An Overview of Privacy Law in Australia: Part 2

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

Communications, Surveillance, Marketing and Other Laws

It is important to note the limited coverage of Australian Federal privacy law. There is at present no common law right of action in Australia for intrusion upon an individual's seclusion or private affairs or for misuse or disclosure of private information. The Federal Privacy Act 1988 (the ***Privacy Act***) and some State and Territory Acts regulate the use by government agencies and many businesses of personal information as embodied in particular records. This is really a sub-category of private information that is personally information collected into a material form, such as a record, for use by regulated businesses and government. Some modes of invasion upon personal seclusion or private affairs are specifically regulated. There are a number of subject matter specific federal and state laws governing telecommunications interception (including access to stored communications such as emails), employee, optical (including video) surveillance, workplace surveillance and the use of recording devices, listening devices and tracking devices.

State and territory statutes dealing with interception, monitoring and surveillance laws vary substantially, both in scope of coverage and drafting

Certain forms of unsolicited marketing are also specifically regulated. New APP 7 regulates use or disclosure of personal information for the purpose of direct marketing activities. Direct marketing involves the use or disclosure of personal information to communicate directly with an individual to promote goods and services. A direct marketer may communicate with an individual through a variety of channels, including telephone, SMS, mail, email, online advertising and social media. Key factors in applying APP 7 are:

- ensuring that sensitive information is not used (unless there is express opt-in consent) for direct marketing;
- determining whether a particular marketing activity is 'direct marketing' that is regulated by APP 7;
- determining whether the *Spam Act 2003* (Cth) (***Spam Act***) or the *Do Not Call Register Act 2006* (Cth) (***DNCR Act***) apply to regulate the particular activity, such that APP 7 does not apply (because an exception in APP 7.8 operates); and

determining whether the organisation collected the personal information from the individual in circumstances where the individual would reasonably expect the organisation to use or disclose the personal information for the purpose of direct marketing; or whether the individual would not reasonably expect their information to be used or disclosed for that purpose or the information was collected from a third party.

APP 7 requires the direct marking organisation to provide a simple way for the individual to request not to receive direct marketing communications from the organisation. There must be a visible, clear and easily understood explanation of how to opt out and a process for opting out which requires minimal time and effort that uses a straightforward communication channel accessible at no more than nominal cost. In addition, in any circumstance where the individual would not reasonably expect their information to be used or disclosed for the purpose of direct marketing or personal information about them was collected from a third party, in each direct marketing communication with the individual the organisation must include a prominent statement ('opt out statement'), or otherwise draw the individual's attention to the fact, that the individual may request an opt-out.

Other instruments dealing with electronic marketing, interception, monitoring and surveillance, include the following:

- *the Spam Act 2003* (Cth) (***Spam Act***), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;
- *the Do Not Call Register Act 2006* (Cth) (***DNCR Act***), which regulates unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register and imposes certain conditions as to telemarketing generally (including as to time of day of calling);
- eMarketing Code of Practice, which contains rules and guidelines for the sending of commercial electronic messages. The Code is given legal effect by registration of that Code with the Australian Communications and Media Authority (***ACMA***);
- *Telecommunications (Interception and Access) Act 1979* (Cth), which among other things, regulates the interception of, and access to, stored communications by law enforcement agencies;
- a range of federal and state and territory statutes governing the use of listening devices and workplace surveillance;
- a more limited range of federal and state and territory statutes governing the use of unauthorised optical surveillance and tracking devices;
- state and federal criminal law provisions dealing with unauthorised access to computer systems; and
- the Australian Guideline for Third Party Online Behavioural Advertising.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being sent or caused to be sent. Com-

mercial electronic messages may only be sent with an individual's consent (express or implied in certain circumstances) and where the message contains accurate sender identification and a functional unsubscribe facility.

The Spam Act defines a 'commercial electronic message' as any electronic message (including e-mail, SMS, multimedia messages, instant messages or any other direct electronic messaging) where having regard to:

- the content of the message;
- the way in which the message is presented; and
- content that can be accessed by following any links, phone numbers or contact information in the message,

it could be considered that a purpose, or one of the purposes, of the message is to:

- offer, advertise or promote the supply of goods, services, land or business or investment opportunities;
- advertise or promote a supplier of goods, services, land or a provider of business or investment opportunities; or
- assist or enable a person to dishonestly obtain property, commercial advantage or other gain from another person.

Any electronic message that passes this test of commerciality is caught by the Spam Act (subject to certain exceptions). Commerciality may be a secondary purpose: for example, if a message is mainly factual or useful information, but has some marketing or promotional content, it is a commercial electronic message.

A message has an 'Australian link' if it originates or was commissioned in Australia, or originates overseas but was sent to an address accessed in Australia. The Spam Act expressly includes e-mails, SMS, instant messages and MMS. Whether the Spam Act can be applied to social media postings is less clear: although these may not be 'electronic messages' within the meaning of the Act, this position has not been tested.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the DNCR Act and associated legislation and instruments, including the important *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard* 2007.

Marketing faxes are regulated under the DNCR Act. This Act provides an 'opt-out' framework for these forms of marketing. Unsolicited telemarketing calls or faxes must not be made to an Australian number registered on the Do Not Call -Register.

The Spam Act and the DNCR Act are administered by the ACMA. Extensive material as to the operation of these statutes and enforcement activity by the ACMA is available at www.acma.gov.au.

