INFORMATION SHEET

Privacy and the private sector

Introduction

With effect from 12 March 2014, the *Privacy Act 1988* (Cth) (**Privacy Act**) includes a set of new privacy principles which consolidate the previous National Privacy Principles (NPPs) and Information Privacy Principles (IPPs) into 13 new Australian Privacy Principles (APPs) which regulate the collection, use, storage and disclosure of personal information by some businesses and government agencies. Amendments to the Privacy Act (implemented through the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)) also:

- introduce new penalties for serious or repeated breaches of the Act of up to $1.7 million for companies and $340,000 for an individual; and
- grant increased powers to the Office of the Australian Information Commissioner; and
- introduce a new and more comprehensive credit reporting regime for regulating the management of certain kinds of personal information concerning consumer credit.

These changes to the Privacy Act affect the way that businesses handle and process personal information, use personal information for direct marketing and disclose personal information to people overseas.

The amendments DO NOT introduce a general right of privacy, thus, generally, a person's consent is not required for their photo to be taken or their image to be recorded. For further information see the Arts Law *Unauthorised use of your image* information sheet.

Are you caught under the Act?

The Privacy Act 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 Privacy 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 Privacy 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 Privacy 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 Australian Information Commissioner (which took over the role of the Federal Privacy Commissioner in November 2010) 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 Australian Information Commissioner.

The exemptions under the Privacy Act include:

- any act done, or practice engaged in, with respect to employee records where the act directly relates to a current or former employment relationship (the employment records exemption);[1] any act done, or practice engaged in, by a media organization in the course of journalism (provided the media organization commits to observing privacy standards);[2] and
- political parties registered under Part XI of the Commonwealth Electoral Act 1918, members of parliament, local government councillors, contractors, subcontractors and volunteers for registered political parties.[3]

The employment records exemption only applied to such records held by a private sector employer – the exemption does not cover employment records held by government departments and agencies. It may be possible to access employment records under workplace laws.[4] The employment records exemption is limited in scope and does not apply to: information outside the scope of the employment relationship; personal information about unsuccessful job applicants; and any employee records of contractors and subcontractors that are held by an employer,[5]

The privacy regime that applies to state and territory government departments and agencies is established by the relevant privacy legislation of each state and territory, although there are some jurisdictions that have not enacted information privacy legislation.[6] For example: the Australian Capital

[1] s 7B(3) Privacy Act 1988 (Cth).

[2] s 7B(4) Privacy Act 1988 (Cth).

[3] s 7C Privacy Act 1988 (Cth).

[4] See the website of the Fair Work Ombudsman.

[5] Australian Privacy Law and Practice Report 2008 (ALRC Report 108) [40.6].

[6] Privacy and Personal Information and Protection Act 1998 (NSW) & Health Records Information Privacy Act 2002 (NSW); *Information Privacy Act 2014* (ACT) & Health Records (Privacy and Access) Act 1997 (ACT); Information

Territory information privacy legislation is the *Information Privacy Act 2014* (ACT) that sets out Territory Privacy Principles (TPPs), which apply to the ACT public sector agencies and to contracted service providers (including subcontractors), when they perform obligations under a government contract. The TPPs are similar to Privacy Act APPs but do not include provisions equivalent to the APPs relating to certain private sector and other entities. The privacy regime for health records held by ACT Government agencies (including public hospitals) is established by the Health Records (Privacy and Access) Act 1997 (ACT). Where a state or territory has enacted information privacy legislation there is an office of the privacy commissioner or privacy commission that is responsible for overseeing compliance with the legislation and managing privacy complaints.[7]

What information is caught under the Act?

The Privacy Act specifically relates to the collection, handling and use of "personal information" of individuals. The Privacy Act defines 'personal information' as "information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not; and

b) whether the information or opinion is recorded in material form or not.

'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 Privacy 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 usually be covered by the exemption.

It is clear that in some circumstances a person's image could be regarded as 'personal information' and its publication by an entity subject to the Privacy Act would breach that Act. The website of the Office of the Australian Information Commissioner discusses this issue in more detail.

Privacy Act 2009 (Qld); Information Act (NT); Privacy and Data Protection Act 2014 (Vic); Personal Information and Protection Act 2004 (Tas).

