Australian Data Protection and Privacy Laws
A Primer

Peter Leonard[1]
Principal, Data Synergies

June 2019

[1] Peter Leonard is a data, content and technology business consultant and lawyer advising data-driven business and government agencies. Peter is principal of Data Synergies and a Professor of Practice at UNSW Business School (IT Systems and Management and Business and Taxation Law). Peter chairs the IoTAA's Data Access, Use and Privacy work stream, the Law Society of New South Wales' Privacy and Data Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee. He serves on a number of corporate and advisory boards. including of the NSW Data Analytics Centre. Peter was a founding partner of Gilbert + Tobin, now a large Australian law firm. Following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. The views expressed in this Primer are those of the author not those of any of those other bodies and organisations..

CONTENTS

1 LEGISLATION

1.1 Key statutes

Privacy, surveillance and data protection regulation is shared between federal jurisdiction (Commonwealth of Australia or Australian Parliament), the six states and two territories (Australian Capital Territory and Northern Territory).

The principal statute regulating collection, use, storage and disclosure of 'personal information' is the federal Privacy Act 1988 (**Privacy Act**), including the thirteen Australian Privacy Principles (**APPs**) which form part of that Act.

The Privacy Act is administered by the Office of the Australian Information Commissioner (**OAIC**) and the Australian Privacy Commissioner within that office.

The Privacy Act applies to the handling of personal information about individuals (within and outside Australia) by, amongst others, Australian federal government agencies and most private sector organisations.

Due to the sensitive nature of health information, the Australian health sector is subject to additional and specific statutory restrictions in relation to data protection. Relevant statues include:

- My Health Records Act 2012, My Health Records Rule 2016 and My Health Records Regulation 2012, which creates the legislative framework for the Australian Government's My Health Record system. The My Health Records Act limits when and how health information included in a My Health Record can be collected, used and disclosed. Collection, use or disclosure of My Health Record information without proper authorisation is both a breach of the My Health Records Act and an interference with privacy. The OAIC regulates the handling of personal information under the My Health Record system by individuals, Australian Government agencies, private sector organisations and (in particular circumstances) State and Territory agencies.

- Healthcare Identifiers Act 2010 (Cth), regulating (among other things) the use and disclosure of healthcare identifiers.

- State and Territory health information protection acts. The Health Records Act 2001 (Vic), the Health Records and Information Privacy Act 2002 (NSW) and the Health Records (Privacy and Access) Act 1997 (ACT) govern the handling of health information in both the public and private sectors in Victoria, NSW and ACT respectively.

The telecommunications sector is also subject to additional and specific statutory restrictions under:

- Part 13 of the Telecommunications Act 1997 (Cth), which imposes restrictions on the use and disclosure of telecommunications and communications-related data. Restrictions include offences for unauthorised disclosure by telecommunications carriers and carriage service providers of content of communications;

- Telecommunications (Interception and Access) Act 1979 (Cth), which among other things, regulates the interception of, and access to, the content of communications transiting telecommunications networks and stored communications (e.g. SMS and emails) on carrier networks with enforcement agencies, and requirements provision of interception capability and access to stored communications by Australian telecommunications carriers and nominate carriage service providers. This Act also includes provisions relating to assistance to law enforcement agencies, mandating retention by telecommunications service providers of certain information about communications, and requirements for a broad range of internet service providers to provide assistance to law enforcement agencies in relation to encrypted communications;

- mandatory industry codes of practice administered by the Australian Communications and Media Authority and governing (among other things) telecommunications data relating to consumers; and

- state and territory telecommunications interception laws.

There are a range of other laws in Australia, at the federal, state and territory level, which impact data protection. These include:

- Spam Act 2003 (Cth), which deals with the sending of unsolicited commercial electronic messages, including emails and SMS;

- Do Not Call Register Act 2006 (Cth), regulating unsolicited commercial calling to telephone numbers listed on the national Do Not Call Register;

- federal and state and territory laws governing telecommunications interception and access to stored communications, the use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces and computer and data surveillance of workplaces (including employees working from home or using work supplied devices or other resources);

- federal and state and territory freedom of information legislation, applying to information held by government agencies;

- Data-matching Program (Assistance and Tax) Act 1990 (Cth) which regulates the Federal government data-matching using tax file numbers (**TFN**). The Privacy (Tax File Number) Rule 2015 issued under the Privacy Act also regulate the collection, storage, use, disclosure, security and disposal of individuals' TFN by public agencies and private organisations;

- federal and state criminal laws dealing with unauthorised access to computer systems, including databases;

- federal and some state laws criminalising publication of so-called illegal or offensive content;

- federal and some state laws protecting certain classes of 'whistle-blowers' (for example, in relation to alleged illegal conduct of Federal government agencies and Australian regulated corporations); and

- developing judge-made law extending the equitable doctrine of protection of confidential information (trade secrets).

State and territory information privacy laws apply to state and territory government, government agencies and contractors to government and its agencies. Relevant statutes and instruments include:

- in New South Wales, the Privacy and Personal Information Protection Act 1998 (NSW), the Government Information (Public Access) Act 2009 (NSW) and Health Records and Information Privacy Act 2002 (NSW), as each administered by the NSW Information and Privacy Commission. These statutes regulate the handling of personal information by NSW public sector agencies and providers of health services in New South Wales and those providers' subcontractors. Health privacy complaints may be made to the Health Care Complaints Commission or the NSW Privacy Commissioner. The NSW Privacy Commissioner may refer a complaint to the Health Care Complaints Commission, the federal Privacy Commissioner or to any other person or body the Commissioner considers to be relevant in the circumstances. ;

- in Victoria, the Privacy and Data Protection Act 2014 (Vic), as administered by the Office of the Victorian Information Commissioner, and the Health Records Act 2001 (Vic), as administered by the Victorian Health Complaints Commissioner. These statutes regulate the handling of personal information by Victorian public sector agencies and providers of health services in Victoria and those providers' subcontractors;

- in Queensland, the Information Privacy Act 2009 (Qld) as administered by the Queensland Office of the Information Commissioner. This statute regulates the handling of personal information by Queensland public sector agencies;

- in South Australia, SA Department of the Premier and Cabinet Circular, PC012 – Information Privacy Principles Instruction, 16 September 2013. This is an administrative instruction issued by the South Australian Government requiring government agencies to generally comply with a set of Information Privacy Principles. The Privacy Committee of South Australia is responsible for overseeing the implementation of the Information Privacy Principles Instruction by South Australian public sector agencies. The Privacy Committee reports to the relevant South Australian Minister and provides advice on privacy issues;

- in Tasmania, the Personal Information and Protection Act 2004 (Tas), administered by the Tasmanian Ombudsman. This statute covers the Tasmanian public sector including the University of Tasmania;

- in Western Australia the state public sector in Western Australia does not currently have a statutory privacy regime. Various confidentiality provisions cover government

agencies and some privacy principles are provided for in the Freedom of Information Act 1992 (WA) overseen by the Office of the Information Commissioner (WA) ;

- in the Australian Capital Territory, the Information Privacy Act 2014 (ACT) which regulates the handling of personal information by ACT public sector agencies, and the Health Records (Privacy and Access) Act 1997 which regulates the handling of health information by providers of health services in the ACT and those providers' subcontractors. The Office of the Australian Information Commissioner is currently exercising some of the functions of the ACT Information Privacy Commissioner

- in the Northern Territory, the Information Act 2002 (NT) as administered by the Information Commissioner for the Northern Territory.

Coverage of state owned corporations is inconsistent. Some State and Territory state owned corporations are not regulated under either state or federal state privacy law.

Some state laws also regulate private sector providers of health services. As noted above, New South Wales (NSW), Victoria and the Australian Capital Territory (ACT) have specific health privacy legislation that covers all health service providers (public and private sector) in those jurisdictions. This means that private sector health service providers operating in NSW, Victoria and the ACT must comply with both federal and state or territory privacy legislation when handling health information.

State and territory laws are particularly relevant in relation to deployment and use of surveillance devices, tracking devices and listening devices and monitoring conducted in public places and within workplaces.

In Queensland, Victoria and New South Wales, privacy matters may be addressed by the respective relevant State consumer and administrative appeals tribunal. As these tribunals provide a convenient and low cost or no-cost mechanism for review and redress under the relevant State privacy statutes and an increasing number of privacy complaints concern State agency health service providers or local government authorities, there is a significant and growing body of case law as to interpretation and application of those statutes. Increasingly, the determinations of these tribunals reference earlier determinations and determinations of interstate tribunals. Although these determinations are not judicial precedents, given similarities in laws under determination and the paucity of judicial decisions and published reasons for regulatory determinations under the federal Privacy Act, these State level determinations may be expected to become increasingly influential in shaping application of Australian data protection.

1.2 Other regulators

The Privacy Act is administered by the Australian Privacy Commissioner which is integrated within the Office of the Australian Information Commissioner (**OAIC**). The OAIC is responsible for enforcing compliance with the Privacy Act and reviewing proposed privacy codes.

The Australian Communications and Media Authority (**ACMA**) enforces provisions of the Spam Act, regulating sending of unsolicited commercial electronic messages (including

emails and text messages) and the Do Not Call Register Act. The ACMA also administers a number of privacy-affecting codes in the media and communications sector. Media organisations enjoy a broad exemption from the federal Privacy Act in relation to activities of journalism, subject to compliance with a media privacy code.

The Department of Home Affairs administers provision of lawful assistance to law enforcement agencies under the Telecommunications (Interception and Access) Act 1979.

The Department of Home Affairs also administers the mandatory telecommunications 'metadata' retention requirements as imposed upon Australian communications service providers.

State and territory Privacy, Information or Health Information Commissioners administer state and territory privacy statutes. These statutes apply to personal information held by respective state and territory government departments and agencies and contractors to them, and in some states and territories, to health service providers in the private (non-government) health sector as well as to public sector health service providers. In some states and territories these Commissioners also oversee the state and territory laws affecting use of surveillance devices, tracking devices and listening devices, video and audio-visual monitoring of public places and workplaces and computer and data surveillance of workplaces (including home working).

1.3 Key concepts: personal information

Collection, use, storage (retention, access and deletion) and disclosure of 'personal information' is principally regulated by the federal Privacy Act.

The definition of 'personal information' 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.

The definitions of 'personal information' under state and territory information privacy and health information laws differ, although interpretation of the relevant definitions to date has been broadly similar throughout Australia.

'Personal information' includes 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' under the federal Privacy Act means information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not. Images of individuals in photographs or video are personal information under the federal Privacy Act 1988 where the person's identity is clear or can reasonably be worked out from that image. Images of individuals may also contain sensitive information if, for example, the individual's racial or ethnic origin or religious beliefs is apparent. An APP entity may only collect images of identifiable individuals if it is reasonably

necessary for one of your organisation's functions or activities. Consent is not required to collect image of identifiable individuals unless the image records sensitive information about the individual.

Whether an individual is 'reasonably identifiable' from information will depend on considerations that include:

- the nature and amount of information;
- the circumstances of its receipt;
- who will have access to the information;
- other information either held by or available to the APP entity that holds the information;
- whether it is possible for the individual or entity that holds the information to identify the individual, using available resources (including other information available to that individual or entity). Where it may be possible to identify an individual using available resources, the practicability, including the time and cost involved, will be relevant to deciding whether an individual is 'reasonably identifiable'; and
- if the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.

Personal information is 'de-identified' if the information is no longer about an identifiable individual or an individual who is reasonably identifiable. The Australian Information Commissioner notes that de-identification includes two steps: removing personal identifiers, such as an individual's name, address, date of birth or other identifying information, and removing or altering other information that may allow an individual to be identified, for example, because of a rare characteristic of the individual, or a combination of unique or remarkable characteristics that enable identification.

