Communications Law BULLETIN

CAMLA

Communications & Media Law Association Incorporated

Print Post Approved PP: 100001546

# An Overview of Privacy Law in Australia: Part 1

**In the first of a two part special, Peter Leonard provides a thoughtful commentary on privacy reforms. In this Part 1 he provides a high level overview of the amendments to the Privacy Act 1988 and the new Australian Privacy Principles. In Part 2 to be published in the next edition he provides an in depth analysis of Australia's privacy regime; focusing on the APPs, the regulation of privacy beyond the Privacy Act, issues of extraterritoriality and emerging trends and issues.**

## A quick guide to the changes

The *Privacy Act 1988* (the ***Privacy Act*** or the ***Act***) was amended by the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*. The amendments took effect on 12 March 2014.

The amendments generally add provisions and corresponding compliance obligations.

Two Parts of the Privacy Act are completely replaced.

Part IIIA of the Privacy Act, dealing with credit reporting, is replaced in full by new credit information provisions. There are important changes to the current framework as to credit information policies, the collection and recording of credit related information, and disclosure of credit related information to overseas entities. Banks, retail businesses that issue credit cards, entities who carry on businesses which substantially involve the provision of credit, suppliers of goods and services on credit/payment terms, equipment lessors and hire purchase credit providers are 'credit providers' and must comply with the new framework. That framework is then expanded through a revised Credit Reporting Privacy Code prepared by the Australian Retail Credit Association and registered by the Australian Privacy Commissioner (***Commissioner***) in January 2014, following a lengthy consultation period. This Code also took effect on 12 March 2014.

The National Privacy Principles (***NPPs***) (for private entities, but subject to the small business exception) and Information Privacy Principles (***IPPs***) (for Federal government entities) are replaced with a single regime of privacy principles, the Australian Privacy Principles (***APPs***), which generally (but not universally) apply to Federal government agencies and private organisations alike.

Probably the key change is through APP 1 (privacy policy) and APP 5 (notification obligations), which place a higher onus on entities to institute practices, procedures and policies in relation to the protection of privacy. Many entities continue to focus upon policies and general disclosures and place insufficient emphasis upon the development of processes and procedures that ensure that the policies are in fact implemented and that implementation is effective, repeatable and reliable. Such entities will find the developing focus of the Privacy Commissioner upon whether an entity has taken all reasonable and practical steps to implement policies, rather than just write the policies, as a novel compliance challenge.

Among other implementation challenges, an entity must ensure that it can demonstrate that user consent had been obtained when consent is in issue and that the entity has in place effective procedures to deal with inquiries and complaints about an entity's compliance with the APPs and any applicable registered APP code of practice (when such codes are registered and apply to such organisations).

**Volume 33 Nº 1**
**March 2014**

## Inside This Issue:

# Contents



That is not to suggest that stated privacy policies and collection notices have become less important: to the contrary, the Act has become more prescriptive as to their form, substance, accessibility and intelligibility. A privacy policy must be 'transparent', accessible to the public and available free of charge. A privacy policy will need to include details as to:

## From March 2014, the Commissioner's investigative and enforcement powers are significantly enhanced

- specific kinds of personal information that the entity collects and holds and how it is collected and held;
- purposes (both primary and secondary) for which the entity collects, holds, uses and discloses personal information;
- how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
- how an individual may complain about a breach of the APPs or an applicable registered APP code; and
- how the entity will deal with a complaint (entities will also need to ensure that internal procedures are implemented consistently with this description, including by appropriate training of staff).

Other changes include:

- APP 2 (anonymity and pseudonyms), which provides that where practicable individuals must not be required to disclose their identity and may use a pseudonym. Previously there was only the requirement to provide an option of anonymity: the requirement to allow the use of pseudonyms (where practicable) is new;
- APP 4 (unsolicited personal information), which provides that where an entity receives unsolicited personal information that it could not have obtained through solicited means on reasonable terms, the entity must destroy the information;
- APP 5 (notification of collecting personal information), which is much more prescriptive than the former provision dealing with this subject matter, NPP 1. At or before the time information is collected, or if that is not practicable, as soon as practicable after information is collected, the collecting entity must ensure that it informs an affected individual of certain matters, including that the information has been collected; the purpose of collection; the consequences for the individual if the information is not collected; the procedure to complain about or amend information and any third parties that the information may be disclosed to; and
- APP 7 (direct marketing), which increases requirements for informed user consent in relation to direct marketing. Entities must have a simple means by which an individual can readily request not to receive direct marketing from the entity and ensure that personal information about the individual is not provided to third parties for the purpose of direct marketing.

