



Internet Monitoring and Workplace Privacy in Australia

This document outlines legislation that regulates Internet and network monitoring in Australia. Organizations that are using or intending to implement a form of electronic monitoring can use this document as a starting point to determine their legal rights and responsibilities.

This document is intended as a guide only - it aims to introduce the reader to issues which may be relevant to their organization, and to point out sources from which more detailed information may be obtained. It is **NOT** a substitute for professional legal advice.



WebSpy and Privacy

WebSpy products are used by organizations around the world to monitor the usage of shared electronic resources by their members. This monitoring enables organizations to verify that the resources they provide are being used for the purposes for which they are intended. For any organization currently employing or intending to employ a form of electronic monitoring, it is useful to be aware of current privacy legislation and the effect that it may have upon your monitoring practices.



Current Privacy Legislation in Australia

The *Privacy Act 1988* is the main body of legislation covering issues of privacy in Australia. This act historically only concerned information collected by the public sector and came about due to significant advances in electronic communication as well as a marked increase in information storage.

It was felt that this legislation did not adequately ensure individuals' privacy in the private sector. The *Privacy Amendment Act (Private Sector) Act 2000* (the Amendment Act) was formulated to resolve this issue. This act was passed by the Australian Federal Parliament in December 2000, and it became effective on 21st December 2001.

With these amendments, The Privacy Act 1988 now enforces the ten National Privacy Principles, which specify the way private sector organizations should collect, use, keep secure and disclose personal information.

The Ten National Privacy Principles

The National Privacy Principles (NPPs) were drafted in a technologically neutral manner to widen their applicability and prevent the legislation from rapidly dating, ensuring its use in future years.

The NPPs reflect ideas that have been developed internationally, in particular, the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).

The ten NPPs are as follows:

- 1 **NPP1** deals with the manner and purpose of collection of personal information. Essentially, the collection of data should be necessary, lawful and fair.
- 2 **NPP2** deals with the use and disclosure of personal information. Collected data should not be used for any purpose other than the primary purpose for which the data is collected.
- 3 **NPP3** deals with the accuracy and quality of collected data. Organizations must ensure that any data collected is accurate, complete and up-to-date.

- 4 **NPP4** deals with the security of collected data. Organizations must ensure that necessary steps are taken to avoid misuse, loss, unauthorized access, modification or disclosure of any collected data. Organizations must also ensure that information that is no longer needed is destroyed,
- 5 **NPP5** deals with openness within the organization. Organizations should maintain a well-communicated privacy policy, and inform members of the information that is likely to be recorded about them.
- 6 **NPP6** deals with access and correction. Members should be able to access personal information recorded about them, and have the opportunity to correct the information if it is inaccurate.
- 7 **NPP7** deals with identifiers. An organization is not permitted to adopt a government identity number (such as a Medicare number) as if it were its own identity number. Organizations cannot use Commonwealth government assigned identifiers in a way that is inconsistent with the purpose for which they are originally issued
- 8 **NPP8** deals with anonymity. Individuals must have the option of not identifying themselves when conducting transactions with an organization, whenever it is lawful and practicable.
- 9 **NPP9** deals with transborder data flows. Essentially, Principle 9 prevents organizations from disclosing personal information to an entity in a foreign country that does not enforce comparable privacy principles.
- 10 **NPP10** deals with the collection of sensitive information. Generally, consent is required from members when sensitive personal information about them is collected. However, there are some exceptions to this requirement such as where individuals are legally incapable of providing consent, and in life and health emergencies.

The Information Privacy Principles

The Privacy Act 1988 also includes Information Privacy Principles that apply only to Commonwealth and ACT Government agencies. These organizations need to be aware of these principles, especially if they are using, or are considering using a network and Internet monitoring system.

The areas covered by each principle are listed below.

- **Principle 1** Manner and purpose of collection of personal information
- **Principle 2** Solicitation of personal information from individual concerned
- **Principle 3** Solicitation of personal information generally
- **Principle 4** Storage and security of personal information
- **Principle 5** Information relating to records kept by record-keeper
- **Principle 6** Access to records containing personal information
- **Principle 7** Alteration of records containing personal information
- **Principle 8** Record-keeper to check accuracy etc. of personal information before use
- **Principle 9** Personal information to be used only for relevant purposes
- **Principle 10** Limits on use of personal information
- **Principle 11** Limits on disclosure of personal information

For more information regarding these principles, please refer to the Privacy Act 1988 available on the OFPC website (see resources).



Is Your Organization Affected?