De-identification can be effective in preventing re-identification of an individual, but may not remove that risk altogether. There may, for example, be a possibility that another dataset or other information could be matched with the de-identified information. The risk of re-identification must be actively assessed and managed to mitigate this risk. This should occur both before an information asset is de-identified and after disclosure of a de-identified asset.

Australian privacy regulation does not draw a distinction between 'anonymised information' and 'de-identified information'. These terms are often used interchangeably in Australia.

'Sensitive information' under the federal Privacy Act means 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;
- criminal record,

that is also personal information; and in addition:

- '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; and
- biometric templates.

'Health information' is personal information, about:

- the health or a disability (at any time) of an individual, or
- an individual's expressed wishes about the future provision of health services to him or her, or
- a health service provided, or to be provided, to an individual, or
- other personal information collected to provide, or in providing, a health service, or
- other personal information about an individual collected in connection with the donation, or intended donation, by the individual of their body parts, organs or body substances, or
- genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

Examples of health information include information about an individual's physical or mental health, notes of an individual's symptoms or diagnosis and the treatment given, records held by a fitness club about an individual, information about an individual's suitability for a job, if it reveals information about the individual's health and any other personal information (such as information about an individual's date of birth, gender, race, sexuality, religion), collected for the purpose of providing a health service.

1.4 Key concepts: acts and practices

Key concepts used in Australian privacy regulation are 'collection', 'use' and 'disclosure' of 'personal information', including 'sensitive information'. 'Data controller' and 'data processor' are key concepts in privacy regulation in many countries but not directly relevant in Australia either under federal or state and territory statutes.

Subject to jurisdictional nexus and the 'small business exception', private sector organisations and government agencies that collect, use or disclose personal information are regulated in relation to those activities. Such organisations and Federal government agencies that collect, use or disclose personal information are called 'APP entities' and must comply with the APPs.

State government agencies and in New South Wales, Victoria and the Australian Capital Territory private (non-government) health service providers that collect, use or disclose health related personal information in those states and territories must comply with the Information Privacy Principles and Health Information Privacy Principles in those statutes as well as with the federal Privacy Act: that is, the state and territory statutes and the federal Privacy Act often have concurrent operation.

An APP entity 'collects' personal information only if the entity collects the personal information for inclusion in a print or electronic record or generally available publication. Collection may be manual or automated, entered by the affected individual or otherwise collected directly from that individual or obtained from a third party: the mode of collection is not relevant other than as to a higher level of regulation which applies when collection is other than directly from the affected individual.

A number of APPs (such as APPs 6, 11, 12 and 13) apply to an APP entity that 'holds' personal information. An APP entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'. The term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. This means that one entity can physically possess personal information that another entity controls. In such situations, both entities will 'hold' the information at the same time. If each entity is covered by the Privacy Act, each will have separate responsibilities in relation to handling that information under the Privacy Act.

'Use' and 'disclosure' are key concepts in Australian privacy law: as already noted, privacy law in the European Union and many other countries use concepts of 'data controller' and 'data processor' which have no direct equivalent in Australia.

The Australian Information Commissioner's APP Guidelines (https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/) (**APP Guidelines**) include the following guidance about 'use' and 'disclosure':

- use — generally, an APP entity uses personal information when it handles and manages that information within the entity's effective control; and
- disclosure — an APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.

In practice, an important and difficult distinction is made between:

- APP entities that collect, use or disclose personal information; and
- organisations that as sub-contractors to those APP entities may handle personal information for those entities: for example, operations of data warehouses or data centres and cloud as-a-service providers.

Where personal information is entrusted by an APP entity that collects that personal information to another party for storage and processing, the Australian Information Commissioner looks to whether the second party has 'control' of that information. If the second party can fully access and edit that information, the provision of that personal information to the second party is a 'disclosure' that is subject to relevant notice and consent requirements and the second party is an entity that 'collects' this information.

However, the Australian Information Commissioner has expressed the view that in limited circumstances, an APP entity might retain such a degree of control over the information that the APP entity is considered to be 'using' that information and not disclosing the information to the second party. For example, where an APP entity provides personal information to a cloud service provider, this may be a 'use' if the information is provided for the limited purpose of performing the services of storing the information and ensuring that the entity may access the personal information stored on the entity's behalf and a binding contract between the parties:

- requires the cloud service provider only to handle the personal information for these limited purposes;
- requires any subcontractors of the cloud service provider to agree to the same obligations; and
- gives the entity effective control of how the personal information is handled by the provider. Issues which should be considered include whether the entity retains 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, what type of security measures 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 or at the end of the contract.

Whether or not other examples are considered a 'use', or a 'disclosure', will depend on the circumstances of each individual case, having regard to the degree of control held by the APP entity. Where the provision of personal information to an overseas contractor is a use, the APP entity must comply with the APPs when the entity or the contractor handles the information. Any acts or practices undertaken by the contractor on behalf of the entity will generally be treated as having been done by the entity (s 8(1) of the Privacy Act).

Subject to jurisdictional nexus and the 'small business exception', private sector organisations and government agencies that collect, use or disclose personal information are regulated in relation to those activities. At the federal level such regulated entities are 'APP entities'.

'Holding' of personal information is also relevantly regulated. An APP entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'. 'Data controller' and 'data processor' are key concepts in privacy regulation in many countries but not directly relevant under federal or state and territory statutes in Australia.

Sending of commercial electronic messages and various forms of electronic marketing and direct marketing are also regulated under other laws.

Use of surveillance devices and tracking devices is also regulated under predominately state and territory laws.

1.5 Exceptions

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

While the federal Privacy Act applies to many private and public sector organisations and agencies (entities subject to the Privacy Act are collectively referred to in the Act as **APP entities**), certain entities are excluded from the federal Privacy Act's coverage. These include small business operators, 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. Public schools and public universities in the states and territories are generally not covered by the federal Privacy Act, but may be governed by state or territory privacy laws. State and territory government agencies and state and territory owned corporations are not subject to the federal Privacy Act but may be governed by state or territory privacy laws. Private schools and universities are generally covered by the federal Privacy Act, but some are also covered by state and territory laws.

A 'small business exception' has the effect that (subject to a jurisdictional nexus test), private sector organisations are regulated where annual group global revenue (that is, including revenue of related entities) is greater than AUD3 million. However, some small business operators (organisations with an annual group global revenue of AUD3 million or less) are regulated notwithstanding this 'small business exception', including:

- private sector health services providers;
- businesses that sell or purchase personal information;
- credit reporting bodies; and
- contracted serviced providers for a Commonwealth (Federal government agency) contract.

There is a further exception relevant for corporate groups.

An act or practice by a body corporate is not an interference with privacy if that act or practice consists of disclosure of personal information by a body corporate from or to a

'related body corporate'. However, before an organisation can rely on this exemption to disclose (non-sensitive) personal information to other related companies, that organisation 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 remains 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 that information 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):

- collection and disclosure of 'sensitive information';
- collection of personal information from an entity that is exempt from the Privacy Act;
- where the body corporate is a contractor under a Commonwealth contract;
- disclosure of personal information from or to a related body corporate that is contrary to a relevant contractual provision; and
- where the disclosure is for the purpose of direct marketing.

Media organisations enjoy an exception in relation to activities of journalism, subject to compliance with a published media code of practice.

A number of uses or disclosures of personal information are specifically excepted either within relevant APPs themselves or as 'permitted general situations' as enumerated in section 16A of the federal Privacy Act. These include:

- lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety;
- taking appropriate action in relation to suspected unlawful activity or serious misconduct;
- locating a person reported as missing;
- asserting a legal or equitable claim; and
- conducting an alternative dispute resolution process

The information handling requirements imposed by APP 3 and APP 6 do not apply to an organisation if a 'permitted health situation' exists. This exception applies to a number of specific acts or practices relating to collection, use or disclosure of health information or genetic information by an organisation, such as collection, use or disclosure of health information for certain research purposes.

A number of the APPs provide an exception if an APP entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act differently. Some other provisions refer more narrowly to an act that is 'required by or under an Australian law (other than this Act)' or 'required by or under an Australian law, or a court order' (APP 11.2(d)) and do not include an act that is 'authorised'. For an APP entity to be 'required' by an Australian law or a court/tribunal order to handle information in a particular way the OAIC has expressed the view that the entity must have a legal obligation to do so such that it cannot choose to act differently. An APP entity that is 'authorised' under an Australian law or a court/tribunal order has discretion as to whether it will handle information in a particular way.

Acts and practices within Australia (including collection of personal information from individuals within Australia by organisations outside Australia, and disclosures of personal information about individuals within Australia to persons outside Australia) generally must fully comply with Australian law and are not excused by compliance with requirements of foreign laws. In relation to activities of regulated entities outside Australia and within particular jurisdictions, there is an exemption in relation to acts or practices within those jurisdictions as required by foreign law of those respective jurisdictions.

1.6 Geographical scope

Where personal information about any individual is handled (collected, used or disclosed) by an APP entity, that individual is protected by the APPs. It is not relevant whether that individual resides in Australia or is physically present in Australia or provided the personal information directly to the APP entity. Personal information of persons outside Australia that is held on servers located within Australia is regulated by the Privacy Act.

State and territory laws generally operate in relation to individuals physically present within the relevant state and territory and in some cases extend to acts and practices of entities outside the relevant state or territory in relation to personal information about individuals within the relevant state and territory.

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

The federal Privacy Act applies to an act or practice wherever done outside Australia by an 'agency' (broadly, an Australian federal government entity).

In general, corporations incorporated in Australia and Australian incorporated or constituted bodies are deemed to have an Australian link and regulated by the federal Privacy Act.

The federal Privacy 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 by the federal Privacy Act where

both (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 interpretation of these provisions by the Australian Information Commissioner is the subject of some controversy. 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 (which, when enacted, inserted the relevant provisions into the federal Privacy Act with effect from March 2014) 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 also stated that for the operation of the Privacy 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 or by 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 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.

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.

1.7 Principles, laws and precedents

Although many key provisions of privacy regulation in Australia are expressed as 'principles', these principles operate as law administered by the relevant Commissioners.

The expression in the form of 'principles' stated at a broad level of generality is unusual in Australian legislation. Provisions in federal, state and territory statutes in Australia are usually prescriptively detailed and subject to 'black letter' interpretation. The unusual, principles-based feature of Australian privacy regulation often leads to tensions as to how principles should be interpreted and applied, and as to the importance or otherwise of guidance from the relevant Commissioner concerning interpretation of relevant principles, as opposed to the usual Australian approach of a strict grammatical reading of statutes.

Difficulties in interpretation and application of principles-based law are exacerbated by paucity of decided case law. An exception is the written determinations of consumer and administrative tribunals in some states: in particular in New South Wales, Victoria and Queensland. However, these determinations do not have status as decided case precedents for courts. As a result, privacy professionals are often called upon to advise as to matters which are not the subject of any reliable guidance from courts and where only limited guidance is available from relevant Commissioners, which guidance may or may not be adopted by courts.

However, there is a useful body of quite detailed guidance published by Commissioners in some Australian jurisdictions, in particular, by the federal commissioner (the OAIC), and by the Commissioners in Queensland, New South Wales and Victoria. These Commissioners then apply their respective guidance when negotiating with regulated organisations as to regulatory outcomes which the Commissioners consider appropriate. Because outcomes are usually negotiated rather than litigated, with Commissioners using the prospect of adverse formal regulator determination or media statement as to adverse findings to negotiate an agreed fine or undertaking, the views of the relevant Commissioner as expressed in guidance are often decisive as to practical outcome and sanctions.

