How to keep an eye on staff communication without being a Yahoo

Is keeping your eye on your staff's use of technology an invasion of their privacy or a legitimate way to monitor their productivity? Angus Macinnis from StevensVuaran Lawyers explains using a recent European example.

It's not often that the European Court of Human Rights (ECHR) gets a lot of coverage in the Australian media. However, the ECHR was front and centre after a decision rather luridly headlined (in the *Sydney Morning Herald* in January) as "Bosses can snoop on e-mails to girlfriend, European court finds."

The decision concerned a Romanian man who was dismissed from his job in August 2007 and was still litigating the dismissal up until the point when the ECHR handed down its judgment. (Eight-and-a-half years does sound like a very long period to be running a termination of employment claim, but perhaps there hasn't been much on television in Romania during that time).

The employee had been dismissed for using a Yahoo Messenger account (which was set up, at the employer's direction, to enable the employee to communicate with clients) to communicate with the employee's fiancée and brother. The employee had denied any personal use of Yahoo Messenger, but when the employer covertly accessed the account, the employee's denials turned out to be untrue.

Angus Macinnis
Senior lawyer,
StevensVuaran Lawyers

From an Australian perspective, that doesn't sound like much of a hanging offence. However, the employer had a policy in the following terms:

"It is strictly forbidden to disturb order and discipline within the company's premises and especially … to use computers, photocopiers, telephones, telex and fax machines for personal purposes."

(Don't you hate it when your co-workers are always tying up the telex machine with endless personal telexes?)

In addition, the employee probably didn't help his cause all that much by denying any personal use of Yahoo Messenger, and then, when confronted with a 45-page log of messages showing the extent of personal use, threatening his employer with criminal proceedings for interception of his correspondence.

The extent of the personal use was not set out in the judgment, although the ECHR did find that the messages demonstrated that the employee had been "blatantly wasting time" (as opposed to the surreptitious wasting of time more commonly encountered in Australia).

The employee challenged his dismissal in the Bucharest County Court, failed, appealed and failed again. Obviously deciding that his lack of success could be overcome by choosing a bigger opponent, the employee then sued Romania in the ECHR, alleging that the country had failed to safeguard his rights under Article 8 of the European Convention on Human Rights, which provides – subject to a number of exceptions – that "everyone has the right to respect for his private and family life, his home and his correspondence."

Image: Wavebreakmedia via iStock

A clear computer use policy can make staff and management avoid making yahoos of themselves.

In a decision which is rather more snooze-worthy than the lurid headlines would suggest, the ECHR analysed the use which the Romanian courts had made of the Yahoo Messenger evidence in the courts' determinations of whether the employee had engaged in a disciplinary breach.

The ECHR found that the approach taken by the Romanian courts had reasonably balanced the employee's right of privacy with the legitimate interest of the employer to ensure that the employee actually was (or in this case, was not) doing work.

So, what does this mean in Australia? Australian employees have no 'right of privacy' equivalent to Article 8 of the European Convention, although practitioners in New South Wales and the ACT must – and other Australian practitioners should – be familiar with the legislative requirements of the *Workplace Surveillance Act 2005* (NSW) and the *Workplace Privacy Act 2011* (ACT), respectively.

Australian courts have generally held that if the employer provides computers or networks, the employer is entitled to monitor what is done on the computer or network. The position becomes a bit more complex when an external communication platform is used, as was demonstrated by the famous case in which an employer failed to defend an unfair dismissal case using evidence harvested from his ex-wife's Facebook account without her knowledge.

To avoid your employees making yahoos of themselves, the starting point needs to be a computer use policy which clearly states that employees have no expectation of privacy when using the employer's computer system and which authorises the employer to monitor that use.

A clear policy will often prevent disputes arising, but if disputation can't be avoided, a clear policy will be the best tool to ensure that in an equivalent case, an Australian court should be able to take less than eight-and-a-half years to find that, as an employer, you are entitled to snoop the Messenger.

This article first appeared on HRM Online, www.hrmonline.com.au

About the Author

Angus Macinnis is a senior lawyer at boutique commercial law firm StevensVuaran Lawyers. He has provided employment and safety advice, training and dispute resolution assistance to employers across a range of industries for more than 15 years. Angus can be reached on angus@stevensvuaranlawyers.com