State and territory statutes dealing with interception, monitoring and surveillance laws vary substantially, both in scope of coverage and drafting. There are important inconsistencies both in scope of coverage and treatment of technologies that are covered. Tracking device law makes it an offence in some states to track movement of devices even where there is no identification of the owner of those devices or their communications activities: this appears a simple overreach of regulation that potentially obstructs many benign new users of tracking for logistics, store traffic analysis and transport planning. In any event, surveillance laws do not provide nationally coherent coverage or comprehensive rights of seclusion for individuals. In addition, , many computer crime, unauthorised computer access, tracking devices and surveillance provisions were not drafted with regard to current applications of the internet and mobile devices and are therefore difficult to interpret and apply.

Other specific data protection rules in areas related to privacy include:

- Part 13 of the *Telecommunications Act 1997* (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data;
- state and territory privacy legislation, applying to personal information held by government agencies and, in some cases, health information and records (for example, the *Privacy and Personal Information Protection Act 1988* (NSW));
- the *Healthcare Identifiers Act 2010* (Cth), regulating (among other things) the use and disclosure of healthcare identifiers;
- the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), which regulates federal government data-matching using tax file numbers;
- the *Personally Controlled Electronic Health Records Act 2012* (Cth), which provides strict controls on the collection, use and disclosure of health information included in an individual's eHealth record; and
- federal and state/territory freedom of information legislation applying to information held by government agencies.

There is no legislation in Australia similar to the US Federal *Children's Online Privacy Protection Act of 1998* (***COPPA***), although COPPA principles are commonly applied in Australia as a matter of good corporate practice.

Privacy regulation operates up to the point at which personal information is transformed such that any risk that the information might either of itself, or in combination with other information, enable an individual to be identifiable becomes effectively impracticable

One of the few areas of clear and nationally consistent industry sector specific regulation is as to media reporting: there is a general carve out in the (Federal) Privacy Act for journalism by media organisations that self-regulate privacy compliance in their reporting, such as through the Statement of Privacy Principles administered by the Australian Press Council and the electronic broadcasting codes of practice overseen by the Australian Communications and Media Authority. However, the extent of that exception has itself been controversial: hence the continuing demands of privacy advocates for a broader right of seclusion and the countervailing media concerns as to freedom of reporting.

Personal Information

Generally, the (Federal) Privacy Act covers all processing (in Australian terms, itself a 'use') or use of 'personal information'.

The Act makes no express distinction between entities that control or own personal information, and those that provide services to owners (except in the case of contracted service providers to public-sector agencies). All such entities are regulated as APP entities in respect of their handling of personal information.

The definition of 'personal information' from March 2014 extends to information or an opinion about an individual who is reasonably identifiable, whether or not the information or opinion is recorded in a material form (this includes information communicated verbally) and regardless of whether that identification or re-identification is practicable from the information itself or in combination with or reference to other information.

Personal information will therefore include information about an individual whether collected or made available in a personal or business context and regardless of whether that information is in the public domain and the subject individual is specifically identified or consented for that information to enter the public domain.

Personal information remains such while identification or re-identification of an individual is 'practicable' either from the information itself or by reference to that information in combination with or by reference to other information. Privacy regulation operates up to the point at which personal information is transformed such that any risk that the information might either of itself, or in combination with other information, enable an individual to be identifiable becomes effectively impracticable. That transformation might be through aggregation or anonymisation of the personal information. Many organisations maintain multiple transaction databases, some of which may include personal information and some of which may include transaction data that does not identify a particular individual undertaking a transaction. These databases may be partitioned so that the non-identifying transactional database is not matched against the databases containing personal information. Partitioning of databases within organisations will be ineffective to allow non-identifying transactional data to be used without complying with the rules that relate to use of personal information, wherever there is any way in which an individual could be matched and tied to non-identifying transaction data, because the individual remains 'reasonably identifiable'. The Privacy Commissioner's February 2014 Guidelines put it this way:

APP 8, which deals with the cross-border disclosure of personal information from Australia to outside Australia, is not limited in its application by the nationality of the individual whose personal information is the subject of the transfer

> B.87 Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as 'personal information'. An individual may not be reasonably identifiable if the steps required to do so are excessively time-consuming or costly in all the circumstances.
>
> B.88 Where it is unclear whether an individual is 'reasonably identifiable', an APP entity should err on the side of caution and treat the information as personal information.

This view reflects regulatory guidance in some jurisdictions to the effect that determination as to whether information is 'personal information' is to be made having regard to all relevant circumstances as to possible re-identification by any reasonably contemplated recipient, or as it is sometimes put, to be made 'in the round', rather than having regard to whether the information was passed to the first recipient in apparently de-identified form. In assessing the risk of re-identification, regulatory guidance in some jurisdictions suggests that risk management strategies – or as it is sometimes put, technical, operational and contractual safeguards – are to be taken into account. The United Kingdom regulator suggests a 'motivated intruder' test: this test considers whether a reasonably competent motivated person with no specialist skills would be able to identify the data or information, having access to resources such as the internet and all public documents and making reasonable enquiries to gain more information.

Extraterritoriality

The Privacy Act applies to all acts or practices within Australia in respect of personal information about individuals wherever those individuals may reside. Accordingly, personal information of persons outside Australia that is held on servers located within Australia is regulated by the Act.