Enforcement activity by the federal Commissioner is also affected by enforcement guidelines. In relation to the federal Privacy Act, the federal Commissioner has published a Privacy regulatory action policy and a detailed Guide to privacy regulatory action. The federal Commissioner has also released subject matter specific guides to privacy regulatory action. For example, the Commissioner has various enforcement and investigative powers in respect of the My Health Record system, under both the My Health Records Act and the Privacy Act. The My Health Record system contains online summaries of individual's health information which can be viewed by their registered treating healthcare providers, including doctors, nurses and pharmacists across Australia. Section 111 of the My Health Records Act provides for the Information Commissioner to make enforcement guidelines. The Information Commissioner must have regard to these guidelines in exercising his or her investigative and enforcement powers in relation to the My Health Record system. The My Health Records (Information Commissioner Enforcement Powers) Guidelines 2016 addresses these powers.

The APPs are arranged in the order of the personal information lifecycle, from collection, to use, to disclosure, to retention. Both the federal APPs, and the state and territory IPPs, are not lengthy, but their interpretation can be complex. As there are substantial similarities between many of the federal APPs and corresponding state and territory IPPs, guidance issued by the federal Commissioner can often be applied at the state or territory level, and vice versa. The Australian Information Commissioner's APP Guidelines as to interpretation and operation of the APPs run to over two hundred pages, and these Guidelines are supplemented by more detailed Privacy Resources addressing particular subject matter areas. As stated by the Commissioner, "The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters we may take into account when exercising functions and powers under the Privacy Act". These Guidelines are therefore of significant interest as an expression of the Commissioner's interpretation of key provisions of the Privacy Act. The Commissioner's Guidelines and other guides are not given any legislative status. However, the Guidelines and Guides 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 Privacy Act that is given in the Parliament's Explanatory Memorandum and referenced in the Guidelines does not conform to a plain reading of these provisions on their face. Issues of interpretation are therefore likely to arise.

2 DATA PROTECTION AUTHORITIES

2.1 Relevant Authorities

Federal

The principal federal data protection authorities are:

- in the case of the Privacy Act:

  The Office of the Australian Information Commissioner

  Level 3, 175 Pitt Street

  Sydney NSW 2000

  Australia

  T: +61 2 9284 9749

  F: + +61 2 9284 9666

  W: www.oaic.gov.au

- and in the case of the Spam Act and the Do Not Call Act:

  The Australian Communications and Media Authority

  Level 5 The Bay Centre

  65 Pirrama Road, Pyrmont NSW 2009

  Australia

  T: +61 2 9334 7700

  F: +61 2 9334 7799

  W: www.acma.gov.au

Australian Capital Territory

The Information Privacy Act 2014 (ACT) regulates the handling of personal information by ACT public sector agencies.

The Office of the Australian Information Commissioner is currently exercising some of the functions of the ACT Information Privacy Commissioner. These responsibilities include handling privacy complaints against, and receiving data breach notifications from, ACT

public sector agencies, and conducting assessments of ACT public sector agencies' compliance with the Information Privacy Act.

The Health Records (Privacy and Access) Act 1997 (ACT), the Listening Devices Act 1992 (ACT) and the Workplace Privacy Act 2011 (ACT) are also relevant.

New South Wales

The NSW Information and Privacy Commission undertakes the privacy functions conferred by the Privacy and Personal Information Protection Act 1998 (NSW) and Health Records and Information Privacy Act 2002 (NSW).

The Government Information (Public Access) Act 2009, while primarily addressing routine and proactive release of government information, including information held by the providers of goods and services contracted by government agencies, also has important provisions affecting information privacy rights.

The Workplace Surveillance Act 2005 (NSW) and Surveillance Devices Act 2007 (NSW) are also relevant.

Data sharing between government agencies in NSW is regulated by the Data Sharing (Government Sector) Act 2015 (NSW).

Victoria

The Victorian Information Commissioner is an independent statutory officer established by the Privacy and Data Protection Act 2014 (Vic). This legislation covers the handling of all personal information, other than health information, as well as covering protective data security, in the public sector in Victoria.

Health information privacy is regulated by the Health Services Commissioner under the Health Records Act 2001 (Vic).

The Surveillance Devices Act 1999 (Vic) and the Surveillance Devices (Workplace Privacy) Act 2006 (Vic) is also relevant.

Data sharing between government agencies in Victoria is regulated by the Victorian Data Sharing Act 2017 (Vic).

Queensland

The Information Privacy Act 2009 (Qld) covers the Queensland public sector and is administered by the Queensland Office of the Information Commissioner.

The Public Interest Disclosure Act 2010 (Qld) and the Invasion of Privacy Act 1971 (Qld) are also relevant.

South Australia

South Australia has issued an administrative instruction requiring its government agencies to generally comply with a set of Information Privacy Principles: the SA Department of the

Premier and Cabinet Circular, PC012 – Information Privacy Principles (**IPPS**) Instruction, 16 September 2013.

The Privacy Committee of South Australia is responsible for overseeing the implementation of the Information Privacy Principles Instruction by South Australian public sector agencies. The Privacy Committee reports directly to the Minister and provides advice on privacy issues. Executive support for the Privacy Committee is provided by State Records of South Australia.

The Surveillance Devices Act 2016 (SA) is also relevant.

Data sharing between government agencies in Victoria is regulated by the Public Sector (Data Sharing) Act 2016 (SA).

Tasmania

The Tasmanian Ombudsman may receive and investigate complaints in relation to the Personal Information and Protection Act 2004 (Tas). This statute covers the Tasmanian public sector including the University of Tasmania.

The Listening Devices Act 1991 (Tas) is also relevant.

Western Australia

The state public sector in Western Australia does not currently have a statutory privacy regime. Various confidentiality provisions cover government agencies and some of the privacy principles are provided for in the Freedom of Information Act 1992 (WA) overseen by the Office of the Information Commissioner (WA).

The Surveillance Devices Act 1998 is also relevant.

Northern Territory

The Office of the Information Commissioner for the Northern Territory is the independent statutory body responsible for overseeing the privacy provisions of the Information Act 2002 (NT).

The Surveillance Devices Act 2007 (NT) is also relevant.

2.2 Powers of the OAIC

The Office of the Australian Information Commissioner (**OAIC**) is an independent statutory agency within the portfolio of the Federal Attorney General.

The OAIC's responsibilities relevantly include:

- conducting investigations;
- handling complaints;
- monitoring agency administration;

- providing advice to the public, government agencies and businesses.

The OAIC provides information and advice on privacy to individuals, businesses and agencies via an enquiries line.

Under the Privacy Act a person can make a complaint to the OAIC about handling of personal information by Australian, ACT and Norfolk Island government agencies and private sector organisations covered by the Privacy Act.

The OAIC also has the power to:

- commence a Commissioner initiated investigation into an act or practice that might breach the Privacy Act;
- conduct a privacy performance assessment of whether an entity is maintaining and handling personal information in accordance with the Privacy Act;
- request an entity to develop an enforceable code, and register codes that have been developed on the initiative of an entity, at the OAIC's request or by the Commissioner directly;
- direct a government agency to give the OAIC a privacy impact assessment about a proposed activity or function; and
- recognise external dispute resolution schemes to handle particular privacy-related complaints.

The OAIC also has a range of responsibilities under other relevant laws, including laws relating to data matching, eHealth, spent convictions and tax file numbers.

3 LEGAL BASIS FOR DATA PROCESSING

3.1 Processes and practices

APP 1 requires each APP entity to have ongoing practices and policies in place to ensure that the entity manages 'personal information' collected or held by it in an open and transparent way. The APP entity must:

- take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints;
- have a clearly expressed and up-to-date APP Privacy Policy about how it manages personal information;
- ensure that its APP Privacy Policy addresses each of the matters listed in APP 1.4;
- take reasonable steps to make its APP Privacy Policy available free of charge and in an appropriate form (usually on its website); and

- upon request, take reasonable steps to provide a person or body with a copy of its APP Privacy Policy in the particular form requested.

The federal Commissioner has emphasised in two guides the importance of readily understandable disclosure as to privacy practices and match of policies to practices: see Guide to developing an APP privacy policy and Guide to undertaking privacy impact assessments. A privacy policy will need to include details as to:

- 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).

An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information. Collection and use of personal information for some purposes is subject to a higher level of regulation: as to direct marketing, refer to APP 7, and as to use of government related identifiers, refer to APP 9.

An APP entity that collects personal information about an individual must also take reasonable steps to notify the individual, or otherwise ensure the individual is aware, of the matters listed in APP 5.2. The matters there listed include:

- the APP entity's identity and contact details;
- the fact and circumstances of collection;
- whether the collection is required or authorised by law;
- the purposes of collection;
- the consequences if personal information is not collected;
- the APP entity's usual disclosures of personal information of the kind collected by the entity;
- information about the APP entity's APP Privacy Policy; and

- whether the APP entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located.

An APP entity must provide notification before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

There is significant overlap between the matters as listed in APP 1.4 which must be addressed in an APP privacy policy and the matters listed in APP 5.2 which must be addressed in a privacy notification, generally in the form of a service specific, product specific or practice specific privacy notice. The balance between the two is sometimes resolved by specific disclosure of more unusual or particular aspects of collection, use or disclosure of personal information in the privacy notice as provided at the time of provision of a particular product or service and cross-reference in that privacy notice to disclosure of more general, business-wide aspects of handling of personal information in the APP entity's APP Privacy Policy.

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 Australian Information Commissioner has emphasised the importance of privacy management by APP entities through implementation of 'privacy by design to achieve compliance with, in particular, APP 1 (privacy policy) and APP 5 (notification obligations). This places a significant onus on APP entities to institute demonstrably reliable and verifiable practices, procedures and policies in relation to the protection of personal information handled by those entities, including through conduct of privacy impact assessments prior to introduction of significantly privacy affecting initiatives such as introduction of new products or services.

Many entities continue to focus their compliance activities upon publication of privacy statements or policies of general application, service-specific disclosures through collection notices and written privacy consents where consent is required for collection, use or disclosure of particular classes of personal information. This focus can lead to insufficient emphasis being placed upon establishment of processes and procedures which are reliable and verifiable and demonstrate full compliance with published privacy statements and service-specific collection notices and privacy consents. Entities concentrating upon statement of policy over practicalities of implementation may find conflict with increasing focus of the Australian Information Commissioner upon whether an APP entity has taken all reasonable and practical steps to implement policies and notices. Private litigants may also challenge incomplete or inconsistent implementation of stated privacy policies through exercise of rights of action that arise where an entity has engaged in misleading or deceptive conduct by failing to comply with the entity's 'holding out' as to its practices, whether in more formal and privacy specific privacy statements, collection notices or privacy consents, or more general public statements such as service descriptions and marketing collateral. Misleading or deceptive conduct is actionable under section 18 of the Australian Consumer Law (Schedule 2 to the Competition and Consumer Act 2010) through

private right of action or through enforcement action by the Australian Competition and Consumer Commission (**ACCC**).

Among other implementation challenges, an APP entity must ensure:

- where user consent is required and alleged, that the entity can demonstrate through an audit trail that user consent was in fact obtained; 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).

That is not to suggest that stated privacy policies and collection notices have become less important. To the contrary, the 2014 amendments to the Federal Privacy Act rendered its provisions more prescriptive in requirements as to the form, substance, accessibility and intelligibility of privacy policies and collection notices.

