Computer Monitoring of Government Employees: Not An Invasion of Privacy

Marlia Saunders, Melanie Bartlett and Sophie Dawson consider a recent Federal Court decision which found that monitoring a Commonwealth employee's personal use of IT systems was not an invasion of privacy.

The Federal Court of Australia has confirmed in *Griffiths v Rose* [2011] FCA 30 (31 January 2011) that the monitoring by a government department of its employees' personal use of IT systems will not constitute an invasion of privacy so long as employees are informed that such scrutiny will occur.

Although the case preserves the rights of Commonwealth agencies to check their employees' emails and internet browsing habits, such employers should take care to ensure that their IT usage policies are broad enough to cover all types of personal information that they may collect in the course of undertaking such monitoring activities, in order to avoid a finding that they have collected information by unfair means in breach of s16 of the *Privacy Act 1988* (Cth) (***Privacy Act***).

Background facts

Mr Griffiths (the ***Applicant***), a senior public servant, was fired from a Commonwealth department after being found to have viewed a number of websites which contained pornographic images on his work laptop. He had viewed the websites at home using his own internet connection, then deleted the website entries from the browser's internet history.

The Applicant claimed he was not aware that the department used a software program which logged the occurrence of particular keywords on its IT systems, took snapshots of the desktop every 30 seconds and collected all emails, attachments, internet searches and instant messages performed or sent by a user. The information gathered was then retained on the department's server when the laptop was reconnected to the network, and the department would conduct regular audits of the information.

The department became aware of the Applicant's conduct during such an audit, and after conducting an internal investigation, found the Applicant had breached the department's IT policy, which prohibited employees from using departmental IT facilities to deliberately access or download pornography. In the course of the investigation, the department found that the Applicant was in breach of the 'Australian Public Service Code of Conduct' contained in the *Public Service Act 1999* (Cth) (***Code of Conduct***), which requires public servants to comply with any lawful and reasonable direction by an agency, to use Commonwealth resources in a proper manner and to uphold the values, integrity and good reputation of the Australian public service. The Applicant's employment was consequently terminated.

The Applicant's argument

The Applicant claimed that his privacy had been grossly invaded by the department using software to monitor his browsing habits during periods of personal use. The Applicant sought orders quashing the finding that he had breached the Code of Conduct and the decision that his employment be terminated. He also sought a declaration that the Commonwealth could no longer investigate his conduct insofar that it related to him accessing lawful pornography in private and outside working hours.

The Applicant argued that the direction in the department's IT policy not to view pornography was not lawful or reasonable because it invaded his privacy to the extent it permitted the department to monitor his personal usage of the laptop, and no legitimate interest of the department was protected as a result of such monitoring. In particular, he submitted that:

- the direction infringed Information Privacy Principle 1 (***IPP 1***) and was therefore contrary to s16 of the Privacy Act;
- even if the direction was lawful, it was not reasonable because it infringed common law and equitable rules relating to privacy, including Article 17 of the *International Covenant on Civil and Political Rights* (***Article 17***), which provides for a right not to be subjected to any 'arbitrary or unlawful' interference with privacy; and
- the direction was not reasonable in the ordinary sense.

the information obtained by the Commonwealth was for the lawful purpose of ensuring compliance with the Code of Conduct, and the means of collection could not be regarded as 'unfair' in circumstances where employees had been specifically warned by the department that their computer use is monitored for this purpose

The Commonwealth's argument

The Commonwealth argued that since it was the owner of the laptop, it had the right to regulate how it was used, and to insist that it not be used to look at pornography. In particular, the department had a legitimate interest in ensuring that its equipment was not used in connection with pornography so that it did not accidentally reappear or display in the workplace. Further, the Applicant had been clearly warned of the risks of viewing this type of material. It was submitted that, although the Applicant had rights of privacy, it did not follow that he had a right to use the laptop contrary to the express instructions not to view pornography.

The Decision

Breach of IPP 1

IPP 1 provides that the Commonwealth may only collect personal information which is necessary for a lawful purpose directly related to a function of the Commonwealth and that it must not be collected by unlawful or unfair means.