The Privacy Act extends to any use outside Australia or disclosure from Australia of personal information that has been collected within Australia, although the extraterritorial application of the Act in this area is subject to some uncertainty.

The Privacy Act has express extraterritoriality provisions, based upon a nexus of 'Australian link'. In general, corporations incorporated in Australia and Australian incorporated or constituted bodies are deemed to have an Australian link. The Act applies to an act or practice wherever done outside Australia by an agency (broadly, an Australian federal government entity). The Act also applies in relation to an act or practice outside Australia of an organisation or small business operator wherever that organisation or small business operator has a relevant 'Australian link'. However, a small business operator is regulated in relation to an act or practice outside Australia only to the extent similarly regulated in Australia.

Corporations and other bodies and agencies that do not fall into the above categories - broadly, any foreign corporation or body - will be regulated where: (1) the organisation carries on business in Australia; and (2) the personal information was collected or held by the organisation in Australia, either before or at the time of the act or practice.

The collection of personal information 'in Australia' includes the collection of personal information from an individual who is physically within the borders of Australia, or an external territory, by an overseas entity. The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* states that a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory and personal information is collected from that individual via a website and the website is hosted outside of Australia and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. The Explanatory Memorandum goes on to state that for the operation of the Act, entities such as those described in the last sentence who have an online presence (but no physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'. However, this interpretation is not supported by a plain reading of the Act and prior Australian jurisprudence (as to other statutory provisions) concerning 'carrying on business in Australia'. Accordingly, the operation of the Privacy Act in this scenario (without other factors indicating business presence in Australia) should be considered currently uncertain and potentially contentious.

An overseas act or practice (that takes place outside Australia and its external Territories) will not breach the APPs, an approved APP Code, or interfere with an individual's privacy, if the act or practice is required by an applicable foreign law. However, a similar act or practice within Australia pursuant to compulsion of an applicable foreign law is not excused from breach of the APPs or an approved APP Code, or from being an interference with an individual's privacy.

It is also important to note that APP 8, which deals with the cross-border disclosure of personal information from Australia to outside Australia, is not limited in its application by the nationality of the individual whose personal information is the subject of the transfer. In other words, APP 8 will apply to a cross-border disclosure of personal information collected in Australia, irrespective of whether the information relates to an Australian citizen or Australian resident or not.

Regulation of Collection, Use and Disclosure of Personal Information

The Privacy Act requires that the collection, use and disclosure of personal information must be justified on specific grounds.

An organisation must have an APP-compliant privacy policy that contains specified information, including the kinds of personal information it collects, how an individual may complain about a breach of the APPs, and whether the organisation is likely to disclose information to overseas recipients.

An organisation also needs to take reasonable steps to make its APP privacy policy available free of charge and in an appropriate form.

APP 1 also introduces a positive obligation for organisations to implement practices, procedures and systems that will ensure compliance with the APPs and any registered APP codes. APP 1 requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way. '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 has been suggested to require implementation of privacy assurance practices and procedures – so-called 'Privacy by Design' principles - into business processes and products.

APP 3 outlines when and how an organisation may collect personal and sensitive information that it solicits from an individual or another entity. An organisation must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the organisation's functions or activities.

APP 3 clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent if the collection is also reasonably necessary for one or more of the organisation's functions or activities.

An organisation must only collect personal information from the individual, unless it is unreasonable or impracticable to do so.

APP 4 creates obligations in relation to the receipt of personal information which is not solicited. Where an organisation receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If so, APPs 5 to 13 will apply to that information. If the information could not have been collected under APP 3, the organisation must destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.

APP 5 specifies certain matters about which an organisation must generally make an individual aware, at the time, or as soon as practicable after, the organisation collects their personal information.

In addition to other matters listed in APPs 1.4 and 5.2, APP 5 requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information.

APP 6 outlines the circumstances in which an organisation may use or disclose the personal information that it holds about an individual. If an organisation collects personal information about an individual for a particular purpose (the primary purpose), it must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents to the use or disclosure, or another exception applies.

Additional protections apply to the collection, use and disclosure of a subcategory of personal information called 'sensitive information', which the Privacy Act defines as information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions;
- membership of a political association;
- religious beliefs or affiliations;
- philosophical beliefs;
- membership of a professional or trade association;
- membership of a trade union;
- sexual orientation or practices; or
- criminal record,

which is also personal information; and

- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.

An organisation must not collect an individual's sensitive information unless an exception applies. Sensitive information may be collected about an individual with consent and if the information is reasonably necessary for one or more of the organisations activities or functions. Further, an organisation may collect sensitive information if required or authorised by or under an Australian law or a court/tribunal order or in certain permitted health situations, such as where the entity reasonably believes that the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety.

The positive obligation for organisations to implement practices, procedures and systems has been suggested to require implementation of privacy assurance practices and procedures – so-called 'Privacy by Design' principles - into business processes and products

The Privacy Act also contains special provisions that apply to personal information included in individuals' credit information files or in credit reports, including information about an individual's repayment history. These provisions also provide for consumer protection in relation to processes dealing with notification, data quality, access and correction and complaints.

The Privacy Act also provides for the making of guidelines by the Commissioner concerning the collection, storage, use and security of tax file number information. Compliance with the Tax File Number Guidelines is mandatory for all tax file number recipients.