APP 1.2 imposes a distinct obligation upon an APP entity to ensure that the entity complies with the APPs and any binding registered APP code relevant to its activities. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The requirement to implement practices, procedures and systems is qualified by a 'reasonable steps' test. The reasonable steps that an APP entity should take will depend upon the relevant circumstances, that are stated by the Australian Information Commissioner (in the APP Guidelines) to include:

- the nature of the personal information held. More rigorous steps may be required as the amount and sensitivity of personal information handled by an APP entity increases;

- the possible adverse consequences for an individual if their personal information is not handled as required by the APPs;

- the nature of the APP entity. Relevant considerations include an entity's size, resources and its business model. For example, the reasonable steps expected of an entity that operates through franchises or dealerships, or gives database and network access to contractors, may differ from the reasonable steps required of a centralised entity; and

- the practicability, including time and cost involved. A 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to an APP entity. However, an entity is not excused from implementing particular practices, procedures or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

The Australian Information Commissioner in the APP Guidelines gives as examples of practices, procedures and systems that an APP entity should consider implementing:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification;
- security systems for protecting personal information from misuse, interference and loss and from unauthorised access, modification or disclosure (such as IT systems, internal access controls and audit trails);
- a commitment to conducting a Privacy Impact Assessment (**PIA**) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed;
- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries;
- procedures that give individuals the option of not identifying themselves, or using a pseudonym, when dealing with the entity in particular circumstances;
- governance mechanisms to ensure compliance with the APPs (such as designated privacy officers and regular reporting to the entity's governance body);
- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2;
- appropriate supervision of staff regularly handling personal information, and reinforcement of the entity's APP 1.2 practices, procedures and systems;
- mechanisms to ensure that agents and contractors in the service of, or acting on behalf of, the entity comply with the APPs; and
- a program of proactive review and audit of the adequacy and currency of the entity's APP Privacy Policy and of the practices, procedures and systems implemented under APP 1.2.

3.2 Collection by lawful and fair means

An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities. Examples of where a collection of personal information may be unfair (some may also be unlawful) include collecting from an electronic device which is lost or left unattended, collecting from an individual who is traumatised, in a state of shock or intoxicated, collecting in a way that disrespects cultural differences or after misrepresenting the purpose or effect of collection, or the consequences for the individual of not providing the requested information.

3.3 Collecting directly from the individual

APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless one of the following exceptions apply:

- for all APP entities, it is unreasonable or impracticable for the entity to collect personal information only from the individual;
- for Government agencies, the individual consents to the personal information being collected from someone other than the individual; and
- for Government agencies, the agency is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual.

3.4 Consent

Consent is relevant to the operation of a number of APPs. In some, consent is an exception to a general prohibition against personal information being handled in a particular way (for example, APPs 3.3(a) and 6.1(a)). In others, consent provides authority to handle personal information in a particular way (for example, APPs 7.3, 7.4 and 8.2(b)).

Consent may be express or implied. The Commissioner's APP Guidelines note that the four key elements of consent are:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current (that is, the consent may be withdrawn and has not been withdrawn) and specific to the privacy affecting activity; and
- the individual has the capacity to understand and communicate their consent.

The Commissioner states that an APP entity should generally seek express (not implied) consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have upon the affected individual.

An APP entity cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information: where consent is required, the relevant APPs clearly require a higher standard than the general requirement of transparent notification as to collection, use and disclosure of personal information. It will therefore be difficult for an entity to establish that an individual's silence can be taken as consent. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.

The federal Commissioner's APP Guidelines note that use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. The Commissioner states that "an APP

entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met":

- the opt out option was clearly and prominently presented;
- it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out;
- the individual was given information on the implications of not opting out;
- the opt out option was freely available and not bundled with other purposes;
- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual;
- the consequences of failing to opt out are not serious;
- an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier.

Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual, if they choose not to consent; and
- the seriousness of any consequences if an individual refuses to consent.

Bundled consent refers to the practice of an APP entity 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not. Bundled consents are not prohibited, but bundling of consent may undermine the necessarily voluntary nature of a consent. Also, the ACMA (as relevant enforcement agency for the Spam Act) is particularly vigorous in enforcement of its view that bundling of consent is not appropriate or reasonable in relation to consumer consent to receive unsolicited commercial electronic messages.

An individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. The information should be written in plain English, without legal or industry jargon.

The OPAIC states that an APP entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to 'all legitimate uses or disclosures' (see also, discussion of 'bundled consent' above). When seeking consent, an entity should describe the purpose to which it relates. The level of specificity required will depend on the circumstances, including the sensitivity of the personal information.

Consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely. The OAIC states that it is good practice to inform the individual of the period for which the consent will be relied on in the absence of a material change of circumstances.

An individual may withdraw their consent at any time. The OAIC states that this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information.

3.5 Capacity to consent

An individual must have the capacity to consent. This means that the individual is capable of understanding the nature of a consent decision, including the effect of giving or withholding consent, forming a view based on reasoned judgement and how to communicate a consent decision.

The OAIC states that an APP entity can ordinarily presume that an individual has the capacity to consent, unless there is something to alert it otherwise, for example, the individual is a child or young person. If an entity is uncertain as to whether an individual has capacity to consent at a particular time, the OAIC expresses the view that the APP entity should not rely on any statement of consent given by the individual at that time. An APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent, such as provision of an interpreter or use of alternative communication methods.

Issues that could affect an individual's capacity to consent include:

- age;
- physical or mental disability;
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia; or
- limited understanding of English.

Consent may also be expressed by a person who can act on behalf of the affected individual's behalf. Options include:

- a guardian;
- someone with an enduring power of attorney;
- a person recognised by other relevant laws, for example in NSW, a 'person responsible' under the Guardianship Act 1987 (NSW) may be an individual's spouse, partner, carer, family member or close friend); or
- a person who has been nominated in writing by the individual while they were capable of giving consent.

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. An APP entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.

As a general principle under Australian law, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

OAIC guidance states that if it is not practicable or reasonable for an APP entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. That OAIC guidance also states that an individual aged under 15 is presumed not to have capacity to consent.

3.6 Form of consent

Express consent is given explicitly, either orally or in writing. This might be expressed as a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

Where consent is required for compliance with the APPs, the practical issue for many APP entities will be how the APP entity can reliably and verifiably evidence that such consent was sought and obtained from an affected individual. Consent may be obtained in a variety of ways, but some of the ways of obtaining consent create significant evidentiary challenges.

3.7 Other legal grounds for data processing

Generally under Australian privacy law, a legal ground for data processing is not required. Australian privacy regulation is principally focussed upon creating transparency for affected individuals as to such acts or practices in relation to personal information about them. It does this through requirements as to appropriate notice and disclosure to affected individuals, and in some cases by specifying that consent of the affected individual is required to a particular act or practice. In each case the focus is not upon the legal grounds for data processing: instead, the focus is whether a particular act or practice for a particular purpose is a relevant collection, use or disclosure of personal information by a regulated entity and if so, as to appropriate notice and disclosure to the affected individuals.

This focus upon transparency is also reflected in requirements in the APPs for disclosure as to the purpose of collection. An APP entity can only use or disclose personal information for the particular purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies, such as where the individual has consented to the use or disclosure of the information.

One of the key questions in application of the APPs is as to 'transparency', not itself a defined term in Australian privacy laws. The Australian Consumer Law (**ACL**), forms part of

the federal Competition and Consumer Act 2010, addresses transparency of terms in consumer contracts, which in turn goes to enforceability. Section 24 of the ACL sets out the framework for determining whether a term of a consumer contract is 'unfair'. A court, under s 24(2), may take into account (a) the extent to which the term is transparent and (b) the contract as a whole. Section 24(3) states that a term will be 'transparent' if it is: expressed in reasonably plain language, legible, presented clearly and is readily available to any party affected by the term.

3.8 Codes of Conduct

The Privacy (Credit Reporting) Code 2014 (**CR Code**) is a mandatory code that binds credit providers and credit reporting bureaus. The CR code supplements the provisions contained in Part IIIA of the Privacy Act and the Privacy Regulation 2013. A breach of the CR code is a breach of the Privacy Act.

The Privacy (Market and Social Research) Code 2014 collection, retention, use and disclosure of personal information about the subjects of and participants in market and social research (so-called 'identifiable research information'). The code is mandatory for members of the Association of Market and Social Research Organisations (**AMSRO**) is the national industry body of market and social research organisations.

The Privacy Act allows for registration by the OAIC of other codes developed by industry groups which, if accepted for registration by the Commissioner, become mandatory in relation to the class of persons stated upon registration to be bound to comply with the code.

Many codes of conduct registered under other statutes and administered by other regulators have mandatory operation under those statues, including the Telecommunications Consumer Protections (TCP) Code and the Commercial Television Industry Code of Practice 2015 as overseen by the ACMA. There are also important industry codes administered by industry groups, such as the Australia Bankers Association's Revised Code of Banking Practice – 2013. Some state and territory privacy frameworks also extensively rely upon codes of practice: for example, fifteen Privacy Codes of Practice have been approved in New South Wales in relation to government agencies and health service providers by the NSW Privacy Commissioner who oversees the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records Information Privacy Act 2002 (NSW).

4 SPECIAL RULES

4.1 Employment

By section 7B(3) of the Privacy Act, an act done, or practice engaged in, by an APP entity that is a private sector organisation that is or was an employer of an individual, is exempt if the act or practice is directly related to a current or former employment relationship between the employer and the individual and an employee record held by the organisation and relating to the individual.

The Privacy Act deals with employee records relating to public sector and private sector employees differently. The handling of personal information by a private sector employer is exempt from the Privacy Act to the extent that this personal information 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 that employer handles current and past employee records and as a result is not obligated to grant access to an employee record to a current or former employee.

However, this Privacy Act exemption relates to private sector organisations only. Australian government employee records are covered by the Privacy Act.

The definition of 'employee records' is also relatively narrow and does not encompass records relating to applicants for employment or records relating to individuals that are independent contractors. Accordingly, this exemption is of limited utility for most businesses.

Other statutes are often relevant in relation to employee privacy, including general laws in relation to surveillance and tracking devices and specific laws addressing workplace surveillance and workplace relations.

4.2 Health

The federal Privacy Act regulates how all private sector health service providers handle health information. The federal Privacy Act applies to all private sector health service providers, irrespective of their annual turnover. An APP entity is considered a 'health service provider' if the entity provides a health service and holds health information, even if providing a health service is a primary activity.

Health service providers are covered by the Privacy Act for all activities involving the handling of personal information, not just activities that relate to providing a health service.

State and territory public sector providers such as public hospitals are regulated by State or Territory privacy law. Sometimes there is a mix of private and public sector providers across both private and public sector sites, such as co-located public and private hospitals. Which statute applies often depends upon the status of the entity that holds the relevant health record and interpretation of contracts which purport to extend statutory obligations to a contracted service provider.

Local health privacy laws in New South Wales, Victoria and the Australian Capital Territory also apply to the private sector. Private sector operators in these states must comply with both the Privacy Act and local state or territory law.

4.3 Finance

There are not specific data protection rules or guidance regarding the processing of financial (personal) data or applicable in the finance sector.

The Privacy Act has a separate regime to govern credit reporting. Part IIIA of the Privacy Act, the Privacy Regulation 2013 and the Privacy (Credit Reporting) Code 2014 (**CR code**)

regulate the handling of personal information about individuals' activities in relation to consumer credit. Part IIIA outlines:

- the types of personal information that credit providers can collect about an individual for the purpose of inclusion in that individual's credit report disclose to a credit reporting body (**CRB**), for the purpose of that information being included in an individual's credit report,
- what entities can handle that information;
- the purposes for which that information may be handled;
- privacy safeguards in relation to the handling of that information; and
- how an individual may access and correct credit related information held about them.

Outsourcing of material business activities of regulated financial institutions is regulated by the Australian Prudential Regulation Authority (**APRA**). In particular, APRA's Prudential Standard CPS 231 Outsourcing and Prudential Practice Guide CPG 235 – Managing Data Risk and Information Paper: Outsourcing involving shared computing services (including cloud), are often relevant in relation to handling of personal information about individuals that are customers of regulated financial institutions by third party entities, including cloud service providers, on behalf of those regulated institutions.