The Amendment Act is aimed primarily, although not exclusively, at information collection by larger private sector organizations.

The National Privacy Principles do **NOT** apply to the following types of organizations:

- Most small business with a turnover of AU\$3million or less
- Registered political parties
- Commonwealth government agencies
- State or Territory authorities

The Amendment Act applies to business with an annual turnover of less than AU\$3million if:

- It is related to another business (for example a holding company or a subsidiary) that has an annual turnover of more than \$3 million
- It provides a health service and holds health records
- It discloses personal information for a benefit service or advantage
- It provides someone else with a benefit, service or advantage to collect personal information
- It is a contracted service provider for a Commonwealth contract



Implications for Monitoring

Monitoring products such as those offered by WebSpy Ltd. can be used by organizations as long as they obey the National Privacy Principles specified in the Privacy Act 1988.

It is possible for organizations to work with the Federal Privacy Commissioner to develop their own privacy code. This privacy code may then be adhered to in place of the National Privacy Principles. Organizations without their own privacy code are bound by the Privacy Act 1988 and must comply with the National Privacy Principles.

Essentially, organizations need to reasonably justify the collection of personal information about their members or clients. If these details are to be retained, the organization is also required to make all reasonable efforts to keep this information accurate, updated and complete.

WebSpy Ltd. recommends that organizations develop comprehensive Privacy and Acceptable Internet and Email Usage policies, and communicate these policies to their members. This policy should at least state the methods and purpose of any monitoring taking place.

The development of a privacy policy will assist the organizations compliance with National Privacy Principle 5 regarding openness. A policy will also help the organization build a trustworthy image and maintain a productive environment.



Penalties for Breaching the Privacy Act

When the Privacy Commissioner finds that an organization has breached the Privacy Act 1988, action is usually taken to ensure the organization remedies the situation and complies with the act in the future.

This may include a written apology, retraining of staff, changing procedures, or amending or deleting personal information.

Monetary compensation is occasionally offered to compensate the individual for any loss or damage they may have suffered. Most of the relatively few compensation amounts to date have been around one thousand dollars.



Resources

The best source of information regarding issues of privacy in Australia is the **Office of the Federal Privacy Commissioner (OFPC)**. This office provides access to all relevant privacy legislation, and publishes a number of guides and information sheets to help organizations determine whether their activities are affected.

- OFPC main page
<http://www.privacy.gov.au/>

Legislation

- The Privacy Act 1988 and associated information can be downloaded from:
<http://www.privacy.gov.au/act/index.html#2.1.1>
- National Privacy Principles
<http://www.privacy.gov.au/publications/npps01.html>
- Information Privacy Principles
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.html

Other Related Legislation

- Telecommunications Act 1997
http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/index.html
- Australian Security Intelligence Organization Act 1979 (extracts)
http://bar.austlii.edu.au/au/legis/cth/consol_act/asioa1979479/s93a.html
- Freedom of Information Act 1982 (extracts)
http://bar.austlii.edu.au/au/legis/cth/consol_act/foia1982222/s4.html
- Archives Act 1983 (extracts)
http://bar.austlii.edu.au/au/legis/cth/consol_act/aa198398/s18.html
- Income Tax Assessment Act (extracts - tax file number provisions)
http://bar.austlii.edu.au/au/legis/cth/consol_act/itaa1936240/s202.html

Guidelines and Information

- Guidelines to the National Privacy Principles
http://www.privacy.gov.au/publications/nppgl_01.html
- Guidelines on Workplace E-mail, Web Browsing and Privacy (30/3/2000)
<http://www.privacy.gov.au/internet/email/index.html>
- Private Sector Guidelines- Business
<http://www.privacy.gov.au/business/index.html>
- Information on formulating a privacy code for your organization
http://www.privacy.gov.au/publications/is11_01.doc
- Privacy In Australia
<http://www.privacy.gov.au/publications/pia.html>

Related Organizations and Interest Groups

- Organisation for Economic Co-operation and Development
<http://www.oecd.org>
- Electronic Frontiers Australia
<http://www.efa.org.au/>
- Australasian Legal Information Institute
<http://www.austlii.edu.au>
- Privacy International
<http://www.privacyinternational.org>
- Privacy Organization
<http://www.privacyexchange.org>
- Privacy Foundation
<http://www.privacyfoundation.org>
- International Labour Organization
www.ilo.org
- Labour Start
<http://www.labourstart.org>
- Electronic Privacy Information Center
<http://www.epic.org>

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Other product and company names herein may be the trademarks of their respective owners.