APP 6 (Use and disclosure) generally restricts the use and disclosure of personal information to the primary purpose for its collection or related secondary purposes within the exceptions discussed above. A user may consent to other uses or disclosures.

Further restrictions on the disclosure of credit-related personal information are set out in the credit reporting provisions of the Privacy Act. Such disclosure restrictions include the following:

- a credit reporting body must not disclose personal information contained in an individual's credit information file to a third party unless one of the specified exceptions applies (such as where the information is contained in a credit report given to a credit provider for the purpose of assessing an application for credit by the individual); and
- a credit provider must not disclose any personal information in a credit report to a third party for any purpose (subject again to specified exceptions).

The Act also imposes specific restrictions on the disclosure of personal information from within Australia to outside Australia, as discussed below in the section on cross-border disclosure.

'Openness' and Notification

APPs 1 and 5 impose 'openness' requirements in relation to collection of personal information.

An APP entity must take reasonable steps to notify an individual, or otherwise ensure that the individual is aware, that its APP-compliant privacy policy contains information about how to access and seek correction of personal information, and information about the organisation's complaints process; and whether it is likely to disclose an individual's personal information to overseas recipients and, if it is practicable, to specify the countries in which those recipients are likely to be located. If it is not practicable to specify the countries in the notification, the organisation may make the individual aware of them in another way.

Notification obligations arise under the Privacy Act at the point of collection of personal information by an organisation, whether collected directly from the individual or obtained from a third party. If the organisation collects the personal information from someone other than the individual, or the individual may not be aware that the organisation has collected the personal information, it must also take reasonable steps to notify an individual, or otherwise ensure that the individual is aware:

- that the organisation collects or has collected the information, and
- of the circumstances of that collection (APP 5.2(b)).

Notification obligations arise under the Privacy Act at the point of collection of personal information by an organisation, whether collected directly from the individual or obtained from a third party

Some notification requirements may be addressed through the publication of a privacy policy. Specifically, APP 1.4 requires APP entities collecting personal information to specify the following matters in their privacy policy:

- the kinds of personal information that the entity collects and holds;
- how the entity collects and holds personal information;
- the purposes 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 Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the entity is likely to disclose personal information to overseas recipients;
- if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

More specific notification requirements are stated in APP 5. At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps as are reasonable in the circumstances to notify the individual of such matters referred to in subclause 5.2; or to otherwise ensure that the individual is aware of any such matters. The matters referred to in subclause 5.2 are:

- the identity and contact details of the APP entity;
- if the APP entity collects the personal information from someone other than the individual; or the individual may not be aware that the APP entity has collected the personal information, the fact that the entity collects or has collected the information and the circumstances of that collection;
- if the collection of the personal information is required or specifically authorised by Australian law or court order, details about that;
- the purposes for which the APP entity collects the personal information;
- the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
- any other person, or the types of persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
- that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
- that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the APPs, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- whether the APP entity is likely to disclose the personal information to overseas recipients;
- if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Use or disclosure of personal information for a purpose other than the primary purpose of collection (being a 'secondary purpose') is permitted under specific exceptions where that secondary use or disclosure is:

- required or authorised by or under an Australian law or a court order;
- necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities. APP 6.2(e) also permits the use or disclosure of personal information for a secondary purpose to an enforcement body for one or more enforcement related activities;
- in the conduct of surveillance activities, intelligence gathering activities or monitoring activities, by a law enforcement agency;
- the conduct of protective (for example, in relation to children) or custodial activities;
- to assist any APP entity, body or person to locate a person who has been reported as missing (where the entity reasonably believes that this use or disclosure is reasonably necessary, and where that use or disclosure complies with rules made by the Commissioner);
- for the establishment, exercise or defence of a legal or equitable claim; and
- for the purposes of a confidential alternative dispute resolution process.

Generally notification is required wherever a use or disclosure of personal information is made, unless a specific exception applies.

Control of Use

There are a number of provisions in the Privacy Act which directly, or indirectly, enable individuals to exercise a degree of choice or control over use of their personal information by organisations.

For example:

- APP 1 (Openness and transparency), which requires organisations to have ongoing practices and policies in place to ensure that they manage personal information in an open and transparent way;
- APP 2 (Anonymity and pseudonymity), which requires that an organisation provide individuals with the option of dealing with it using a pseudonym or anonymously. Both requirements are subject to certain limited exceptions, including where it is impracticable for the organisation to deal with an individual who has not identified themselves, or where the law or a court/tribunal order requires or authorises the organisation to deal with individuals who have identified themselves;
- APP 3 (Collection of solicited personal information), which clarifies that, unless an exception applies, sensitive information must only be collected with an individual's consent and if the collection is also reasonably necessary for one or more of the organisation's functions or activities;
- APP 5 (Notification), which requires organisations to notify individuals about the access, correction and complaints processes in their APP privacy policies, and also the location of any likely overseas recipients of individuals' information;
- APP 7 (Direct marketing), which requires the availability of opt-out mechanisms in relation to direct marketing;
- APP 12 (Access), which requires an organisation to give an individual access to the personal information that it holds about that individual, unless an exception applies. There is a new express requirement for organisations to respond to requests for access within a reasonable period. In addition, organisations must give access in the manner requested by the individual if it is reasonable to do so. If an organisation decides not to give an individual access, it must generally provide written reasons for the refusal and information about the mechanisms available to complain about the refusal; and
- APP 13 (Correction), which requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

Data accuracy

APP 10 (Integrity) requires an organisation to take reasonable steps to ensure that the personal information that it collects is accurate, up-to-date and complete.