Probably the most controversial and least understood change is new section 16C and APP 8 (disclosure to overseas entities).

APP 8 introduces a new 'accountability principle' to the effect that where an Australian entity intends to disclose (including disclosure through provision of electronic viewing access – a physical data transfer is not required) personal information to an overseas entity, the Australian entity must 'take such steps as are reasonable in the circumstances to ensure' that the overseas entity complies with the APPs in respect to the provided information. If the overseas entity does not comply with the APPs in respect to the provided information, then the Australian entity is 'accountable' and liable pursuant to section 16C as if it had not complied itself. This is the case regardless of whether the Australian entity had in fact taken reasonable steps to ensure that the overseas entity complied with the Privacy Act, or failed to take such steps. Accordingly, entities considering providing personal information to overseas entities will need to consider contractually binding such overseas entities to comply with the new privacy legislation and the Australian entity's privacy policy, including as to implementation of privacy safeguards, and the legal exposure of the Australian entity if the overseas entity fails to comply with that contract and implement and observe those safeguards. There are a number of important exceptions to this 'accountability' rule, which will be discussed in Part 2 of this paper.

From March 2014, the Commissioner's investigative and enforcement powers are significantly enhanced. Powers will include a right for the Commissioner to seek a Court injunction against a person engaging in conduct that may contravene the Privacy Act, to obtain enforceable undertakings by a person that has breached the Privacy

Act, and to seek the making by a Federal Court of civil penalty orders where there is either a serious or repeated interference with the privacy of an individual.

These and other changes taking effect from March 2014 or otherwise mooted are examined in more detail in later sections of this paper.

On 21 February 2014 the Commissioner released the Australian Privacy Principles Guidelines (the ***Guidelines***). These Guidelines are of significant interest as an expression of the Commissioner's interpretation of key provisions of the Privacy Act. The Guidelines are not given any express legislative status. However, the Guidelines may influence subsequent judicial interpretation of relevant provisions that are subject to guidance. It is interesting to note in this regard that in some cases the explanation of the intended operation of certain provisions of the amending Act that is given in the Explanatory Memorandum to the amending Act does not appear to conform to a plain reading of corresponding provisions of the amending Act. Issues of interpretation are therefore likely to arise.

## Australian privacy framework and coverage

The use of 'personal information' (sometimes referred to as ***personally identifying information*** or ***PI***) in Australia is primarily regulated by the Privacy Act. This is a federal Act administered by the Federal Attorney-General. The Privacy Commissioner is integrated within the Office of the Australian Information Commissioner (***OAIC***) (www.oaic.gov.au).

The amendments to the Privacy Act that commenced on 12 March 2014 substantially increase the level of federal privacy regulation and powers and sanctions of the federal enforcement agency. The following discussion focusses on the APPs as they will apply to private sector organisations: note that the rules applicable to government agencies differ in important matters of detail that are outside the scope of this review.

The Privacy Act is drafted in less prescriptive terms than European legislation. It does not use the European concepts of 'data owner', 'data controller' or 'data processor'. The Privacy Act does use other terms and concepts that are similarly used in other national privacy laws. However, the Privacy Act differs in varying respects to all other national privacy laws, including national laws in other APEC countries including Singapore, Malaysia and New Zealand. For this reason caution should be exercised when considering examples of regulatory action in other jurisdictions, even where the relevant terms used in the legislation appear to be similar. Also, privacy jurisprudence in other jurisdictions, particularly in the European Union, is often influenced by constitutional law or human rights principles that do not affect consideration of Australian privacy law. European privacy regulation also places significant reliance upon use of standardised contractual terms and rulings as to the adequacy of levels of protection of privacy under particular foreign jurisdictions for cross-border data transfers. These concepts are not generally used in Australian privacy law.

