

## PRIVACY AND THE PRIVATE SECTOR

---

### Introduction

In 2001, the *Privacy Act (Cth) 1988* (“the Act”) was amended. These amendments built on the existing privacy responsibilities for the public sector, extending the protection of personal information to the private sector. As a result, organisations are currently subject to minimum standards in relation to the collection, use, maintenance and disclosure of personal information. At the heart of the Act are ten National Privacy Principles (“NPPs”).

Essentially, the NPPs require every organisation caught under the Act to ensure that it:

- collects only personal information which is necessary for its legitimate functions and activities;
- takes reasonable steps to inform individuals from whom it is collecting personal information of the identity of the organisation, how to contact it, the purposes for which the information is collected and the organisations to whom this information is normally disclosed;
- wherever possible, only collects personal information from the individual and, where information is collected from someone else, takes reasonable steps to provide the information described in the above paragraph to the individual;
- only uses and discloses personal information for the primary purpose for which it was collected;
- does not transfer personal information overseas without taking steps to ensure that the recipient is bound by laws offering no less protection than the NPPs, or that it will deal with the information as if it were subject to the NPPs;
- protects and maintains the security and accuracy of personal information which is collected, and gives individuals the right to access and update personal information which is held about them; and
- develops policies regarding how personal information will be collected, used and managed within an organisation and makes these policies readily available to the public.

### Are you caught under the Act?

The private sector provisions apply to “organisations”, defined in the Privacy Act as “an individual, a body corporate, a partnership, any other unincorporated association or a trust”. This definition can include not for profit entities and co-operatives.

The Act, however, specifically exempts organisations with an annual turnover of \$3 million or less. These organisations are regarded as “small businesses”. Despite the general exemption, the Act applies to certain types of small businesses, for example where the small business:

- provides personal information in exchange for any benefit, service or advantage (for example, where a theatre company, whose turn-over is less than \$3 million, enters into a sponsorship deal with a company, and as part of that sponsorship deal the customer list of the theatre is passed on to the sponsor corporation, the theatre company may now be caught under the Act);

- is related to a business that has an annual turnover of greater than \$3 million;
- provides someone else with a benefit, service or advantage to collect personal information;
- provides health services and holds health information other than employee records; or
- is a contracted service provider for a Commonwealth contract.

Small businesses who aren't covered by the Act, but who wish to be treated as an organisation for the purposes of the Act can choose to "opt-in" to the private sector provisions. The Federal Privacy Commissioner will keep the names of these businesses in a publicly available register. If, at any time and for any reason, that small business decides to opt-out, all that is required is written notification to the Federal Privacy Commissioner.

Also exempt are:

- State and Territory authorities;
- political parties and acts of political representatives;
- acts or practices with respect to employee records where the act directly relates to a current or former employment relationship;
- acts or practices of media organisations in the practice of journalism; and
- Commonwealth government agencies which are already covered by the Act.

## What information is caught under the Act?

The *Privacy Act* specifically relates to the collection, handling and use of "personal information".

The Act defines "personal information" as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion". "Personal information" therefore includes any form of data that has the ability to identify an individual. For example, it would include information like a person's phone number, email address, postal address, income bracket, marital status, name of partner and name of any dependants or children, as long as such information can be linked to an identifiable individual.

The *Privacy Act* prevents the use of a tax file number as an identifier, and individuals have the right to withhold this information. Where a tax file number is provided, its use is usually limited to tax related, assistance agency and superannuation purposes. The *Privacy Act* also strictly governs the handling of credit reports and other credit worthiness information about individuals by credit reporting agencies and credit providers.

As mentioned above, the Act also protects all records if they are held by an organisation that is a health service provider, even if the organisation's annual turnover is less than the \$3 million threshold. Additionally, there is a general exemption for the handling of employee records that is directly related to a current or former employment relationship. Any health information in those employee records would be usually be covered by the exemption.

Please note that there are also obligations under the various State and Territory legislation. In Victoria, for example, the *Health Records Act 2001* imposes obligations on the collection and handling of health information, despite the fact that the organisation may be exempt from compliance with the *Privacy Act*.

## What are the obligations?

Once an organisation is caught under the private sector provisions, the Act requires that the organisation comply with the ten National Privacy Principles (NPPs). The NPPs are legally binding principles which set the basic standard for privacy protection and stipulate how organisations can collect, use and disclose personal information. Organisations that do not have their own privacy code (see below) must comply with the NPPs.

In essence, the NPPs require organisations to take reasonable steps to advise individuals that it is collecting personal information about them; the purpose for which it is collecting the information and who it might pass that information on to. The NPPs also impose restrictions on how personal information can be used and when it can be disclosed or transferred overseas. Generally, individuals will have the right to get access to their personal information held by an organisation and to have that information corrected.

If your organisation is caught by the Act, the “National Privacy Principles” and the “Guidelines to the National Privacy Principles”, available on the Privacy Commissioner’s website ([www.privacy.gov.au](http://www.privacy.gov.au)), are essential reading.

## Can you develop your own privacy code?

The Act allows organisations to develop their own privacy code which, when approved by the Federal Privacy Commissioner, replaces the obligations of the NPPs for that organisation. In order for the code to be approved, the Act requires that the Federal Privacy Commissioner be satisfied, amongst other things, that the obligations in the code are at least equivalent to the NPPs and that members of the public have been given adequate opportunity to comment on a draft of the code. It should be noted that the Federal Privacy Commissioner has the power to revoke the code at any time.

## What happens if an individual’s privacy is breached?

Where an organisation has implemented an approved privacy code, all complaints about the breach of an individual’s rights under the Act should follow the code’s complaints handling procedure. Where an organisation chooses not to develop its own code, or where that code does not have a complaints handling mechanism, the Office of the Federal Privacy Commissioner has the power to handle all privacy complaints.