In relation to use and disclosure, the APP 10 requirement is that an organisation will need to take reasonable steps to ensure that the personal information is relevant (in addition to being accurate, up-to-date, and complete), having regard to the purpose of that use or disclosure.

APP 13 (Correction) requires an organisation to take reasonable steps to correct personal information to ensure that, having regard to a purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading, if either the organisation is satisfied that it needs to be corrected, or an individual requests that their personal information be corrected. Organisations generally need to notify other APP entities that have been provided with the personal information of any correction, if that notification is requested by the individual.

Amount and Duration of Data Holding

There are no express restrictions as to the quantity of personal information an organisation may collect or hold, but organisations are prohibited from collecting and holding personal information unless the information is reasonably necessary for one or more of the organisation's functions or activities.

In addition, where the personal information is sensitive information, organisations are prohibited from collecting and holding that sensitive information unless the individual consents and the information is reasonably necessary for one or more of the organisation's functions or activities or if an exception applies.

APP 11.2 requires an APP entity to take reasonable steps to destroy or de-identify personal information if the organisation no longer needs it for any for which it may be used or disclosed in accordance with the APPs. There are two exceptions to this requirement: if the personal information is contained in a Commonwealth record, or if the organisation is required by or under an Australian law or a court order to retain the information.

Finality Principle

European privacy lawyers sometimes refer to a 'finality principle', to the effect that use and disclosure of personal information is limited by the purposes for which it was originally collected (subject to various exceptions). The concept is that organisations cannot change their minds about the uses they (or others) wish to make of personal information, after the event of collection.

The Australian Law Reform Commission (ALRC) recommended the introduction of a mandatory data breach notification scheme in its 2008 report

The 'finality principle' is partially reflected in APP 6 (Use or disclosure). If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless the individual has consented to the use or disclosure of the information; or an exception in subclause 6.2 or 6.3 applies.

Exceptions include:

- the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is, if the information is sensitive information, directly related to the primary purpose; or if the information is not sensitive information, related to the primary purpose;
- the use or disclosure of the information is required or authorised by or under an Australian law or a court order;
- the use or disclosure of the information is necessary to lessen or prevent a serious threat to any individual's life, health or safety, or to public health or safety, and it is unreasonable or impracticable to obtain the consent of the individual;
- the use or disclosure of the information is necessary in order for an organisation to take appropriate action in relation to a reasonable suspicion of unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities; or
- the individual has consented to the use or disclosure.

An APP entity may also use or disclose personal information for the secondary purpose of direct marketing subject to the prescriptive requirements of APP 7.

Data Security and Notification of Data Breaches

APP 11 (Security) requires organisations to take reasonable steps to protect personal information from misuse, interference and loss and unauthorised access, modification or disclosure. When personal information is no longer needed for an authorised purpose by an organisation, it must take reasonable steps to destroy or permanently de-identify it.

Reasonable steps in relation to protection of personal information will vary with the circumstances. Relevant circumstances include (by way of non-exhaustive examples) how sensitive the personal information is, how it is stored (e.g. paper or electronically), the likely harm to the data subject if a breach occurred and the size of the organisation. Similarly, destruction or de-identification processes will vary. In any event, personal information should be destroyed securely and de-identified such that the data subject's identity is no longer reasonably ascertainable from the personal information.

In April 2013, the Office of the Australian Information Commissioner (***OAIC***) published a guide to information security which discusses some of the circumstances that the OAIC takes into account when assessing the reasonableness of the steps taken by entities to ensure information is kept secure. This guide presents a set of non-exhaustive steps and strategies that may be reasonable for an entity to take in order to secure personal information. The OAIC has stated that the Commissioner will refer to this guide when assessing an entity's compliance with security obligations in the Privacy Act.

The transfer of personal information to entities providing outsourced processing services in Australia, therefore, constitutes a disclosure of personal information for the purposes of the Privacy Act

The Privacy Act does not presently impose obligations on agencies or organisations to notify either the OAIC, or the individual concerned, of security breaches involving personal information.

However, the OAIC recommends notification in its guidelines on this area 'Data Breach Notification: A guide to handling personal information security breaches, April 2012'. These guidelines are generally followed by corporations in Australia.

The Australian Law Reform Commission (ALRC) recommended the introduction of a mandatory data breach notification scheme in its 2008 report, 'For Your Information: Australian Privacy Law and Practice'. In 2013, the then federal government introduced the Privacy Amendment (Privacy Alerts) Bill 2013. This Bill had not been passed by both Houses of the Federal Parliament when the Parliament was prorogued and accordingly lapsed. If enacted, this Bill would have built upon the OAIC's scheme of voluntary notification of serious data breaches by entities, as set out in the OAIC's guidelines. The Bill proposed a high threshold based on a reasonable belief by the entity concerned that the data breach is sufficiently serious to pose a real risk of serious harm to affected individuals. In the event of such a breach, the provisions of the Bill, if enacted, would have required the entity to notify affected individuals and the Information Commissioner as soon as practicable. The provisions of the Bill would require that the data breach notice include:

- the identity and contact details of the entity;
- a description of the breach;
- the kinds of personal information concerned;
- recommendations about the steps that individuals should take in response to the breach; and
- any other information specified in any made regulations under the Bill (if enacted).