Further complexities arise through the longevity of Australian privacy law when measured in internet time. Although the amendments to the Privacy Act commencing on 12 March 2014 are significant, these amendments were developed from an Australian Law Reform Commission (***ALRC***) review into the Privacy Act that was completed in May 2008. That review predated important technological and business developments including availability of tablet and mobile apps, broad adoption of social networking services, extensive use of data hosting services, delivery of software applications as a service (often provided from overseas and sometimes transient and indeterminate locations), extensive use of geo-location services, online behavioural advertising and 'big data' based customer data analytics. Each of these developments challenge traditional privacy concepts of territorial based regulation and informed user consent based upon privacy statements and privacy notices. In September 2013 the Privacy Commissioner developed a guide for app developers to embed better privacy practices in their products and services and to help developers operate in the Australian market in accordance to Australian privacy law. However, mobile and tablet apps were not considered in the ALRC review. The international rollout of apps and delivery of app based services creates fundamental difficulties in application of national privacy regulation such as the Australian Act.

Compounding the problem, the Privacy Act has sketchy geographical and jurisdictional nexus provisions that are difficult to interpret and apply in relation to internet delivered services provided across national borders. Frequently, jurisdictional questions cannot be clearly answered and the laws of multiple jurisdictions must be applied.

The Privacy Act is intended to, at least partly, implement Australia's privacy obligations under the International Covenant on Civil and Political Rights and to give effect to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. However, international law has had limited influence on the development of Australian privacy jurisprudence. Also, and as at January2014, there is no right of individuals in Australia conferred by international law or the Australian Constitution that protects an individual's seclusion or other 'rights' of privacy. Nor is there a common law or other general legal right of protection from invasion of privacy. Although some Australian court dicta supports the possibility of the development of a tortious cause of action for serious invasion of personal privacy, on current Australian law the availability of that right, and availability of practical and effective remedies to enforce it, is highly questionable. There has been an active debate in Australia as to whether there should be a statutory cause of action for serious invasion of personal privacy and, if so, as to the appropriate remedies and enforcement mechanisms. That debate had been significantly influenced by concerns that investigative journalism could be significantly constrained by any private right of action in privacy. In June 2013, the then Australian Attorney-General commissioned the ALRC to conduct an inquiry into the protection of privacy in the digital era. The Terms of Reference require the ALRC to report by June 2014 and to make recommendations regarding, among other things, the legal design of a statutory cause of action for serious invasions of privacy, including legal thresholds; the effect of the implied freedom of political communication; jurisdiction; fault elements; proof of damages; defences; exemptions and access to justice. The ALRC's Discussion Paper, including its draft recommendations, is expected to be released in March 2014.

**international law has had limited influence on the development of Australian privacy jurisprudence**

Although private rights of action for privacy related acts or practices are currently limited, private rights of action may arise through recourse to other causes of action, including where an entity has engaged in misleading or deceptive conduct by failing to comply with the entity's privacy policy. This might lead to proceedings under section 18 of the Australian Consumer Law (Schedule 2 to the *Competition and Consumer Act 2010*) through private right of action or enforcement action by the Australian Competition and Consumer Commission (***ACCC***). The United States Federal Trade Commission (***FTC***) does not have any express jurisdiction to address privacy breaches, but the FTC has become an active privacy regulator through prosecution of alleged violations of section 5 of the *US Federal Trade Commission Act* or the *FTC Act* (15 USC 45), which bars unfair and deceptive acts and practices in or affecting commerce. This power has been used in law enforcement to require companies to live up to promises to consumers that they will safeguard their personal information and enabled the FTC to exact very substantial fines where companies fail to do so.

Practical remedies for Australians adversely affected by privacy invasive practices of businesses may also be available through the operation of binding APP codes and other binding sector-specific codes with privacy provisions. These include codes regulating broadcasting and the print media, the banking and financial services sectors and the provision of telecommunications services (including internet access services) to Australian consumers.

## More detail about the federal Privacy Act

Under the Australian federal system, the Privacy Act applies to the handling of personal information by the Australian federal government and its agencies and the Australian Capital Territory (ACT) government and its agencies. The federal Privacy Act also governs the private sector, including corporations and other businesses, but (subject to important exceptions) only operates where annual Australian revenue of the Australian group business is greater than AU$3 million.

Organisations and agencies are collectively referred to as 'APP entities'. Many provisions of the Privacy Act apply to all APP entities, but some apply only to agencies, and some only to organisations.

The Privacy Act defines 'organisation' broadly to include an individual, body corporate, partnership, trust or any unincorporated association.

