise for policies not to be clearly described to any employee obtaining access to the Internet for the first time.*
>
> *… [B]oth men were aware that while they could use the Internet for personal use there was a limit based on reasonable use. This unfortunately is a vague term for any employee to interpret in the absence of defined guidelines."*

A Court of Appeal decision[4] confirms that, while an employer must take reasonable steps to ensure that employees are made aware of policy requirements, employees are also under an obligation to acquaint themselves with those requirements and to comply with them. Where the employer has taken reasonable steps, claims of ignorance by employees may not assist them.

But that only goes so far, as the Judge said in the Employment Court case:[5]

> "*The [employer's] investigators were reasonably sceptical of [the employee's] claims about their lack of knowledge of their policies. As longstanding employees they were expected to be familiar with them and keep themselves up to date. That is a reasonable expectation but equally the employees are entitled to clear and unambiguous statements of the policy particularly where a breach could, as in this case, lead to the most serious consequences of dismissal."*

Peter Chemis has recently provided a very useful overview of the approach to drafting an internet and email policy:[6]

> *"In our view, the best strategy for preventing and dealing with pornography (and other internet or email misuse) in the workplace is to:*
>
> 1. *Have in place a clearly defined policy, contained in one document, that regulates the use of internet and email;*
> 2. *Make compliance with that policy a contractual obligation;*
> 3. *Train employees about the policy. Also, have them sign an acknowledgement that they have received training and understood the policy, and make sure the acknowledgements are retained on the employees' files;*
> 4. *Remind the employees about the policy at reasonable intervals;*
> 5. *Advise employees that compliance with the policy may be monitored, and ensure that compliance is monitored;*
> 6. *Enforce the policy, and enforce it evenly."*

There is of course a lot more detail lying under this.[7] For example, there is no quick cookie-cutter approach. Each organisation needs to look to what it is seeking to achieve, its own risk issues, considerations relevant to employee needs, etc.

In our experience, it's not only the policy that is frequently deficient, even in large organisations. Often, even more importantly, its implementation (that is, getting it sufficiently notified over time to employees) is botched. The company in the Employment Court case is by no means unique in insufficiently notifying its policies. In fact in many ways it had much better processes than other organisations, large and small.

As so often with these things, the devil can be in the detail. A couple of examples illustrate this. These policies often use "*pornography*" as a benchmark, sometimes referring back to the relevant legislation. However, this will often be a much higher standard than what would otherwise be regarded as appropriate. Other language and examples need to be used.

Here's another example. As was the situation in the Employment Court case, an employee will often be allowed to use his or her computer for personal use for an undefined reasonable period. But what is reasonable to one person is unreasonable to another. The

[4] *IRD v. Buchanan* 22 December 2005, CA 2/05 at para 38.

[5] At para 142.

[6] *Pornography: A growth industry* in the New Zealand Law Society Employment Law Conference Papers, October 2006, page 148.

[7] Much is in the Peter Chemis paper and other articles in the NZLS conference papers.

employer in that case had its own ideas about the number of hours that constitutes reasonable use. However, it did not communicate that to the employees. That created a further problem for the employer, said the Judge, particularly when something as serious as dismissal was at stake.

How far can employers intrude into an employee's privacy?

Organisations have a lot at stake, and plenty of reasons why they should intrude heavily into what would otherwise be an employee's personal territory when they are at work.

Take security. The Privacy Act itself is a good starting point to illustrate why organisations can often be intrusive. The fifth information privacy principle (IPP5) requires organisations to take relatively strong measures (depending on the circumstances) to protect information held on behalf of third parties. General law (such as the law as to confidential information and trade secrets) has comparable obligations.

This is one reason why the countervailing privacy interest (that of the employee) in the IPPs can and often should be overridden (or applied in a way that meets the IPP5).

The Privacy Act permits this, for it allows the principles that protect privacy to be overridden if the employee so authorises.[8] That is subject to the privacy principle that information can only be collected if it is necessary.[9]

There are a bunch of other reasons why organisations will want, for example, the ability to read anything, including personal material, on the organisation's electronic systems (including mobiles and so on). Legal risks include:

- protection of the organisation's confidential information and trade secrets; (IP is an increasingly important asset on many organisations' balance sheets);
- minimising the risk of the employer being attacked in relation to sexual harassment of one employee by another;
- minimising copyright, porn, and defamation risk etc. Organisations can be liable even if they only provided the platform for the breach. For more detail see our article *On-line Porn and Other Workplace Vices*[10].

Then there is the all important reputational risk (trying to keep off the front page of the Herald on Sunday for example).

There is ample reason why an organisation would want to be intrusive, where necessary, into the employee's activities at work.

Currently it seems unlikely that employment law will stop this, where the employer can show that the intrusion on the employee's privacy is justified (which will often be the case as most organisations have issues in varying degrees, as noted above).

As so many employees have home computers and internet access these days, this is less of a privacy problem than it used to be: many (or all) personal activities can take place at home. The employee usually has choices.

Thus, for example, it would be increasingly appropriate to stop the use of Hotmail accounts and the like in an office environment (Hotmail-type accounts are a common but difficult-to-trace way for employees to take an organisation's valuable IP for example).

Most organisations will continue to permit some personal use of the internet and computer systems despite the risk.

At present, it does not look like there are any other strong legal impediments to relatively stringent controls so long as they meet the Privacy Act necessity test in IPP1[11].

[8] There will be issues sometimes whether there is genuine authorisation given (for example, in all the circumstances whether the employee really did authorise or was faced with no practical choice). Also "small print" authorisation may not be adequate. Additionally there are issues around transitioning existing staff to new policies where this is not specifically provided for appropriately in the employment contract. So, setting up the employment contract optimally in the first place is best.

[9] IPP1. "Necessary" has been given a broad interpretation by the Privacy Commissioner.

[10] http://www.wigleylaw.com/Articles/ArticleArchive/on-line-porn-and-other-workplace-vices/ . There are several other articles on our website that deal with similar issues.

[11] For example if the New Zealand Bill of Rights Act applies, a decision confirms that an employee is able to consent to waiver of rights under the Act (*Christchurch International Airport v. Christchurch City Council* [1997] 1 NZLR 573).

Obviously, there is a risk for organisations where, having got the employee's authorisation to heavy intrusion, the organisation overreaches. Judgment calls are needed to balance the various factors, not least being an environment in which employees feel they are valued and trusted.

Critically, the employee's authorisation should be clear and well informed if there are to be intrusions.

Conclusion

That takes us back to the need to have great wording and to ensure employee buy-in. Organisations can generally make judgment calls as to the degree to which they have internet and email policies that intrude into employees' privacy. Ideally this should be firmly justified.

Organisations will obviously consider the extent to which policies should be employee-friendly and permit personal use. We all want to work in an environment where we are valued and trusted.

It's a good idea to articulate the reasons for the approach in the policy (in the policy itself and in training materials). That is especially so where there are concerns that are particular to the organisation.

We particularly emphasise what we say below in italics. Each situation varies: what is acceptable in one place won't fly in another.

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.