As at May 2014, it was not clear whether the Coalition Government would re-introduce data breach notification legislation.

Data Protection Officer

Australia has no mandatory requirement to appoint a data protection officer.

It is becoming more common for major corporations to appoint a privacy professional, generally working within a legal or regulatory compliance team. However, there is no legal obligation to do so.

Record Keeping

There is no general requirement as to record keeping. However, the Privacy Act does require an organisation to keep a written note of any use or disclosure of personal information where the organisation reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Written notes must also be made in relation to certain uses or disclosures of credit related personal information, including the use and disclosure of such information for direct marketing pre-screening assessments.

Further, reasonable steps under APP 11 (Security) may require certain processes to be established, depending on the circumstances.

Some Australian states require owners of health-related personal information to keep records of when this type of personal information is disposed of or deleted.

Access

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information (APP 12 (Access)).

Exceptions apply, as outlined below.

An APP entity's privacy policy should include information about how an individual may access personal information about the individual that is held by the entity and seek the correction of such information (APP 1.4(d)).

An APP entity must respond to a request for access to the personal information if the entity is an agency, within 30 days after the request is made; or if the entity is an organisation, within a reasonable period after the request is made; and give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Exceptions applicable to organisations include where:

- the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court order;
- the entity has reason to suspect unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; and
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

If the APP entity refuses to give access to the personal information or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

- the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- the mechanisms available to complain about the refusal; and
- any other matter prescribed by regulations made pursuant to the Act.

A sector specific access and correction framework applies in relation to credit related information.

If an APP entity holds personal information about an individual; and either the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or the individual requests the entity to correct the information, the entity must take such steps as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading (APP 13.1 (Correction)).

A breach of the APPs generally does not give rise to a cause of action exercisable at the suit of the affected individual. However, in certain circumstances the Commissioner can exercise jurisdiction and seek damages on behalf of an affected individual.

Cross-Border Disclosure and Transfer of Personal Information

Transfer of personal information is not regulated as such: the relevant act or practice that is regulated is use or disclosure of personal information. Accordingly, it is not relevant whether the custody and control of the personal information is transferred to the provider of outsourced processing services: it is sufficient if there is a disclosure, such as through the provider being provided with any form of access to the personal information.

The transfer of personal information to entities providing outsourced processing services in Australia, therefore, constitutes a disclosure of personal information for the purposes of the Privacy Act. The Privacy Act makes no distinction between disclosure of personal information to outsourced processing services and disclosure of personal information to any other third party. Each disclosure would need to be undertaken subject to the requirements of APP 6 (Use and disclosure).

APP 6 generally prohibits the disclosure of personal information by organisations unless the disclosure is consistent with the primary purpose for collection of the information, or a related secondary purpose.

However, there is an exception under the Act in relation to use or disclosures by related bodies corporate: broadly, related bodies corporate are treated as a single entity for the purposes of privacy regulation.

APP 8 also imposes restrictions on the disclosure of personal information to recipients outside Australia: these restrictions apply in addition to the disclosure restrictions under APP 6.

As is the case with disclosures to third parties within Australia, transfer of personal information to outside Australia is not regulated as such: for example, in relation to Australian regulated personal information an organisation may transfer Australian regulated personal information from its branch in Australia to another branch of itself outside Australia, or provide its overseas branch with electronic access to its Australian based database. However, in relation to any Australian regulated personal information, provision of electronic access (including read-only access) to a third party 'overseas recipient', including a related body corporate of the discloser, is a disclosure of that personal information. If the third party to whom the personal information is disclosed is outside Australia, APP 8 (Cross-border disclosure) will operate.

APP 8 does not specifically address the common scenario of provision of custody and management of encrypted Australian regulated personal information to a provider of outsourced hosting services. A sensible view is that unless there is any reasonable possibility that the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the personal information might also have the capability to decrypt and thereby at least view personal information, there is no 'disclosure' of that personal information to any overseas recipient. On this view, capability needs to be assessed 'in the round', having regard to technical capability of the provider of outsourced hosting services or persons that might reasonably be anticipated to have access to the encrypted personal information), and operational and contractual safeguards against decryption or other misuse, taken together. The Australian Privacy Commissioner's APP Guideline on APP 8 (Cross-border disclosure of personal information) at paragraph 8.14 suggests that the Privacy Commissioner will consider the provision of personal information to cloud service providers located overseas for the limited purpose of storing and ensuring that the Australian regulated entity may access that information as 'use' rather than a 'disclosure' by the Australian regulated entity if:

In practice, determining whether the provision of information to service providers constitutes a 'disclosure' or 'use' will likely be a difficult exercise and will ultimately turn on the nature of the services provided and the terms of the services agreement

- the contract with the provider requires the provider to only handle the information for these limited purposes;
- the contract with the provider requires that any sub-contractors to the provider must agree to the same obligations; and
- the contract gives the Australian entity effective control of how the personal information is handled by the overseas entity. According to the Privacy Commissioner, contractual indicators that an APP entity has retained effective control of the information include: whether the entity has retained the right or power to access, change or retrieve the personal information; who else will be able to access the personal information and for what purposes; the types of security measures that will be used for the storage and management of the personal information; and whether the personal information can be retrieved or permanently deleted by the entity when no longer required at the end of the contract.