[7] Office of the Australian Information Commissioner (OAIC): State and territory privacy law.

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 falls within the definition of an APP entity, the Privacy Act requires that the organisation comply with the 13 APPs. The APPs are legally binding principles which set the basic standard for privacy protection and stipulate how organisations can collect, use and disclose personal information.

In essence, the APPs require an organisation 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 APPs 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.

The APPs include:

- **APP 1 - Open and Transparent management of personal information** which sets out the requirements for a privacy policy and requires entities to take reasonable steps to make their policies freely available. APP 1 also establishes a new compliance framework requiring entities to take reasonable steps to implement practices, procedures and systems relating to the entities activities that will ensure compliance with the APPs.
- **APP 2 - Anonymity and pseudonymity** requires entities to provide individuals with the option of dealing with an APP entity anonymously or through the use of a pseudonym unless it is impracticable for the entity or the entity is required to do so under Australian law or a court/tribunal order.
- **APP 3 - Collection of solicited personal information** applies to any personal information solicited by the entity and provides that personal information should only be collected if reasonably necessary, by lawful and fair means and from the individual themselves if reasonable and practicable. An APP entity must not collect sensitive information unless consent has been obtained from the individual.
- **APP 4 - Dealing with unsolicited personal information** sets out requirements for situations where the entity did not solicit the information. Within a reasonable period of time, the entity must determine whether that information could have been collected under APP 3. If APP 3 does not apply, the entity must as soon as practicable, but only if it is lawful and reasonable to do so, destroy or deidentify the information.
- **APP 5 - Notification of the collection of personal information** provides that an entity must take reasonable steps to notify an individual at the time of, before or as soon as practicable after the collection.

- **APP 6 - Use or disclosure of personal information** stipulates that an entity must not use or disclose personal information about an individual unless the individual has consented or the use of the information falls within another exception.
- **APP 7 - Direct Marketing** specifies that an entity may only use an individual's personal information for direct marketing purposes where it meets certain specific requirements.
- **APP 8 - Cross-border disclosure of personal information** sets out that entities must take reasonable steps to ensure overseas recipients do not breach the APPs in relation to that information, unless an exception applies.
- **APP 9 - Adoption, use of disclosure of government related identifiers** restricts the use of government related identifiers by the private sector.
- **APP 10 – Quality of personal information** requires entities to take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete.
- **APP 11 – Security of persona information** provides that an entity must take reasonable steps to protect the personal information they possess from misuse, interference, loss, unauthorised access, modification or disclosure.
- **APP 12 – Access to personal information** requires entities to provide an individual with access to the information at their request.
- **APP 13 – Correction of personal information** states that where an individual can establish that the personal information is not accurate, complete or up-to-date; the entity must take reasonable steps to correct the information.

If your organisation is caught by the Privacy Act, the *'Australian Privacy Principles Fact Sheet'* and the *'Australian Privacy Principles Guidelines'*, available on the Australian Information Commissioner's website are essential reading.

Can you develop your own privacy code?

The Privacy Act allows organisations to develop their own privacy code which, when approved by the Australian Information Commissioner, replaces the obligations of the APPs for that organisation. In order for the code to be approved, the Act requires that the Australian Information Commissioner be satisfied, amongst other things, that the obligations in the code are at least equivalent to the APPs 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 Australian Information 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 Privacy Act should follow the code's complaints handling procedure.

In relation to an individual's privacy, the Australian Information Commissioner has power to:

- investigate complaints made to the Office of the Australian Information Commissioner by an individual or a code adjudicator;
- investigate all complaints made about a Federal Government contractor;
- investigate, on the Australian Information 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 Privacy Act; and
- review the code adjudicator's decision if an individual requests.

Under the new amendments, the Australian Information Commissioner has enhanced powers to investigate an interference with an individual's privacy and can:

- seek civil penalties in the case of serious or repeated breaches of an individual's privacy;
- accept enforceable undertakings; and
- conduct an audit of the performance for both agencies and businesses.

A serious or repeated breach of the Privacy Act will allow the Commissioner to make a determination and apply to the Federal Court to enforce the determination. Civil penalties of up to $1.7 million for a corporation and $340,000 for an individual may be sought.