The APPs are arranged in the order of the personal information lifecycle, from collection, to use, to disclosure, to retention. They are not lengthy, but their interpretation can be complex. The Commissioner's new Guidelines as to their interpretation and operation of the APPs run to over two hundred pages. As already noted, some APPs draw distinctions between organisations and agencies, while otherwise applying to all APP entities. Some APPs require different and higher standards in relation to the sub-category of personal information that is sensitive personal information.

**The APPs are arranged in the order of the personal information lifecycle, from collection, to use, to disclosure, to retention.**

Subject to those qualifications, the coverage of the APPs is summarised below:

**APP 1 - Open and transparent management of personal information**
APP entities (that is, entities regulated by the Australian privacy laws) must manage personal information in an open and transparent way.

This includes having a clearly expressed and up to date APP privacy policy. Collection, use and retention of personal information should be minimised to that reasonably required as notified in a privacy policy or otherwise with a user's consent.

'Transparent' is not defined, but as used in the Australian Consumer Law a contractual term is 'transparent' if it is expressed in reasonably plain language, legible, presented clearly and readily available to the person affected by the term. The positive obligation for organisations to implement practices, procedures and systems to 'manage' personal information has been interpreted as requiring implementation of privacy assurance practices and procedures – sometimes called 'Privacy by Design' - into business processes and products.

**APP 2 - Anonymity and pseudonymity**
APP entities must give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

**APP 3 - Collection of solicited personal information**

Outlines when an APP entity can collect personal information that is solicited by the entity.

APP 3 applies higher standards to the collection of 'sensitive' information, such as health information.

**APP 4 - Dealing with unsolicited personal information**
Outlines how APP entities must deal with unsolicited personal information.

**APP 5 - Notification of the collection of personal information**
Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 1 and APP 5 together set out quite prescriptively those things that need to be notified to an individual in relation to any collection of personal information about that individual.

Special requirements apply where personal information about an individual is collected from anyone other than the affected individual.

**APP 6 - Use or disclosure of personal information**
Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

**APP 7 - Direct marketing**
An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met. Broadly, direct marketing:

- is use or disclosure of personal information to communicate directly with an individual to promote goods and services;
- may only be undertaken where an individual would reasonably expect it, such as with informed consent;
- must provide a prominent statement about a simple means to opt out;
- must be stopped when an individual opts-out.

**APP 8 - Cross-border disclosure of personal information**
Outlines the steps an APP entity must take to protect personal information before it is disclosed to any other entity (including related entities) overseas.

**APP 9 - Adoption, use or disclosure of government related identifiers**
Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

Examples of government related identifiers are divers licence numbers, Medicare numbers, Australian passport numbers and Centrelink reference numbers.

**APP 10 - Quality of personal information**
An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

**APP 11 - Security of personal information**
An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

An entity has obligations to destroy or de-identify personal information in certain circumstances.

**APP 12 - Access to personal information**
An APP entity must provide access when an individual requests to be given access to personal information held about them by the entity.

Some limited, specific exceptions apply.

**APP 13 - Correction of personal information**
An APP entity must correct information held by it about an individual in response to a reasonable request by an affected individual.

Under the Privacy Act as amended from March 2014, industry groups or sectors may develop privacy codes of practice - so-called 'APP codes' - for review and possible registration by Office of the Australian Information Commissioner. If accepted for registration (and then in like manner to ACMA Codes) an APP Code becomes binding upon organisations within the industry sector specified in the Code. In other words, a Code once registered binds not only initial or later signatories to the Code, but also binds organisations within the industry sector to which the Office of the Australian Information Commissioner designates the Code applies. To date, only a small number of such codes have been approved, including in particular the Credit Reporting Privacy Code issued under the Privacy Act. It is expected that other industry codes will be now developed and registered with the OAIC.

## Other privacy laws

The Privacy Act does not regulate the handling of personal information by Australian state or territory governments and their agencies, except to a very limited extent. Some Australian states and territories have enacted privacy statutes containing data protection principles broadly similar to the federal privacy principles that, in general, are enforced by State officers styled 'Privacy Commissioners' or similar. These state and territory laws govern acts and practices of the respective Australian state or territory government and its agencies. In some cases these statutes also govern handling by the private sector on behalf of the government or its agency of personal information collected by the government or its agencies. In addition, some Australian state and territory jurisdictions have legislation that extends to private sector handling of particular categories of sensitive personal information collected directly by the private sector. One example is the State of Victoria's *Health Records Act 2001,* which regulates health related Information about individuals that is collected in the State of Victoria. Workplace surveillance, surveillance in public places, use of tracking devices, geo-tracking and recording technologies is currently regulated by state and territory statutes that are diverse and inconsistent.