The Office of the Australian Information Commissioner has also published a Guide to securing personal information, which sets out a range of 'reasonable steps' that may be adopted to protect personal information in order to comply with APP 11.1. This guide notes that if an APP entity continues to 'hold' personal information when storing or using it in the cloud, reasonable steps may include robust management of the third party storing or handling of personal information entrusted to the APP entity, including effective contractual clauses, verifying security claims of cloud service providers through inspections, and regular reporting and monitoring. If an APP entity adopts cloud computing, the agency should to assess the security controls of the provider to ensure that the APP entity remains complaint with APP 11. Other APPs may also apply in these circumstances, including APP 8 (where personal information is disclosed to an overseas recipient), and APPs 12 and 13 (access and correction).

4.4 Telecommunications

The federal Telecommunications Act 1997 (**Telecommunications Act**) prohibits telecommunications carriage service providers from disclosing information (telecommunications data) about their customers' use of telecommunications services. These provisions operate concurrently with relevant restrictions and requirements of the Privacy Act.

Section 276 in Part 13 of the Telecommunications Act regulates the use or disclosure of information or a document relating to the:

- contents or substance of a communication carried, or being carried, by a carrier or carriage service provider;
- carriage services supplied or intended to be supplied by a carrier or carriage service provider; and
- affairs or personal particulars (including any unlisted telephone number or any address) of another person.

Contravention of section 276 is a criminal offence.

Information or a document protected under Part 13 relates to many forms of communications, including fixed and mobile telephone services, internet browsing, email and voice over internet telephone services. For voice communications, this would include subscriber information, call numbers of the parties involved, the time of the call and its duration. In relation to internet-based applications, the information protected under Part 13 would include the Internet Protocol (**IP**) address used for the session, destination URLs and the start and finish time of each session.

Part 13 is subject to important exceptions, including in relation to requests for lawful assistance made by law enforcement agencies and disclosure with the consent of affected individuals.

The Telecommunications (Interception and Access) Act 1979 (**TIA Act**) prohibits live interception of the interception of communications and access to stored communications on certain communications infrastructure. The TIA Act sets out certain exceptions to these prohibitions to permit eligible Australian law enforcement and security agencies to:

- obtain warrants to intercept communications;
- obtain warrants to access stored communications;
- authorise the disclosure of telecommunications data.

Agencies can only obtain warrants or give authorisations for national security or law enforcement purposes set out in the TIA Act.

The Surveillances Devices Act 2004 governs the use of surveillance devices by Australian Government agencies. Under that Act, an eligible Australian government agency can apply for a warrant to use a surveillance device to investigate a relevant offence.

The Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 (**2015 Act**) amended the TIA Act and the Telecommunications Act to require telecommunications carriage service providers that operate telecommunications infrastructure within Australia to retain and secure a specified set of data fields about communications carried over their services for a period of two years. The set of metadata required to be collected, retained and secured is defined by reference to the following six types of information: the identity of the subscriber to a communications service; the source of the communication; the destination of the communication; the date, time and duration of the communication; the type of the communication; and the location of the equipment

used in the communication. Data collected and retained by carriage service providers under the data retention regime solely for the purpose of meeting the mandatory retention requirements is deemed to be personal information and therefore subject to the Privacy Act and the APPs.

The 2015 Act departed from previous statute law by being the first mechanism to mandate a requirement of capture of relevant information about communications, and then retention of that information, on a pre-emptive and service-wide basis and not case-by-case responsive to a specific request by a law enforcement agency.

4.5 Decryption assistance

On 9 December 2018 the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 came into law, adding Part 15 to the Telecommunications Act 1997, substantially expanding the digital collection powers of Australian law enforcement and surveillance agencies, and reforming the framework through which they seek help from the communications sector.

All providers of telecommunications services within Australia, and providers of encryption products and encryption-based internet services that have one or more end users in Australia are potentially subject to the prospective operation of the new Australian encryption laws.

The fact that a provider has its head office in Australia (or elsewhere) is not relevant.

A service or product provider is subject to a legally enforceable obligation to assist decryption of communications of customers only if a technical assistance notice or a technical capability notice is issued in accordance with the new Act.

A technical assistance notice or technical capability notice must not require a provider to do any act or thing which would require a legal warrant or legal authorisation under relevant statutes. The consequence is intended to be that a technical assistance notice or technical capability notice cannot be used as an alternative to a warrant or authorisation under any relevant statute.

A technical assistance notice or technical capability notice must be reasonable, proportionate, practicable and technically feasible.

A technical assistance notice or technical capability notice must not:

- have the effect of requiring a relevant entity to implement or build a systemic weakness, or a systemic vulnerability (such as, but not only, to implement or build a new decryption capability), into a form of electronic protection (such as authentication and/or encryption),
- prevent a designated communications provider from rectifying a systemic weakness, or a systemic vulnerability, in a form of electronic protection.

References to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection include:

- any action that would render systemic methods of authentication or encryption less effective,
- any act or thing that will, or is likely to, jeopardise the security of any information held by any other person.

'Systemic vulnerability' is defined as a vulnerability that affects a whole class (particular mobile device models, carriage services, electronic services or software) of technology (rather than a single item of technology) but does not include a vulnerability that is selectively introduced, on a case-by-case basis, to one or more target technologies that are connected with a particular person.

Issue of notices are subject to relatively prescriptive and detailed thresholds and other requirements of the Act. There are significant controls and safeguards in the Act. These controls and safeguards are less than ideal, but they will operate as significant checks upon exercise by Australian agencies of powers conferred by this Act.

The provisions of the Act are not apt to legally compel a provider of a product or service to actively consult with and work with a user of a provider's product or service to break or workaround encryption.

The provisions of the Act as to confidentiality preclude a product or service provider from informing customers as to any consultation with relevant law enforcement agencies as to prospective issue of a notice, or in fulfilment of requirements of a notice. This lack of transparency was justified by the Australian Government on the basis that often the relevantly affected customer or user will be a person of interest in terms of the serious offence that is being investigated. This lack of transparency is practically problematic.

The Act has been the subject of a great deal of ill-informed criticism and less sensible and balanced criticism. The Act was rushed through without proper consultation. Many provisions were not well crafted, there is over-reach and uncertainty in scope, controls and safeguards are inadequate and there is insufficient independent oversight.

4.6 Historical, statistical and scientific research purposes

There is no broad exception from privacy regulation for collection, use or disclosure for historical, statistical and scientific research purposes. There are a few specific exclusions, including the following.

APPs 4.3 and 11.2 require the destruction or de-identification of personal information in certain circumstances. These requirements do not apply to information contained in a federal record. Retention, destruction and alteration of Commonwealth records is governed by the federal Archives Act 1983. A federal record can, as a general rule, only be destroyed or altered in accordance with s 24 of the Archives Act. The grounds on which this may be

done include pursuant to records disposal authority from the National Archives of Australia or in accordance with 'normal administrative practice.

In certain circumstances, the Privacy Act permits the handling of health information and personal information for health and medical research purposes, where it is impracticable for researchers to obtain individuals' consent. This endeavours to balance:

- the need to protect health information from unexpected uses beyond individual's healthcare; and
- the important role of health and medical research in advancing public health.

The OAIC has approved two sets of guidelines issued by the National Health and Medical Research Council. Researchers must follow these guidelines when handling health information for research purposes without individuals' consent. The guidelines also assist Human Research Ethics Committees (**HRECs**) in deciding whether to approve research applications. The guidelines are legally binding pursuant to sections 95 and 95A of the Privacy Act. The guidelines are:

- Guidelines under Section 95 of the Privacy Act 1988, which set out procedures that HRECs and researchers must follow when personal information is disclosed from a Commonwealth agency for medical research purposes.
- Guidelines under Section 95A of the Privacy Act 1988, which provide a framework for HRECs to assess proposals to handle health information held by organisations for health research (without individuals' consent). They ensure that the public interest in the research activities substantially outweighs the public interest in the protection of privacy.

State and territory public health sector providers such as public hospitals are regulated by State or Territory privacy law. Local health privacy laws in New South Wales, Victoria and the Australian Capital Territory also apply to the private sector. Private sector operators in these states must comply with both the Privacy Act and local state or territory law.

4.7 Children

There is no Australian equivalent to the U.S. federal Children's Online Privacy Protection Act and no other national law prescribing a minimum age at which individuals can make their own privacy decisions. For consent to be valid, an individual must have capacity to consent. Where consent is required for an organisation or agency to handle the personal information of an individual under the age of 18, the organisation or agency will need to determine on a case-by-case basis whether that individual 18 has the capacity to consent.

The OAIC's APP Guidelines state:

> As a general principle [of Australian law], an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person, for example, if the child is young or lacks the maturity or understanding to do so themselves.

> If it is not practicable or reasonable for an organisation or agency to assess the capacity of individuals under the age of 18 on a case-by-case basis, they may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.'

The My Health Record system allows young people (under the age of 18) to have a My Health Record. A My Health Record is an online summary of an individual's health information, such as medicines the individual is taking, any allergies she or he may have and treatments received. Your My Health Record allows your doctors, hospitals and other healthcare providers (such as physiotherapists) to view this health information in accordance with the individual's access controls.

A person with parental responsibility for a person under 18 may register for a My Health Record on their behalf. A child may take control of their My Health Record when they turn 14. From this age an individual may register for a record or take control of their existing record. If they choose to manage their own record, they can decide whether to allow their parent or legal guardian to also access as a nominated representative.

4.8 Email, internet and video monitoring

The use of video monitoring in Australia is regulated both at the federal and state level but does not require separate registration or notification to, or prior approval from, the relevant data protection authority. Regulation is generally by way of requirements for notice to individuals subject to surveillance and, in some cases (notably, workplace surveillance), their consent.

The federal Privacy Act does not require an entity to register, notify or seek the prior approval of the Australian Information Commissioner in relation to the use of video monitoring. Similarly, state surveillance legislation does not require an organisation to register, notify or seek the approval of state data protection authorities.

The use of video monitoring by employer entities is regulated primarily on a State and Territory basis by a mixture of workplace-specific and general surveillance legislation. See, for example, the Workplace Surveillance Act 2005 (NSW), which regulates an employer's use of workplace surveillance in the State of New South Wales, the Surveillance Devices Act 1999 (Vic), which governs the use of surveillance devices in general, and the Surveillance Devices (Workplace Privacy) Act 2006 (Vic).

Generally, employers may not engage in workplace surveillance without first providing notice to the affected employees. To the extent that such surveillance involves the collection of personal information for inclusion in a record, APP 5 of the federal Privacy Act would also require an entity to take reasonable steps to ensure that the employees were made aware of certain mandatory information, such as the purpose for which the information is collected.

Australian entities typically meet the notification requirements by providing prospective employees with notice through workplace agreements and associated policy documents.

Under the Workplace Surveillance Act 2005 (NSW), entities may provide notice by way of an email to the employee. Entities must also, however, place surveillance notices at each entrance to a workplace in which surveillance by camera occurs. The Workplace Surveillance Act 2005 (NSW) and the Workplace Privacy Act 2011 (ACT) prohibits the surveillance by employers of their employees at work except where employees have been given notice or where the employer has obtained covert surveillance authority from a magistrate. These Acts regulate the surveillance of employees by way of camera, computer and tracking surveillance. Workplace monitoring by way of 'computer surveillance' (surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, the sending and receipt of emails), requires:

- 14 days' prior (advance) notice to employees; and
- notice to each prospective employee before the prospective employee commences employment.

Computer surveillance clearly would include surveillance of workplace emails and instant messages.

The notice must indicate:

- the kind of surveillance to be carried out (camera, computer or tracking);
- how the surveillance will be carried out;
- when the surveillance will start;
- whether the surveillance will be continuous or intermittent;
- whether the surveillance will be for a specified limited period or ongoing;
- in the ACT, the purpose for which the employer may use and disclose the surveillance records; and
- in the ACT, that the employee may consult with the employer about the conduct of the surveillance.