The Applicant argued that the direction in the department's IT policy not to look at pornography indirectly breached IPP 1 because

of the risk that the direction might be enforced in a way that interfered with an individual's privacy and thereby breach Article 17. The Applicant sought to rely on a finding by the United Nations Human Rights Committee in *Toonen v Australia* (CCPR/C/50/D/488/1992, UN Human Rights Committee (HCR), 4 April 1994), which held that Tasmanian laws banning homosexuality were unlawful since the only way to detect a breach of the laws would constitute an invasion of an individual's privacy.

Justice Perram rejected this argument, and found that the information obtained by the Commonwealth was for the lawful purpose *of ensuring compliance with the Code of Conduct*, and the means of collection could not be regarded as 'unfair' *in circumstances* where employees had been specifically warned *by the department* that their computer use is monitored for this purpose. The department's IT policy explicitly stated that the department may record all emails sent and received by staff and all URL logs, to make sure that employees were not using the department's systems for improper purposes, and the Applicant had signed a document recording that he understood the IT policy.

there may be circumstances where the collection of data by the software program may give rise to unfair collection of information in some circumstances

However, his Honour did note that there may be circumstances where the collection of data by the software program may give rise to unfair collection of information in some circumstances. For example, the department's policy did not warn employees that it may inadvertently collect personal banking information or credit card details during periods of personal use, even though the policy permitted limited personal use for these purposes.

Breach of privacy under common law, equity and Article 17

The Applicant argued that his general rights to privacy under common law and equity were infringed by the direction not to view pornography, insofar as it related to his use of the laptop at home while connected to his own internet service.

Justice Perram stated that, since it was the Commonwealth's laptop, the department was entitled to request that the Applicant not use it to view pornography and had explicitly warned him that his use of the laptop would be monitored with a view to detecting any prohibited use. Given these conclusions, his Honour found that this case did not provide an appropriate vehicle to look at how an equitable action to prevent misuse of confidential information (which has been recognised in a number of lower Courts in Australia) might extend to the personal affairs and private life of a plaintiff.

Justice Perram also rejected the Applicant's argument that the Commonwealth had breached Article 17, finding that there was nothing 'arbitrary or unlawful' about monitoring the Applicant's internet usage when he had been told that it would happen. His Honour distinguished Article 17 from the broader right of privacy contained in Article 8 of the *European Convention on Human Rights*. Even so, his Honour stated that there is authority that even Article 8 will not be infringed where an employee's use of a work phone is monitored, provided that the employee is expressly warned.

Whether the direction was generally unreasonable

Finally, as to whether the direction was reasonable in the ordinary sense, Justice Perram held that it was, reiterating the point that the Commonwealth had a right to stipulate how its own property is used and had a legitimate concern to avoid accidental viewing by others in the workplace.

Conclusion

This decision confirms that it is not a breach of the Privacy Act for a government agency to monitor its employees' use of work computer equipment where they have been warned that such monitoring may take place.

The current employee records exemption under the Privacy Act means that private sector organisations are not required to comply with the Privacy Act in respect of acts or practices directly related to the employment relationship with their employees and to employee records held by the organisations. However, the lessons from this case are also relevant to private sector employers, since any monitoring activities by employers might also access non-employment related information about their employees, in which case the Privacy Act could apply.

All employers should ensure that their IT policies adequately inform employees of the types of information that they may collect in the course of undertaking such monitoring activities, particularly where software systems may gratuitously capture unnecessary information. Employers should also ensure that any monitoring engaged in is reasonable in the circumstances, such as to ensure that prohibited practices are not being conducted by employees.

Marlia Saunders is a Senior Associate, Melanie Bartlett is a Paralegal and Sophie Dawson is a Partner at Blake Dawson.

Editors note

In related developments, significant privacy law reforms are currently working their way through the Australian Parliament. The Australian Law Reform Commission (***ALRC***), in Recommendation 40-1 of its report *For Your Information: Australian Privacy Law and Practice*, Report 108 (2008), recommended that the employee records exemption be removed.

If implemented this reform would mean that employers would be required to comply with the Privacy Act in relation to all personal information about their employees. This recommendation is to be considered by the Australian Government in the second stage of its two-stage response to the ALRC Report. Various other reforms are also proposed – see the website of the Office of the Australian Information Commissioner for more information: http://www.privacy.gov.au/law/reform.

The first stage of reforms will be debated after the Senate Finance and Public Administration Committee delivers its final report on its inquiry in the Exposure Drafts of Australian Privacy Amendment Legislation, due on 1 July 2011. It is expected that the reforms will be put in place in late 2012.