Certain criminal laws also provide protection for individuals from intrusions about their right to seclusion, including in particular laws on unauthorised access to computer systems, electronic stalking and harassment, and unauthorised audio-visual capture of sexual activity, also regulate and protect privacy. Handling of telecommunications customer data is subject to sector specific regulation, principally through the *Telecommunications Act 1997*, a federal Act. The *Telecommunications Act 1997* is administered by the Federal Minister for Communications and by the Australian Communications and Media Authority (***ACMA***). The ACMA also administers Codes registered under the *Telecommunications Act 1997* that, once registered by the ACMA, become binding upon the section of the telecommunications industry to which the code relates. The Telecommunications Consumer Protection Code 2012 is an important legally binding instrument that regulates the handling of customer data by Australian telecommunications carriers and carriage service providers. The federal *Telecommunications (Interception and Access) Act 1979,* administered by the Federal Attorney-General, regulates interception of telecommunications (including email) traffic and access to stored communications held on email and other servers in Australia that are controlled by Australian licensed telecommunications carriers.

There are other industry specific codes that include privacy protective provisions that have varying levels of enforceability and sanctions. Perhaps the most important are the broadcasting codes of practice administered by the ACMA, which codes may be contravened where a television or radio broadcaster broadcasts material that is a serious invasion of an individual's privacy. The Australian Press Council administers a code of practice as to print media and its associated electronic outlets, which is contravened where a Council member publishes material that is a serious invasion of an individual's privacy. Other industry sectors deal with customer privacy in industry codes, including the Banking Industry Code of Practice and the Insurance Industry Code of Practice.

There are no cookie-specific laws such as those in the European Union. The use of cookies requires appropriate notification to internet users whenever personal information is collected through the use of those cookies.

*The Australian Guideline for Online Behavioural Advertising* is a self-regulatory guideline for third party online behavioural (interactive) advertising. The guideline regulates sharing of information between signatories to the guideline and third parties that would enable third parties to serve behavioural advertising to an internet user. In such a circumstance user consent and provision of a ready means for an individual to opt-out is required, regardless of whether personal information is disclosed by code signatory to the third party and regardless of whether cookies or other tracking technologies are used. The guideline prescribes the relevant requirements.

## Enforcement of the Privacy Act

As already noted, the Privacy Act is administered by the Commissioner within the OAIC. The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes. This involves investigating instances of non-compliance by agencies and organisations and prescribing remedies to redress non-compliance. The terms 'Privacy Commissioner' and 'OAIC' are often used interchangeably.

There are criminal penalties under the Privacy Act for unauthorised access to and disclosure of credit reporting PI. If, during an investigation, the Commissioner forms the opinion that these offences (and certain others under other Acts) may have been committed, he or she must refer the matter to the Australian federal police.

Criminal sanctions also apply to the unauthorised disclosure of PI during an emergency or disaster situation. The Australian federal police would investigate such offences.

The Commissioner has the power to investigate on his or her own motion, or in response to a complaint (from an individual or a class), acts and practices of organisations that may breach the APPs. In conducting investigations, the Commissioner must follow a prescribed process. The Commissioner can require the production of documents and information, and may also require people to appear and answer questions.

## The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes

The Commissioner may make a non-binding determination following investigation of a complaint where there has been a breach of the APPs. The Commissioner may determine that the conduct must not be repeated; that the agency or organisation must take action to redress the loss or damage caused; or that the complainant is entitled to a specified amount of compensation. The Commissioner may also dismiss the complaint or decide to take no further action. If it is necessary to enforce the Commissioner's determination, action must be taken in the Federal Courts.