In addition, computer surveillance of an employee must not be carried out unless:

- the surveillance is carried out in accordance with a policy of the employer on computer surveillance of employees at work; and
- the employee has been notified in advance of that policy in such a way that it is reasonable to assume that the employee is aware of and understands the policy.

The position in relation to monitoring of inbound emails or instant messaging sent from third party senders to employees is much less clear: some State statutes appear to require two party (sender and recipient) consent, others (Victoria, Queensland and the ACT) allow one party to consent (sometimes referred to as a 'participant monitoring exception').

The Surveillance Devices Act 1999 (Vic) regulates the use of listening, optical, tracking and data surveillance devices generally (whether used in a workplace or otherwise). Relevantly, the Act prohibits the installation, use or maintenance of optical surveillance devices to observe private activities without the express or implied consent of the individuals concerned.

Other State and Territory laws regulating use of tracking devices and surveillance devices, including listening devices and optical surveillance devices, take a variety of inconsistent forms. Particular care needs to be taken in this area given the absence of national standards, inconsistency in enforcement stances of State and Territory authorities, and criminal penalties for contravention.

4.9 Direct marketing and cookies

Electronic marketing is partly regulated through subject matter-specific federal laws such as the Spam Act 2003, which governs most forms of electronic marketing, and the Do Not Call Register Act 2006, which regulates unsolicited telemarketing calls.

The Spam Act prohibits 'unsolicited commercial electronic messages' with an 'Australian link' from being sent or caused to be sent. Commercial electronic messages may only be sent with an individual's consent (express or implied in the circumstances), and the message contains accurate sender identification and a functional unsubscribe facility. 'Commercial electronic messages' relevantly include unsolicited emails, SMS and MMS, where promotion of goods or services is one purpose of the electronic communication. It is unclear whether unsolicited promotional postings to social media pages may be 'messages' that are regulated as 'spam'.

Voice calls, including synthetic or recorded calls (such as robocalls), are separately regulated under a 'do not call' regulatory framework established under the Do Not Call Register Act 2006 and associated legislation and instruments, including the Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007.

APP 7 of the federal Privacy Act also regulates use or disclosure of personal information for the purpose of direct marketing activities above. If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing. There are exceptions to this prohibition. Generally, organisations may use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or the individual has a reasonable expectation that their personal information will be used for this purpose, and the organisation meets a number of conditions relating to provision of a convenient opt-out mechanism.

Although the drafting of APP 7.8 is not clear, it appears to be the legislature's intention that where those Acts impose particular prohibitions, restrictions or requirements, these will apply and, to the extent of any inconsistency, APP 7 will not apply. It also appears to be the legislature's intention that APP 7 may also operate in relation to unsolicited commercial electronic messages and telemarketing to the extent that APP 7 is not inconsistent with other relevant Acts. It follows that each of the Acts referred to above must be considered

and applied in relation to any prospective direct marketing activity involving commercial electronic messaging or outbound voice telemarketing.

The Privacy Act contains no cookie or technology-specific rules. To the extent that the use of cookies involves the collection, use or disclosure or transfer of personal information, the APPs will apply. The concept of 'collection' of personal information applies broadly, and includes information associated with web browsing, such as personal information collected by cookies. Collection of personal information using cookies could occur provided that the notice and consent requirements were followed, although any responsive electronic communication would likely be regulated as requiring prior consent either as direct marketing under APP 7 or spam (depending upon the nature of that responsive communication).

Analytical information collected from cookies (e.g., the number of times a page was visited) will not be personal information under the Privacy Act unless an individual is reasonably identifiable.

Voluntary and self-regulatory guidance in the form of the Australian Best Practice Guideline for Third Party Online Behavioural Advertising (**OBA**) (**OBA Guideline**) (available at www.youronlinechoices.com.au) is generally observed as best practice with respect to the collection and use of data for the purpose of third party OBA. The Guideline recommends that online service providers engaging in third party OBA should obtain express consent from web users in relation to their collection and use of OBA data.

4.10 Data analytics

The federal Privacy Act does not preclude the use or disclosure of personal information in connection with big data and analytics. The Act is not prescriptive as to the due diligence that is required in these circumstances. Rather, the standard principles with respect to notification of collection (APP 5) and secondary purpose use and disclosure (APP 6) will apply to the use or disclosure of personal information for these purposes.

Entities proposing to use or disclose personal information for big data and analytics would also be subject to the requirements to take reasonable steps to ensure that they protect the information from (among other things) misuse, unauthorised modification and disclosure. Reasonable steps in this context may require an organisation to undertake due diligence to ensure that big data and analytics providers maintain sufficient technical and operational safeguards to protect personal information.

Effective de-identification of personal information, so that no individual is reasonably identifiable either from the information itself or other information available to that person, has the effect that the information ceases to be regulated as personal information. Many data analytic applications may be undertaken utilising de-identified information. The OAIC will consider whether de-identification has been effective to mitigate re-identification risk 'in the round', that is, having regard to relevant facts and circumstances including limitations upon any subsequent use or disclosure of the deidentified information and any technical, operational and contractual safeguards against re-identification.

This area of regulation is rapidly developing. Care should be taken to review and follow guidance as and when issued by the Australian Information Commissioner.

4.11 Mobile apps

There are no specific rules or guidance regarding the processing of personal data in connection with mobile apps.

The OAIC has developed a guide, Mobile privacy: A better practice guide for mobile app developers, to help mobile device application (**app**) developers embed better privacy practices in their products and services and help developers that are operating in the Australian market to comply with Australian privacy law and best practice.

5 DATA QUALITY REQUIREMENTS

An APP entity must take reasonable steps to ensure that the personal information it collects is accurate, up-to-date and complete (APP 10.1).

An APP entity must also take reasonable steps to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2). It is implicit that this requirement only applies to personal information 'held' by an entity.

The requirements in APP 10 to take reasonable steps to ensure the quality of personal information are complemented by other requirements in APP 3 (collection of solicited personal information), APP 11 (security of personal information), APP 12 (access to personal information) and APP 13 (correction of personal information).

6 OUTSOURCING AND DUE DILIGENCE

6.1 Outsourcing

There are no specific rules with regard to the outsourcing of data processing to third parties (within the jurisdiction) in Australian data protection law.

Outsourcing of material business activities of regulated financial institutions is regulated by the APRA. APRA's Prudential Standard CPS 231 Outsourcing, Prudential Practice Guide CPG 235 – Managing Data Risk and Information Paper: Outsourcing involving shared computing services (including cloud) are often relevant in relation to handling of personal information about individuals that are customers of regulated financial institutions by third party entities, including cloud service providers, on behalf of those regulated institutions.

6.2 Due diligence

The sale of businesses in Australia, whether in the form of an asset sale or share sale, will generally enliven the application of Australian privacy law. Specifically, the sale of a business may involve the disclosure and collection of different types of personal information during both a due diligence process and on sale completion, including:

- employee information;

- customer information; and
- business associates' information.

APP entities that are subject to the federal Privacy Act must comply with the APPs when handling personal information in the course of due diligence and completion processes.

If the personal information is 'sensitive information' (such as health information), the handling of such information will attract additional restrictions under the APPs.

The restrictions set out in the credit reporting provisions of Part IIIA of the federal Privacy Act will also apply to the extent that the target collects and handles consumer or commercial credit information about individuals.

The federal Privacy Act currently exempts most businesses from the requirements of the Act if they have an annual turnover of less than $3 million (commonly called the "small business exemption"). Accordingly, vendors and purchasers that fall below this threshold do not need to comply with the Privacy Act when disclosing or collecting personal information during sale processes. However, the small business exemption will not apply where the relevant business:

- is related to a body corporate that is not a small business; or
- provides a health service and handles health information; or
- is a credit reporting body ; or
- trades in personal information (including by way of selling its customer database).

In summary, APP 6 provides that an APP entity that holds personal information about an individual can only use or disclose the information for a particular purpose for which it was collected (known as the 'primary purpose' of collection), unless an exception applies. Where an exception applies, the entity may use or disclose personal information for another purpose (known as the 'secondary purpose').

Exceptions to the general rule under APP 6 include where the:

- use or disclosure is related to the primary purpose for collection, and the individual would reasonably expect the entity to use or disclose the information for the secondary purpose (hereafter, the 'related purpose' exception); and
- relevant individuals have consented to the secondary purpose use or disclosure.

The OAIC has stated that, in most cases, the vendor's disclosure of personal information to prospective purchasers would be permitted under the related purpose exception on the basis that the disclosure is directly related to the primary purpose of collecting the information and within the individual's reasonable expectations as a matter of standard business practice.

7 SECURITY OF DATA PROCESSING

7.1 Confidentiality

The obligation upon APP entities to maintain confidentiality of personal information arises through operation of APP 11, which requires an APP entity to take active measures to ensure the security of personal information it holds and to actively consider whether it is permitted to retain personal information. APP 11.1 provides that an APP entity that holds personal information must take reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure (APP 11.1).

Accordingly, confidentiality must be construed having regard to the notified purpose of collection, disclosure and use of personal information, including disclosures as to specific entities or classes of entities to whom personal information may be disclosed.

It therefore follows that where an APP entity fails to take reasonable steps to protect personal information it holds from unauthorised access or disclosure and a data breach occurs which is attributable to that failure to take reasonable steps, the APP entity will be in breach of APP 11.

7.2 Security requirements

The federal Privacy Act does not require APP entities to adopt particular data security standards. Rather, the Act (through APP 11) imposes a general obligation upon APP entities to take such steps as are reasonable in the circumstances to protect personal information that the APP entity holds from misuse, interference and loss, and from unauthorised access, modification or disclosure.

An APP entity holds personal information 'if the entity has possession or control of a record that contains the personal information' (s 6(1)). OAIC guidance states that the term 'holds' extends beyond physical possession of a record to include a record that an APP entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, holds that personal information.

Accordingly, each APP entity should determine what reasonable data security standards it must adopt to protect personal information given the circumstances of the particular act or practice. Such an exercise will include consideration of a range of factors, including the amount and sensitivity of the personal information concerned and the practicability and cost of the security measures contemplated.

Reasonable steps might include any of taking steps and implementing strategies to manage governance, ICT security, data breaches, physical security, personnel security and training, workplace policies, the information life cycle, standards and regular monitoring and review.

The Office of the Australian Information Commissioner has published a Guide to securing personal information which sets out a range of 'reasonable steps' that may be adopted to protect personal information.

7.3 Cyber-security

The OAIC notes that assessment of cybersecurity should be context specific and suggests that there are no general standards that can be applied to determine whether an APP entity has taken reasonable steps to protect personal information. Compliance with a standard is one way such that an APP entity may gain some confidence regarding its security practices, but complying with a standard does not of itself mean that the entity has taken reasonable steps to protect personal information. Compliance with a standard may be a reasonable step, but it may need to take further action to meet obligations under APP 11.

Entities should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any of these that are particular to their sector or industry (for example the National eHealth Security and Access Framework, which is relevant to the health sector). Australian Government agencies must apply the Attorney-General's Department's Protective Security Policy Framework and the Australian Signals Directorate's Australian Government Information Security Manual. These documents articulate the Australian Government's requirements for protective security, and standardise information security practices across government. They may also be used by other government agencies (including state and territory agencies) and the private sector as a model for better security practice.

The OAIC also refers to the ISO/IEC 27000 series of information security management standards and the ISO/IEC 31000 of risk management standards published by both the International Organization for Standardization and the International Electrotechnical Commission, parts of which have been adopted by Standards Australia. The 27000 series of standards provide recommendations on information security management, risks and controls. The 31000 series relates to standards for the design, implementation and maintenance of risk management processes. Compliance with standards can be tested internally or certified by a third party.

8 DATA BREACH NOTIFICATION

A Notifiable Data Breach (NDB) scheme was introduced into the federal Privacy Act from 22 February 2018.