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 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.
- **Check procedures for collecting personal information** and ensure that these procedures include the new notification requirements and provide a process for handling unsolicited information.
- **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 Privacy Act** to determine what discrepancies, if any, exist.
- **Formulate a privacy policy for the organisation that complies with the APPs.** The privacy officer should be responsible for co-ordinating and implementing the privacy policy for the organisation. This policy needs to comply with the new minimum requirements and be made freely available to individuals, such as on your website.

- **Review third party contracts with subcontractors and service providers** especially where they involve the disclosure of any personal information to offshore providers.
- **Review your complaints policy and processes** to ensure that it enables you to deal with complaints and inquiries about your compliance with the APPs.
- **Review your marketing consents and opt out statements** to ensure they comply with the requirements of the new direct marketing privacy principle.
- **Train staff** on privacy procedures and the organisation's privacy policies.

Your actual practice in dealing with personal information must be consistent with your published privacy policy. Promising something in a privacy policy and then failing to deliver may be misleading or deceptive conduct and breach section 18 of the Australian Consumer Law (ACL).

The Office of the Australian Information Commissioner (OAIC) publishes privacy guides on the application of the Privacy Act for individuals, businesses and government agencies.

Further information on the compliance with the Privacy Act by digital developers and mobile app developers is provided in the Arts Law information sheet New Media - Issues for creators working with and across multiple platforms.

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.

In the United Kingdom, the House of Lords case in *Campbell v Mirror Group Newspapers (MGN)* (2004) 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. In 2015 the Court of Appeal confirmed that under UK law the misuse of private information is a tort.

In New Zealand, the case of *Hosking v Runting* (2003) 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 in a public place. The court also stated that public figures should have a lower reasonable expectation of privacy due to the public nature of their lives. *C v Holland* (2012) considered the surreptitious installation of a video camera above a shower in shared accommodation. The issue was whether the invasion of privacy of this type, without the public dissemination of the video, was an actionable tort in New Zealand. The judge held that a tort of intrusion upon seclusion was part of New Zealand law, which involved: an intentional and unauthorised intrusion into intimate personal activity, space or affairs; that involved the infringement of a reasonable expectation of privacy, which is highly offensive to a reasonable person.

The High Court of Australia in *ABC v Lenah Game Meats* (2001) considered, but did not decide, whether there is a tort of invasion of privacy. This case 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.

ABC v Lenah has been considered in cases decided by state courts. Different conclusions have been reached. Some courts come to the conclusion that the law of Australia has not developed to the point of recognising an action for breach of privacy, while others have held that an invasion of privacy was an actionable wrong which gives rise to a right to recover damages according to the ordinary principles governing damages in tort. Other courts have looked to the UK development of a duty of confidence in relation to private information as the basis for legal remedies for an invasion of privacy.

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, however the High Court of Australian has not had an opportunity to confirm that there is a tort action for breach of privacy.

In a report tabled in August 2008, the Australian Law Reform Commission recommended the creation of a statutory right of action for an invasion of privacy. However this report has not resulted in the enactment of legislation that creates a statutory right of action to protect personal privacy. In June 2015, the NSW Legislative Council established an inquiry to consider remedies for the serious invasion of privacy in that State. The final report is due in March 2016.

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 Australian Information Commissioner 1 300 363 992 or enquiries@oaic.gov.au

Justice Connect, Not-for-profit Law has published the *Privacy Compliance Manual for use by Australian charities and not-for-profits*.

Need more help?

Contact Arts Law if you have questions about any of the topics discussed above . Telephone: (02) 9356 2566 or toll-free outside Sydney 1800 221 457. Also visit the Arts Law website (www.artslaw.com.au**)** for more articles and information sheets

Disclaimer

*The information in this information sheet is general. It does not constitute, and should be not relied on as, legal advice. The Arts Law Centre of Australia (**Arts Law**) recommends seeking advice from a qualified lawyer on the legal issues affecting you before acting on any legal matter.*

While Arts Law tries to ensure that the content of this information sheet is accurate, adequate or complete, it does not represent or warrant its accuracy, adequacy or completeness. Arts Law is not responsible for any loss suffered as a result of or in relation to the use of this information sheet. To the extent permitted by law, Arts Law excludes any liability, including any liability for negligence, for any loss, including indirect or consequential damages arising from or in relation to the use of this information sheet.

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