Can you read an employee's private email? Addressing the legal concerns

Svantesson, Dan Jerker B

Published in:
Internet Law Bulletin

Published: 01/01/2009

Document Version:
Publisher's PDF, also known as Version of record

Licence:
Other

Internet Law
Bulletin

Can you read an employee's private email? Addressing the legal concerns

Dan Svantesson *EDGE LEGAL*

This article focuses on privacy in the e-workplace, with particular emphasis on regulating the surveillance of employee use of electronic resources such as email and the internet.[1]

The employee's right of privacy is often overlooked. The employer may unknowingly violate the employees' right of privacy and thereby run the risk of acting in breach of Australian law. This article will assist legal practitioners by:

- outlining relevant legislation;
- highlighting particular legal issues that must be considered; and
- describing some steps that employers can take to address the legal concerns.

Instances and types of privacy breaches in the workplace will vary depending on the nature of the industry, the type of services that the employee provides and the employers' access to personal information about the employee. Some common workplace privacy breaches relate to:

- performance monitoring;
- telephone monitoring;
- geographical monitoring (for example, by use of a GPS device);
- email and internet monitoring;
- drug testing; and
- genetic testing.

Despite being a serious issue, workplace privacy has gained surprisingly limited attention. Textbooks on employment law often limit themselves to noting, for example, that "at common law, there is no authority according an employee a right of privacy in relation to activities or conduct at the workplace",[2] followed by a brief and superficial discussion of the relevant statutes.

Right of privacy

Privacy is a fundamental human right, recognised in several international instruments, such as the International Covenant on Civil and Political Rights. The starting point of any discussion of employee privacy must be the realisation that employees do not totally abandon this human right when entering the workplace. In other words, employers must respect their employees' right of privacy.

Relevant legislation

Employers have to abide by a patchwork of privacy-related legislation, and the applicable law depends on which state or territory the employer is based in. Some of the key pieces of legislation an employer must consider are:

- Privacy Act 1988 (Cth);
- Workplace Surveillance Act 2005 (NSW);
- Surveillance Devices (Workplace Privacy) Act 2006 (Vic); and
- Surveillance Devices Act 1998 (WA).

The article "Employee privacy — the forgotten issue" by Patrick Fair and Ryan Grant (2007) 10(4&5) *IPLB* discusses the relevant state workplace surveillance Acts in some detail, so I will focus here on Federal legislation.[3]

Workplace privacy under the Privacy Act 1988 (Cth)

Being a federal Act, the Privacy Act 1988 (Cth) is applicable Australia-wide. It outlines 10 National Privacy Principles (NPPs) regulating matters such as:

- the collection of personal information;
- the use and disclosure of personal information;
- data quality and security;
- openness, access and correction;
- identifiers and anonymity; and
- trans-border data flow.

It also has special rules regulating so-called sensitive information.[4]

Importantly, the Privacy Act contains several exemptions, one of which is an exemption for employee records.[5] However, this exemption only applies to an act done or practice engaged in by an employer if the act or practice is directly related to:

(a) a current or former employment relationship between the employer and the individual; or

(b) an employee record that relates to the individual and that is held by the employer.

Consequently, information about prospective employees is not exempt.

Further, the term "employee records" is given a rather limited interpretation, and is stated to mean a record of personal information relating to the employment of the employee. The Privacy Act lists a range of examples of what it considers to fall within this definition, including personal information relating to:

- the engagement, training, disciplining or resignation of the employee;
- the termination of the employment of the employee;
- the terms and conditions of employment of the employee;
- the employee's personal and emergency contact details;
- the employee's performance or conduct;
- the employee's hours of employment;
- the employee's salary or wages;
- the employee's membership of a professional or trade association;
- the employee's trade union membership;
- the employee's recreation, long service, sick, personal, maternity, paternity or other leave; and
- the employee's taxation, banking or superannuation affairs.[6]

Taking account of the nature of these examples, and the wording "personal information *relating to the employment* of the employee" [emphasis added], it seems clear that information such as the content of an employees' private emails and the details of what websites an employee has visited do not fall within the exemption for employee records, and that the Privacy Act consequently applies to such information. Indeed, as the content of the private emails and the details of the websites an employee has visited may amount to sensitive information, the stricter rules of NPP 10 may apply to how an employer deals with such information.

What can employers do?

There are several steps employers can take. Perhaps most importantly, they should frequently assess and reassess how they collect, use and disclose personal information.

Employers should ensure that the information they collect about their employees contains a minimum of personal information and that the collection of sensitive personal information is avoided wherever possible. On a practical level, this means that the employers need to consider whether data can be collected, what needs to be collected on a routine basis, and whether less wide—ranging data would be sufficient for satisfying, for example, the need for security and work efficiency.