The NDB scheme requires organisations covered by the Privacy Act to notify any individuals likely to be at risk of serious harm by a data breach. This notice must take a prescribed form and must include recommendations about the steps that individuals should take in response to the data breach. The OAIC must also be notified.

An 'eligible data breach' arises when the following three criteria are satisfied:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds, and
- this is likely to result in serious harm to one or more individuals to whom the information relates, and

- the entity has not been able to prevent the likely risk of serious harm with remedial action.

Under the NDB scheme, if personal information is lost in circumstances where subsequent unauthorised access to or disclosure of the information is unlikely, there is no eligible data breach. For example, if the personal information is remotely deleted before an unauthorised person could access the information, or if the information is encrypted to a high standard making unauthorised access or disclosure unlikely, then there is no eligible data breach.

'Serious harm' is not defined in the Privacy Act. In the context of a data breach, serious harm to an individual may include serious physical, psychological, emotional, financial, or reputational harm. Examples may include:

- identity theft,
- significant financial loss by the individual,
- threats to an individual's physical safety,
- loss of business or employment opportunities,
- humiliation, damage to reputation or relationships,
- workplace or social bullying or marginalisation.

The likelihood of a particular harm occurring, as well as the anticipated consequences for individuals whose personal information is involved in the data breach if the harm materialises, are relevant considerations.

9 INTERNATIONAL DATA TRANSFERS

9.1 Applicable rules

Generally, the federal Privacy Act does not prevent an APP entity from storing or processing personal information outside Australia, either by itself or through a third party service provider. The disclosure or transfer of personal information out of Australia does not require registration, notification or prior approval from the OAIC. The APP entity must comply with the APPs in sending personal information to an overseas cloud service provider or pursuant to any other overseas outsourcing arrangement.

APP 8 regulates the cross-border disclosure of personal information to recipients outside of Australia. Before disclosing personal information to an overseas recipient, APP 8.1 requires an APP entity to 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 disclosing entity (s 16C). This is commonly referred to as the 'accountability principle'. Generally, the accountability principle will apply where APP 8.1 applies to the disclosure, 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 (and therefore to the operation of the accountability principle in s 16C). For example, APP 8.1 will not apply where:

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

An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by a privacy or data protection law that applies in the jurisdiction of the recipient;
- required to comply with another law that imposes obligations in relation to the handling of personal information (such as some taxation laws which expressly authorise and prohibit specified uses and disclosures and include a right of access to an individual's personal information;
- subject to an industry scheme or privacy code that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code; or
- subject to Binding Corporate Rules (**BCRs**).

An overseas transfer of personal information to an overseas recipient may not be a 'disclosure' if the personal information at all times remains under the effective control of the APP entity. The OAIC has drawn a distinction between limited and controlled access to information by an overseas recipient under conditions prescribed by the APP entity, which may in appropriate circumstances be a 'use' by the APP entity rather than a 'disclosure' to an overseas entity. This distinction will be important in relation to many outsourcing and offshoring arrangements, including cloud service or 'as-a-service' offerings.

This area of regulation is developing and care should be taken to check and follow recent OAIC guidance. See in particular OAIC APP Guidelines chapter 8 and Privacy business resource 8: Sending personal information overseas.

Note that some categories of personal information are subject to special or additional rules. Part IIIA of the Privacy Act regulates credit reporting and includes some restrictions on sending information held in the Australian credit reporting system overseas. The legislative framework for the Australian Government's My Health Record system prevents certain My Health Record operators and service providers from holding, taking, processing or handling

records held for My Health Record purposes outside Australia, and from causing or permitting anyone else to do so. Some State and Territory health privacy acts limit transfer of health information out of the relevant State or Territory.

9.2 Data transfer agreements

Typically, Australian businesses will seek to satisfy the requirement of APP 8.1 by entering into an enforceable contractual arrangement with the overseas recipient (and any subcontractors) to handle the personal information in accordance with the APPs.

The OAIC has stated that it is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1), and further that it will take active steps to ensure compliance with those contractual arrangements.

No particular form of contract is prescribed or recommended by the OAIC. The OAIC guidance states that contractual arrangements may include:

- the types of personal information to be disclosed and the purpose of disclosure;
- a requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the personal information (for example, a subcontractor);
- the complaint handling process for privacy complaints; and
- a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP entity where there are reasonable grounds to suspect a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract).

The 'reasonable steps' test under APP 8.1 may also require an entity to take additional and more rigorous steps depending on the nature of the disclosure and, for example, the sensitivity of the information concerned. Such steps may include the imposition of audit rights to monitor the recipients' compliance with the terms of the contract and, by extension the APPs, in relation to the information.

9.3 Binding corporate rules (BCRs)

BCRs have no formal status in Australian privacy regulation.

An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity reasonably believes that the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information. The OAIC has provided guidance to the effect that where BCRs form a stringent, intra-corporate

global privacy policy that satisfies EU standards, and mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (as required by APP 8.2(a)), BCRs may fall within the relevant exception to APP 8.1.

9.4 Safe harbour

There are no pre-approved safe harbour destinations for data transfers (disclosures).

As stated above, an APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity reasonably believes that there are laws, or binding scheme, that have the effect of protecting the information in a way that is substantially similar to the way the APPs protect the information, and mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (APP 8.2(a)).

The OAIC has provided guidance noting that whether there is substantial similarity is a question of fact and that factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme includes a comparable definition of personal information that would apply to the personal information disclosed to the recipient;
- the law or scheme regulates the collection of personal information in a comparable way;
- the law or scheme requires the recipient to notify individuals about the collection of their personal information;
- the law or scheme requires the recipient to only use or disclose the personal information for authorised purposes;
- the law or scheme includes comparable data quality and data security standards;
- the law or scheme includes a right to access and seek correction of personal information.

As to whether mechanisms can be accessed by the individual to enforce that protection of the law, the OAIC states that an enforcement mechanism should meet two key requirements: it should be accessible to the individual and it should have effective powers to enforce the privacy or data protections in the law or binding scheme. A range of mechanisms may satisfy those requirements, from a regulatory body similar to the OAIC, to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers.

9.5 Other legal bases

An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the APP entity expressly informs the individual that if they consent to the disclosure, APP 8.1 will not apply; and
- the individual then consents to the disclosure (APP 8.2(b)).

The OAIC has issued guidance that an APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent. At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs, the entity will not be accountable under the Privacy Act and the individual will not be able to seek redress under the Privacy Act.

10 OTHER MATTERS

10.1 E-discovery and law enforcement requests

An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is 'required or authorised by or under an Australian law or a court/tribunal order' (APP 8.2(c)).

However, an APP entity cannot rely upon such a requirement or authorisation to authorise a disclosure made by it in an overseas jurisdiction.

The cross-border principle will not apply if a permitted general situation exists for that disclosure (APP 8.2(d)). Section 16A of the Privacy Act lists five permitted general situations that may exist for a cross border disclosure.

10.2 Representative

There are no specific requirements to appoint an in-country representative in Australia.

However, it would usually be difficult for an APP entity to discharge access and correction obligations to individuals without a contact point within Australia.

10.3 Data Protection Impact Assessments, Audits and Seals

APP 1 requires APP entities to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. In this way, the APPs require 'privacy by design', an approach whereby privacy compliance is designed into projects dealing with personal information right from the start, rather than being bolted on afterwards.

Privacy impact assessments (**PIAs**) do not confer any protection under Australian privacy laws, but PIAs are commonly used as a means to assure privacy compliance. A number of privacy regulators have published guidance, including the OAIC Guide to undertaking privacy impact assessments and the Information and Privacy Commission NSW's Guidance: Guide to Privacy Impact Assessments in NSW.

Some Australian statutes have included requirements for particular implementations, such as MyHealth Record, to be the subject of PIAs. It is also not uncommon for major government contracts which involve outside entities handling personal information entrusted to government agencies to subject their handling of that personal information to a PIA.

There are no audit or seal formalities.

10.4 Registrations

There are no authorisation or registration obligations generally under Australian privacy laws, nor general requirements to record provision of access to personal information.

10.5 Data Protection Officer

The federal Privacy Act and State or Territory privacy acts do not expressly require an APP entity to appoint a privacy/data protection officer.

However, APP 1 requires an entity to implement practices, procedures and systems that will ensure its compliance with the Privacy Act and enable it to deal with inquiries or complaints. The appointment of a data protection or privacy officer may be one of many steps an entity can take to meet this obligation.

An APP Privacy Policy must explain the procedure an individual can follow to gain access to or seek correction of personal information the APP entity holds (APP 1.4(d)). At a minimum, the policy should state:

- that individuals have a right to request access to their personal information and to request its correction (APPs 12 and 13); and
- the position title, telephone number, postal address and email address of a contact person for requests to access and correct personal information. An APP entity could establish a generic telephone number and email address that will not change with staff movements (for example privacy@agency.gov.au).

The OAIC recommends consideration of governance mechanisms to ensure compliance with the APPs, such as designated privacy officers and regular reporting to the entity's governance body. Appointment of a data protection or privacy officer may assist an APP entity to meet its obligation to implement practices, procedures and systems that will enable it to deal with inquiries or complaints about its compliance with the Privacy Act.

Data protection or privacy officers are typically responsible for overseeing implementation of an APP entity's privacy compliance strategy, including verifying that processes and practices conform with stated policy and statutory requirements.

Activities may include designing and facilitating staff privacy training, data flow mapping, either commissioning or undertaking privacy impact assessments, consulting with information security teams as to steps to protect information security, developing both external and internal-facing privacy policies and dealing with complaints regarding the entity's handling of personal information.

A data protection or privacy officer may also perform whistle-blower notification responsibilities.

11 INFORMATION OBLIGATIONS

APP 1 requires each APP entity to have ongoing practices and policies in place to ensure that the entity manages 'personal information' collected or held by it in an open and transparent way.

An APP entity must provide notification as to collection of personal information by it, the purposes of collection, and the other matters prescribed in APP 5.2, before, or at the time it collects personal information. If this is not practicable, notification should be provided as soon as practicable after collection.

More specifically, an APP entity that collects personal information about an individual must take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters listed in APP 5.2, or to otherwise ensure that the individual is aware of any such matters.

There is significant overlap between the matters as listed in APP 1.4 which must be addressed in an APP privacy policy and the matters listed in APP 5.2 which must be addressed in a privacy collection notification, generally in the form of a service specific, product specific or practice specific privacy notice. The balance between the two is sometimes resolved by specific disclosure of more unusual or particular aspects of collection, use or disclosure of personal information in the privacy notice as provided at the time of provision of a particular product or service and cross-reference in that privacy notice to disclosure of more general, business-wide aspects of handling of personal information in the APP entity's APP Privacy Policy.

Each APP entity that collects, uses or discloses personal information about individuals, including certain 'holding' of personal information, regardless of whether that personal information is collected directly from affected individuals or disclosed to the APP entity by another person or organisation.

The information must be made conveniently available to the affected individual.

The matters listed in APP 1.4 must be addressed in an APP privacy policy and the matters listed in APP 5.2 must be addressed in a privacy notification.

There are no relevant exceptions specific to:

- the requirements to publish an APP privacy policy and to provide privacy notifications; or
- as to the matters listed in APP 1.4 that must be addressed in an APP privacy policy and as to the matters listed in APP 5.2 that must be addressed in a privacy notification.

However, the collection notification requirement is itself qualified. An APP entity that collects personal information about an individual is required to take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters listed in APP 5.2

as are reasonable in the circumstances, or to otherwise ensure that the individual is aware of any such matters.