From March 2014, the Commissioner also has a power to seek a Court injunction against a person engaging in conduct that may contravene the Privacy Act, to obtain enforceable undertakings by a person that has breached the Privacy Act, and to seek the making by a federal court of civil penalty orders where there is either a serious or repeated interference with the privacy of an individual. A civil penalty order may require a body corporate to pay up to $1.7 million. A civil penalty is a pecuniary penalty imposed by a court according to civil (as opposed to criminal) processes. It is expected that the new power to accept court enforceable undertakings from organisations will be used to gain agreement from organisations that experience data breaches to implement privacy compliance programmes and change existing information security and information handling practices. This power to accept court enforceable undertakings is similar to that enjoyed, and frequently used, by the ACCC under the *Competition and Consumer Act 2010* and by the ACMA under the *Spam Act 2003* and the *Do Not Call Register Act 2006*.

The Commissioner's new enforcement powers are summarised in the diagram on page 6.

In many cases there is parallel and potentially concurrent operation of federal law, state and territory law and industry codes of practice. This sometimes leads to simultaneous and sometimes coordinated enforcement action by multiple regulators, such as the OAIC and the ACMA. This has been the case on multiple occasions in relation to misuse of telecommunications customer data. Overlap may also arise in respect of other sectors. For example, a health PI data breach in Victoria may be handled by both the Victorian Health Services Commissioner and the Australian Privacy Commissioner.

## Exempt sectors and institutions

The Privacy Act does not apply to the collection, holding, use, disclosure or transfer of PI by an individual for the purposes of, or in connection with, the individual's personal, family or household affairs.

While the Privacy Act applies to many private and public sector organisations and agencies, certain entities are excluded from the Act's coverage. These include small business operators (generally, operators of businesses with an annual Australian turnover (determined on a corporate group basis) of less than A$3 million), registered political parties, organisations that are individuals acting in a non-business capacity, organisations acting under a state contract, employer organisations acting in respect of employee records and the Australian intelligence agencies.

The Privacy Act deals with employee records of public sector and private sector employees differently. The handling of personal information by a private sector employer is exempt from the Privacy Act if it is directly related to a current or former employment relationship or an employee record. The effect is that a private sector employer does not need to comply with the APPs when it handles current and past employee records, or grant a current or former access to the employee record about them. However, the employee records exemption relates to private sector organisations only: Australian, ACT and Norfolk Island government employee records are covered by the Privacy Act.

An act or practice is not an interference with privacy if it consists of the collection or disclosure of personal information by a body corporate from or to a 'related body corporate'. Before an organisation can rely on this exemption to disclose (non-sensitive) personal information to other related companies, it must take reasonable steps to ensure that the individual knows that the organisation has collected the information, the use that will be made of the information and the types of organisations to which the information is usually disclosed. In addition, although related companies may share personal information, the handling of that information is still subject to the APPs in all other respects. For example, each company within the group of related companies must only use the information for the primary purpose for which it was originally collected, and may only use the personal information for a secondary purpose permitted for the collecting organisation.

This partial exemption for related bodies corporate also does not apply in a range of circumstances, including (but not only) the collection or disclosure of 'sensitive information'; the collection of personal information from an entity that is exempt from the Privacy Act; where the company is a contractor under a Commonwealth contract and; the collection or disclosure of personal information from or to the related company is contrary to a contractual provision; and where the collection of personal information is for the purpose of meeting an obligation under the contract and the disclosure is for direct marketing purposes.

The journalistic activities of media organisations are exempt from the Privacy Act to the extent that such organisations publicly commit to observe published privacy standards (such as industry codes of practice). Currently, both print and broadcast media in Australia are required to adhere to principles and industry codes of practice that contain privacy standards applicable to journalistic activities, respectively the Australian Press Council's Statement of Privacy Principles and a number of broadcast television and radio Industry Codes of Practice administered by the ACMA. The area of media and convergent services regulation, including the effectiveness of media self-regulatory schemes, has been the subject of considerable controversy and a number of government reviews over recent years. It is likely that privacy regulation in the media sector will significantly change in the foreseeable future.

Further privacy reform, including as to the coverage exemptions, is likely. The ALRC recommended the repeal of the coverage exemptions for small business, registered political parties and employee records. The previous Australian (Labor) government undertook to consider these recommendations: it is unclear whether the current Australian coalition government will further consider the ALRC's recommendations.

Part 2 of this article will appear in the next edition of CLB.

***Peter Leonard is a partner at Gilbert+Tobin Lawyers and a director of the International Association of Privacy Professionals ANZ (iappANZ).***