Finally, employers should have clear privacy policies[7] informing their employees about matters such as:

- the circumstances under which personal information is collected;
- how such information is used;
- who within the organisation has access to that information;
- how long such information will be kept;
- the extent to which such information is disclosed;
- the circumstances under which such information is disclosed; and
- the employees' right to access to and correction of such information.

While, as mentioned above, little attention has been given to workplace privacy, one useful source for further guidance is the *Guidelines on Workplace E-mail, Web Browsing and Privacy* issued by the Office of the Federal Privacy Commissioner in March 2000.[8] The guidelines are now somewhat dated, but remain valuable. Further, while the guidelines were issued for the public sector, the Office of the Federal Privacy Commissioner has made it clear that the guidelines can be adopted by private sector organisations as best practice.[9]

The point of departure for the guidelines is the observation that "most staff do not expect to completely sacrifice their privacy while at work."[10] However, the guidelines also make clear that "as the organisation has responsibility for its computer systems and networks, it has the right to make directions as to its use."[11] Further, the guidelines highlight that it is crucial for an organisation to develop clear policies on the use of email and other internet activities at work. Indeed, the guidelines suggest that if staff are not "made aware of the logging of their network activities, then this [the collection of personal information] could be considered to be unfair"[12] and thereby violate the Privacy Act.

Six principles of internet use policy

One of the most important features of the guidelines is that it outlines six principles to be followed in developing or improving policies relating to staff internet use. They are as follows.

1. The policy should be communicated to staff and management should ensure that it is known and understood. Ideally the policy should be linked to from a screen that the user sees when they log on to the network.
2. The policy should be explicit as to the activities that are permitted and forbidden.
3. The policy should clearly set out what information is logged and who in the organisation has rights to access the logs and content of staff email and web browsing activity.
4. The policy should refer to the organisation's computer security policy. Improper use of email may pose a threat to system security, the privacy of staff and others and the legal liability of the organisation.
5. The policy should outline, in plain English, how the organisation intends to monitor or audit staff compliance with its rules relating to acceptable use of email and web browsing.
6. The policy should be regularly reviewed in order to keep up with the fast pace of development of the internet and information technology. The policy should be reissued whenever significant change is made. This would help to reinforce the message to staff.[13]

Importantly, the guidelines suggest that the relevant policies ought to be developed in consultation with staff as such an approach "is likely to result in a policy that staff understand and accept."[14]

Finally, it is relevant that the guidelines conclude by noting that:

> While it is acknowledged that access to staff e-mails and browsing logs by system administrators may be required in certain circumstances, it is unlikely that pervasive, systematic and ongoing surveillance of staff e-mails and logs should be necessary.
>
> Organisations are encouraged to foster an environment where staff are assured that the privacy of their communications will be respected as long as they abide by the organisation's stated policy.
>
> Balancing the legitimate interests of organisations and staff may be difficult and this balance may vary in different organisations. Policy or practice which leads staff to believe that their privacy in the workplace is not respected may be regarded as intrusive and oppressive and have a negative impact on morale and productivity.[15]

Conclusion

In 2004, the Office of the Federal Privacy Commissioner noted that "privacy issues in the workplace have to be faced, and employers need solid policy and procedures to guide them."[16] Unfortunately now, five years later, employers still lack clear and solid policy and procedures to guide them.

An organisation that is found to have breached privacy laws may find itself in a position where it not only has to pay the aggrieved party a significant amount of damages, but also suffers irreparable harm due to negative publicity and the public's loss of confidence in its ability to properly deal with and maintain their personal and private information.

Prudent business practice suggests that organisations should undergo regular privacy audits in order to ensure compliance with the applicable privacy laws.

Dr Dan Svantesson,
Consultant, Edge Legal.
Dr Dan Svantesson is Associate Professor, Faculty of Law, Bond University. This article is written as consultant for Edge Legal and the views expressed are the author's alone.

Footnotes

1. The July/August 2007 issue of the *Internet Law Bulletin* contained an informative article: Fair P and Grant R "Employee privacy — the forgotten issue" (2007) 10 (4&5) *IPLB* pp 52–4. In writing this, I have tried to avoid unnecessary overlap with that article.
2. C Sappideen et al, *Macken's Law of Employment*, 6th ed, Lawbook Co, Pyrmont, 2008, p 19.
3. Above.
4. NPP 10.
5. Privacy Act 1988 (Cth) s 7B(3).
6. Above s 6.
7. Electronic Frontiers Australia has issued a Model Acceptable Use Policy for Employee Use of the Internet that provides useful guidance: see www.efa.org.au/Publish/aup.html.
8. Office of the Federal Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (30/3/2000) at www.privacy.gov.au/materials/types/guidelines/view/6056.
9. Office of the Federal Privacy Commissioner, *Submission: Employee Records Privacy Review* (May 2004) at www.privacy.gov.au/materials/types/download/8663/6507, at 6.
10. Above n 8.
11. Above.
12. Above.
13. Above.
14. Above.
15. Above
16. Above n 9 at 11.