In practice, determining whether the provision of information to service providers constitutes a 'disclosure' or 'use' will likely be a difficult exercise and will ultimately turn on the nature of the services provided and the terms of the services agreement. APP entities are expected to take a cautious approach to this issue until further clarity around the concept of 'disclosure' is provided by the Australian Privacy Commissioner or the courts.

APP 8 and section 16C of the Act also introduce an accountability approach to cross-border disclosures of personal information.

Before an organisation discloses personal information to an overseas recipient, the organisation must take reasonable steps to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information. In some circumstances an act done, or a practice engaged in, by the overseas recipient that would breach the APPs, is taken to be a breach of the APPs by the organisation. Generally, this will apply where:

- APP 8.1 applies to the disclosure (APP 8.1 applies to all cross-border disclosures of personal information, unless an exception in APP 8.2 applies); and
- the overseas recipient is not subject to the APPs, but the act or practice would be a breach of the APPs if they were.

APP 8.2 lists a number of exceptions to APP 8.1. For example, APP 8.1 will not apply where:

the organisation reasonably believes that the recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is, overall, substantially similar to the APPs; and there are mechanisms available to the individual to enforce that protection of the law or binding scheme (APP 8.2(a)); or

an individual consents to the cross-border disclosure, after the organisation expressly informs them that APP 8.1 will no longer apply if they give their consent (APP 8.2(b)).

the Australian Privacy Commissioner has not issued a list of countries whose laws, or binding privacy schemes, that the Australian Privacy Commissioner considers have the effect of protecting the information in a way that is, overall, substantially similar to the APPs and allow for appropriately effective and available enforcement mechanisms

Each of these two exceptions is difficult to interpret and apply. Attempts to invoke the exceptions are likely to be the subject of significant debate and regulatory scrutiny.

As to the former, the Australian Privacy Commissioner has not issued a list of countries whose laws, or binding privacy schemes, that the Australian Privacy Commissioner considers have the effect of protecting the information in a way that is, overall, substantially similar to the APPs and allow for appropriately effective and available enforcement mechanisms. Law firms may be expected to be unwilling to 'sign off' based upon an 'overall' assessment of laws and remedies or as to a contractual scheme, noting the difficulties of such an assessment and the exposure of the Australian entity to strict liability under section 16C in the event of any subsequent determination by the Australian Privacy Commissioner (or court enforcing a determination of the Australian Privacy Commissioner) that the foreign laws or a scheme did not in fact not qualify for the exception in APP 8.2(a). However, the Privacy Commissioner's Guidelines (at paragraph 8.21) do give some support to the use of binding corporate rules (BCRs) by international organisations, at least where the BCRs reflect "the stringent, intra-corporate global privacy policy that satisfies EU standards".

As to notice and consent, the form, prominence (conspicuousness) and level of comprehensibility of the 'express informing' are likely to be controversial. It is clear that the express notice needs to be sufficiently clear, but to ensure fully informed consent must the notice spell out what the practical effect of APP 8.1 not applying will be? The Privacy Commissioner's Guidelines (at paragraphs 8.28 to 8.30) are not prescriptive as to the form of notice, beyond stating that at the minimum the statement should explain that if the individual consents to the exposure and the overseas recipient handles the personal information in breach of the APPs, the (Australian regulated) entity will not be accountable under the Privacy Act and the individual will not be able to seek redress under the Privacy Act. Many notices as recently revised do not comply with these 'minimum' requirements. For example, consider a notice as follows (following a description of permitted purposes):

> You consent to your personal information being disclosed to a destination outside Australia for these purposes, including but not limited to the United States of America, and you acknowledge and agree that Australian Privacy Principle 8.1 will not apply to such disclosures and that we will not be required to take such steps as are reasonable in the circumstances to ensure such third parties outside of Australia comply with the Australian Privacy Principles.

The notice does not include the second limb required by the Commissioner: it does not state that the individual will not be able to seek redress under the Privacy Act. Other questions remain. How prominent does this notice need to be? If the consent is to have an ongoing operation, does the notice or consent need to be reinforced, or otherwise the subject of reminders, at periodic intervals, and if so, how often? Is the form of consent required for APP 8.2(b) different to the form of consent for other purposes, noting in this regard the unusual juxtaposition in the drafting of APP 8.2(b) of expressly informs and after being so informed, the individual consents?

APP 8.2 also introduces a number of other circumstances in which APP 8.1 will not apply:

- where the cross border disclosure is required or authorised by or under an Australian law, or a court/tribunal order (APP 8.2(c));
- where an organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (APP 8.2(d), s16A item 1);
- where an organisation reasonably believes that the disclosure is necessary to take action in relation to the suspicion of unlawful activity or misconduct of a serious nature that relates to the organisation's functions or activities (APP 8.2(d), s 16A item 2);
- where an organisation reasonably believes that the disclosure is necessary to assist any APP entity, body or person to locate a person who has been reported as missing (APP 8.2(d), s 16A item 3).

The restrictions of APP 8 apply equally to overseas transfers to service providers as to other overseas recipients. The accountability requirements of APP 8 and section 16C of the Act apply in respect of the first recipient and any subsequent recipient.

However, an act or practice engaged in outside Australia does not breach the APPs if that act or practice is required by an applicable law of a foreign country.