With regards to an individual’s privacy, the Federal Privacy Commissioner has power to:

- investigate complaints made to the Office of the Federal Privacy Commissioner by an individual or a code adjudicator;
- investigate all complaints made about a Federal Government contractor;
- investigate, on the Federal Privacy Commissioner’s initiative, an act or practice that may be a breach of privacy, even if no complaint has been made;
- seek an injunction from the court to stop conduct that does or would breach the Act; and
- review the code adjudicator’s decision if an individual requests.

The Federal Privacy Commissioner does not have power to fine or jail people or organisations that are in breach of the Act. However, the law does allow the Federal Privacy Commissioner to make a determination for compensation through Federal and State Magistrates Courts in circumstances where a person is adversely affected by what has happened to them.

## Complying with the *Privacy Act*?

Once an organisation has established that the private sector provisions apply to it, it must consider what it needs to do to comply with these provisions. The following are some suggestions as to what an organisation should do to comply with the *Privacy Act* private sector provisions:

- **Appoint a privacy officer** to be responsible for developing and implementing privacy policies. The privacy officer should be the first point of contact in the organisation when a privacy issue arises and is responsible for ensuring the organisation's privacy policy and procedures are fully implemented.
- **Conduct a privacy audit** to determine what sort of personal information the organisation collects, holds and discloses. The audit should also reveal how the organisation protects the personal information it collects, and how it is updated.
- **Compare current practices with requirements in the Act** to determine what discrepancies, if any, exist.
- **Formulate a privacy policy for the organisation.** The privacy officer should be responsible for co-ordinating and implementing the privacy policy for the organisation. This policy needs to be made available to any member of the public who asks for it and must, of course, accurately reflect the practices of the organisation. At this stage, consideration should be given as to whether the organisation should develop its own privacy code. If so, the privacy officer should be responsible for getting a draft code approved in line with the requirements of the Act.
- **Train staff** on privacy procedures and the organisation's privacy policies.

## Developments: tort of invasion of privacy

Apart from the requirements contained in the *Privacy Act* there is no general right to privacy in Australia. However, recent developments overseas and in the Australian courts leave open the possibility of a future tort of invasion of privacy in Australia. A tort is a private, civil wrong or injury for which the court may provide a remedy for any damage caused.

Unlike the United States where there is an over-arching, all-embracing cause of action for invasion of privacy, the United Kingdom (UK) only has limited privacy protection. However, recent decisions, and the development of privacy law spurred by the enactment of the Human Rights Act 1988 (UK) have led to developments in the UK. For example, the House of Lords case in *Campbell v Mirror Group Newspapers (MGN)* considered the surreptitious photographs taken of model Naomi Campbell whilst she was leaving a narcotics anonymous meeting, which were then published in the Mirror newspaper. The House of Lords held that this was wrongful disclosure of private information as the details of Campbell's treatment were of a private nature and that this imposed a duty of confidence on MGN. This decision was also made with reference to Article 8 of the European Convention on Human Rights. At present Australia does not have Human Rights Bill and as this is a decision of a court in another country the case would only be persuasive in the Australian courts. Further, the case did not recognise a tort of invasion of privacy.

In a country closer to home, New Zealand, the case of *Hosking v Runting and others* concerned photographs taken of the twin children of a well-known New Zealand television presenter whilst his wife was shopping. The parents tried to stop the images from being published. Whilst the court recognised that there is a tort of invasion of privacy they held that in this situation the pictures were not offensive and there was no reasonable expectation of privacy as the mother of the twins was only out shopping. The court also stated that public figures should have a lower reasonable expectation of privacy due to the public nature of their lives.

In Australia there have been two decisions which have raised the possibility of a tort of privacy. First, the case of *ABC v Lenah Game Meats* (2001) involved the secret filming of possum slaughtering at a meat processing plant. The decision is significant as it recognised that according to contemporary standards, certain kinds of activities are meant to be unobserved and any disclosure or observation would be highly offensive to a reasonable person. This case left open the potential for the development of a tort of privacy in Australia.

Secondly, in the case of *Grosse v Purvis* (2003) monetary damages were awarded for a breach of privacy. This case involved extreme circumstances in which Grosse was stalked, spied on and threatened physically and verbally by Purvis over a period of more than six years. The court held that Purvis committed many breaches of Grosse's privacy. However, it is important to note that this case concerned long-term harassment of an offensive nature and the case was decided in a Queensland court, so whilst it may be persuasive in other states and territories it is not binding authority outside Queensland.

Consequently, whilst there are a number of developments in the area of privacy law and the tort of invasion of privacy overseas and in Australia, as yet there has been no introduction of a tort of invasion of privacy in Australia, which would directly affect the private sector beyond the obligations under the *Privacy Act*.

## Further Information

The purpose of this Information Sheet is to provide general information about privacy and the private sector. The issues surrounding the *Privacy Act* can be complex and require consideration on a case-by-case basis. If more information is required on how the law applies to a particular situation, please contact the Arts Law Centre of Australia or the Office of the Federal Privacy Commissioner ([www.privacy.gov.au](http://www.privacy.gov.au)).

---

© Arts Law Centre of Australia 2002, 2006

*You may photocopy this information sheet for a non-profit purpose, provided you copy all of it, and you do not alter it in any way. Check you have the most recent version by contacting us on (02) 9356 2566 or tollfree outside Sydney on 1800 221 457.*

---

*The Arts Law Centre of Australia has been assisted by the Commonwealth Government through the Australia Council, its arts funding and advisory body.*