Credit Related Provisions

Probably the most complex changes to the Privacy Act are the credit related provisions now completely redrafted in Part IIIA of the Privacy Act (the ***CR Scheme***).

The CR Scheme applies exclusively to the collection, use and disclosure of personal credit-related information about individuals and regulates the handling of a particular type of personal credit-related information, namely credit information. Credit information comprises, on the whole, information about an individual's consumer credit history. However, credit information may also include some information about an individual's commercial credit history. One example is court proceedings information about an individual, which may relates to both commercial and consumer credit history.

The CR Scheme sets out the limited purposes for which a credit provider may use an individual's credit information. These permitted purposes include the assessment of an application for consumer credit or commercial credit (the latter only with the individual's express consent). As such, the application of the CR Scheme is not necessarily dependant on whether an individual is applying for consumer or commercial credit. Rather, the determining factor as to the

CR Scheme's application is whether a credit provider is proposing to collect, use or disclose credit information about an individual.

The majority of the restrictions in the CR Scheme address collection, use and disclosure of credit information in the course of a credit provider's engagement with a credit reporting bureau (***CRB***), such as Veda Advantage or Experian. (There are also other provisions that deal specifically with a credit provider's disclosure of information to other entities, such as debt collectors). Accordingly, if a credit provider does not collect from a CRB, or disclose to a CRB, credit information about individuals, many of the key provisions in the CR Scheme are not applicable.

The following categories of credit information are regulated under the CR Scheme.

- As noted above, the first and foundational category of information regulated by the CR Scheme is called credit information. In basic terms, credit information is essentially the personal credit-related information a credit provider collects from its dealings with an individual and discloses to a CRB. Credit information is defined exhaustively in the CR Scheme to include limited kinds of personal credit-related information, such as identification information, default information and repayment history information.
- Credit information is repackaged and consolidated with other information held by a CRB to form credit reporting information. Credit reporting information includes credit information and any information derived by CRB from the credit information. CRBs disclose credit reporting information about individuals to credit providers that request the information.
- In the hands of a credit provider, credit reporting information becomes credit eligibility information, which comprises the credit reporting information that is obtained from a CRB and any other information a credit provider derives from that information. The restrictions in the CR Scheme that govern use and disclosure of credit eligibility information by a credit provider apply only to information obtained from a CRB (and information derived therefrom) and not any other information a credit provider may have collected directly from the individual.

The CR Scheme must be read in conjunction with the terms of the Credit Reporting Privacy Code (***CR Code***). The CR Code is legally binding on credit providers and sets out further and more detailed restrictions and obligations relating to (among other things) the collection, use and disclosure of personal credit-related information.

For the purpose of determining whether an organisation is a credit provider under the CR Scheme in relation to a particular transaction, it is irrelevant whether the organisation provides a customer with consumer credit or commercial credit. This distinction only becomes relevant in relation to the purposes for which the entity may use and disclose credit information. Section 6G of the Privacy Act describes a number of scenarios in which an entity is deemed to be a credit provider. Of most general relevance, an organisation is a credit provider if it carries on a business in the course of which it provides credit in connection with the sale of goods, or the supply of services, by the supplier; and the credit is available for at least 7 days.

Emerging trends and issues

Emerging trends in Australian privacy law will reflect global trends, concerns and issues as they arise. Australia tends to closely follow major global trends, paying particular attention to regulatory developments in the U.S.A., European Union and ASEAN region.

Current trends include:

- Applications for registration and registrations of APP codes. The amendments to the Privacy Act effective from March 2014 give a prominent role to enforceable industry codes. It is expected that there will be significant industry sector activity in development of codes.
- Possible introduction of mandatory data breach notification requirements.
- Increased focus upon privacy by design and information security by design principles and practical implementation of privacy protective processes and systems by corporations.
- Review of published privacy policies for 'transparency': prominence, readability and structuring appropriate to the likely readers and as to the description of primary and secondary purposes of personal information.
- Pressure for expansion of privacy protection in relation to surveillance and geo-tracking devices and extension of the definition of personal information, or introduction of new restrictions as to 'profiling', to address concerns as to particular, perceived socially detrimental uses of big data analytics.
- Extension of privacy policy development and privacy and information security related enforcement activities by the ACMA (www.acma.gov.au), a well-resourced regulator by comparison with the Australian Privacy Commissioner.

For the purpose of determining whether an organisation is a credit provider under the CR Scheme in relation to a particular transaction, it is irrelevant whether the organisation provides a customer with consumer credit or commercial credit

- Changes to privacy regulation of news gathering and news reporting by the print and electronic media. It is likely that media codes or other media regulation affecting privacy will change in the foreseeable future.
- The ALRC's consultation and report (due June 2014) as to introduction of a statutory cause of action for serious invasion of privacy.
- Continuing pressure for more extensive regulation of third party online behavioural advertising.
- More active cross-border coordination and joint enforcement activity by the Australian Privacy Commissioner and comparable regulators in other jurisdictions.
- Continuing consultation as to alignment of privacy regulation in the Asia Pacific region.
- Focus upon law enforcement exceptions to privacy laws following the Edward Snowden revelations as to activities of the U.S. National Security Agency and national security collaboration between the 'Five Eyes' countries, including Australia.

Given the volatility and unpredictability of emergence of issues in privacy regulation, it is likely that the above list will change by addition of further issues.

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