OAIC guidance states that the reasonable steps for an APP entity will depend upon circumstances that include:

- the sensitivity of the personal information collected. More rigorous steps may be required when collecting 'sensitive information;
- the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases;
- any special needs of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the notice;
- the practicability, including time and cost involved. However, an entity is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

A privacy notification in accordance with APP 5 must be given to the affected individual at or before the time of collection (whether directly from the individual or in any other way) or, if that is not practicable, as soon as practicable thereafter.

A privacy collection notification may be through a variety of formats, provided the matters required to be addressed are expressed clearly. A notice may also be provided in layers, from a full explanation to a brief refresher as individuals become more familiar with how the APP entity operates and how personal information is handled.

12 RIGHTS OF INDIVIDUALS

An individual is conferred rights by the Privacy Act, exercisable in relation to acts and practices of APP entities, to:

- know who is collecting, using or disclosing personal information about them
- why personal information is being collected and how it will be used or disclosed and who it will be disclosed to;
- have the option of not identifying herself or himself or of using a pseudonym, in certain circumstances;
- ask for access to personal information about herself or himself (including your health information);
- stop receiving unwanted direct marketing;

- ask for access to personal information that an APP entity holds about them and for any personal information that is incorrect to be corrected;
- make a complaint about an APP entity, if the individual considers that they have mishandled personal information about them.

An individual has the right to lodge a complaint with the OAIC for alleged breaches of the federal Privacy Act. Generally, the complainant must first register a complaint with the APP entity to which the complaint relates. If dissatisfied with the response, a complainant can complain to the OAIC or to an external dispute resolution scheme of which the APP entity is a member (if applicable). In conducting its investigations, the Commissioner may require the production of documents and information, and compel people to appear and answer questions.

There is no general right for an individual to object to collection, use or disclosure of personal information about that individual. The federal Privacy Act generally requires notice to individuals as to these activities and consent in relation to particular activities, notably including notice from which consent may be reliably proven and reasonably inferred as to collection, use or disclosure of sensitive information and use and disclosure of personal information for the purpose of direct marketing.

Nor is there a general 'right to be forgotten'. However, there is a limited indirect right to insist upon deletion or de-identification of personal information that an APP entity holds about an individual. Pursuant to APP 11.2, if an APP entity holds personal information about an individual, and the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity and the information is not required by law or a court/tribunal order to be retained, the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

APP 2 provides that individuals must have the option of dealing anonymously or under a pseudonym with an APP entity. However, an APP entity is not required to provide those options where:

- the entity is required or authorised by law or a court or tribunal order to deal with identified individuals; or
- it is impracticable for the entity to deal with individuals who have not identified themselves.

Anonymity means that an individual dealing with an APP entity cannot be identified and the entity does not collect personal information or identifiers. A pseudonym is a name, term or descriptor that is different to an individual's actual name. Where applicable, an APP entity must ensure that individuals are made aware of their opportunity to deal anonymously or by pseudonym with the entity.

If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

There are exceptions to this prohibition. Generally, organisations may use or disclose personal information for direct marketing purposes where the individual has either consented to their personal information being used for direct marketing, or the individual has a reasonable expectation that their personal information will be used for this purpose, and the organisation meets a number of conditions relating to provision of a convenient opt-out mechanism.

The Spam Act 2003, the Do Not Call Register Act 2006, and state and territory information privacy acts, also confer important privacy rights.

An individual who is conferred rights by the Privacy Act may either exercise those rights in their own capacity or through a legal personal representative such as a parent or guardian or a person acting under a power of attorney or other legal authority conferred by the individual.

An APP entity that holds personal information about an individual must, on request, give that individual access to the information (APP 12.1).

APP 13.1 provides that an APP entity must take reasonable steps to correct personal information it holds, to ensure it is accurate, up-to-date, complete, relevant and not misleading, having regard to the purpose for which it is held.

APP 13.1 requires an APP entity to take reasonable steps to correct personal information it holds, in two circumstances: on its own initiative, and at the request of the individual to whom the personal information relates.

Upon receiving a request an entity must decide if it is satisfied that the information is incorrect, and if so, take reasonable steps to correct it.

There are a number of exceptions to the obligation for organisations to provide an individual access to their personal information, including 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; or
- giving access would have an unreasonable impact on the privacy of other individuals.

APP 12 also sets out minimum access requirements, including the time period for responding to an access request, how access is to be given, and that a written notice, including the reasons for the refusal, must be given to the individual if access is refused.

For example, an APP entity must respond to a request for access to the personal information if the entity is a government 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.

Neither APP 12 nor APP 13 stipulate formal requirements that an individual must follow to make an access request or correction request, or require that a request be made in writing, or require the individual to state that the request is an APP 12 or an APP13 request.

However, an APP entity must be satisfied that a request is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. If an entity gives access to the personal

information of another person, this could constitute a disclosure, which may not comply with APP 6.

An APP entity must give access to personal information in the manner requested by the individual, if it is reasonable and practicable to do so (APP 12.4(b)). The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record. Access may be by provision of redacted copy or summary where this is reasonable.

A government agency cannot impose upon an individual any charge for providing access to personal information under APP 12 (APP 12.7).

An organisation cannot impose upon an individual a charge for the making of the request to access personal information. An organisation may, however, impose a charge for giving access to requested personal information, provided the charge is not excessive (APP 12.8). OAIC guidance states that charges must be cost reflective and may include:

- staff costs in searching for, locating and retrieving the requested personal information, and deciding which personal information to provide to the individual;
- staff costs in reproducing and sending the personal information;
- costs of postage or materials involved in giving access; and
- costs associated with using an agreed intermediary.

13 ENFORCEMENT AND SANCTIONS

13.1 Enforcement action

Before the 2014 amendments to the Federal Privacy Act the OAIC had seldom exercised the power to make determinations as to an alleged breach of privacy. However, in the period 2014-2015, the OAIC made six privacy related determinations, and thereafter an upward trend in formal enforcement activity has continued. That noted, in most cases the Commissioner seeks to conciliate complaints between the relevant parties. An apology to the complainant is the most common remedy achieved through conciliation, followed by compensation, usually less than AU$100,000. The Commissioner has also sought for the respondents to amend information handling procedures and to train staff in accordance with the revised procedures.

Since March 2014 the Commissioner has significant new enforcement powers, including the power to:

- seek civil penalties against an organisation for serious or repeated interferences with the privacy of an individual (with penalties of up to AU$1.8 million for corporations); and
- accept enforceable undertakings as to a compliance with the Privacy Act.

An enforcement undertaking may impose a significant administrative and operational load upon the party giving the undertaking.

By way of example, following two information security breaches by Singtel Optus, the Commissioner initiated an investigation which concluded with the Commissioner agreeing to accept an enforceable undertaking from Singtel Optus. Optus undertook:

- to engage an independent auditor to conduct reviews and provide audit certifications, including as to whether Optus's practices, procedures and systems are reasonable to protect the personal information Optus holds from misuse, interference or loss, or unauthorised access, modification or disclosure; and whether enhancements to Optus's monitoring program of change management that has the potential to affect the security of its customers' personal and sensitive information and as to Optus's penetration testing for fixed and mobile services were effective;

- to conduct on an ongoing basis an audit review of new procedures for review of all major IT projects as part of Optus's Security Risk Assessment process and as part of its annual monitoring program;

- to conduct a review of Optus's vulnerability detection processes across the organisation, certifications of a privacy incident review, a service level security posture assessment, an architecture review of Optus's principal IT systems (top 20, applying a risk-based approach), and a review of Optus' new voicemail platform.

The OAIC also actively investigates and enforces alleged breaches of the Privacy Act in relation to the use and disclosure of personal information for direct marketing activities. In most cases, the OAIC will seek to conciliate any complaints as to alleged breaches of the direct marketing restrictions in APP 7.

The OAIC publishes its privacy regulatory action policy and a guide to privacy regulatory action, available at www.oaic.gov.au/about-us/our-regulatory-approach.

The ACMA is more active in enforcing court actions to enforce provisions of the Spam Act and the Do Not Call Register Act. However, in most cases the ACMA follows a similar 'graduated enforcement' approach to that adopted by the OAIC. It follows that in most cases the ACMA will, as an initial step, issue a formal warning to entities that breach the Acts. The ACMA regularly accepts enforceable undertakings and issues infringement notices to address non-compliance with the Spam Act and the Do Not Call Register Act.

The ACMA publishes its ACMA compliance and enforcement policy, available at acma.gov.au. The graduated model used by the ACMA to respond to potential non-compliance ranges from encouraging voluntary compliance and informal resolution to administrative action and, where necessary, civil action.

14 REMEDIES AND LIABILITY

14.1 Administrative and judicial remedies

The OAIC has a range of regulatory powers including powers to:

- conduct an assessment of whether an entity is maintaining and handling personal information in accordance with relevant provisions (such as the APPs);
- direct an agency to give the OAIC a PIA;
- request entities to develop an APP code or impose one where appropriate;
- investigate an entity following a complaint;
- investigate an entity on its own initiative, that is, without someone making a complaint (Commissioner initiated investigation);
- accept an enforceable undertaking from an entity. An enforceable undertaking is a promise by an entity that it will take specified action or refrain from taking specified action in order to comply with relevant privacy provisions, or to ensure it does not do an act or engage in a practice that interferes with an individual's privacy;
- make a determination as to a privacy complaint. The OAIC can also make a determination after conducting a Commissioner initiated investigation;
- apply to the courts for an injunction to restrain a person from engaging in conduct that would constitute a breach of relevant privacy provisions or for an order that an entity pay a civil penalty.

A breach of an APP in respect of personal information is an 'interference with the privacy of an individual'. The OAIC may apply for Federal Court and Federal Circuit Court orders for civil penalties to be imposed for serious or repeated breaches of the APPs (s 13G of the Privacy Act).

The Privacy Act provides several complaints paths for individuals where there has been (or is suspected to have been) a breach of an APP. The primary complaints process is through a complaint to the Australian Information Commissioner, initiating an investigation by the Commissioner (s 36 and 40). This process typically requires that the individual has first complained to the relevant APP entity. An investigation may result in a determination by the Commissioner, containing a declaration that:

- the respondent's conduct constituted an interference with the privacy of an individual and must not be repeated or continued;
- the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;

- the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;
- the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint; or
- that no further action is needed (s 52(1)).

A complainant may apply to the Federal Court of Australia or the Federal Circuit Court of Australia to enforce a determination of the Commissioner (s55A). An individual may also apply to the Federal Court or Federal Circuit Court for an injunction where a person has, is, or is proposing to engage in conduct that was or would be a breach of the Privacy Act (s 98). There is not a private right to claim damages, only a right to enforce a declaration by the Commissioner for compensation or to seek an injunction. The private right to seek injunctive relief has been used very infrequently: there appear to have been only two reported cases.

State and territory legislation which creates information privacy requirements similar to those under the Privacy Act provide various mechanisms for individuals to make complaints and seek redress. The Privacy and Personal Information Protection Act 1998 (NSW), for example, provides powers to the NSW Privacy Commissioner that are primarily conciliatory. The Information Privacy Act 2009 (Qld) provides for the referral of complaints to Queensland's Civil and Administrative Tribunal (QCAT), which may order, among other things, that the complainant is entitled to up to $100,000 in compensation.

14.2 Class actions

Although class actions are becoming more common in Australia there have been no reported class actions to date based upon privacy related causes of action. This is unlikely to change unless a private right of action for serious invasions of privacy is enacted, given the limitations imposed under current information privacy statutes as to private causes of action. That noted, the developing law as to misuse of confidential information, and as to misleading and deceptive conduct (I particular, as to any gap between stated data handling practices and actual conduct), provide fertile scope for development of class actions based upon privacy related causes of action.

14.3 Liability

Section 80W of the Privacy Act empowers the OAIC to apply to the Federal Court or Federal Circuit Court for an order that an entity, that is alleged to have contravened a civil penalty provision in that Act, pay to the Commonwealth of Australia a penalty.

A civil penalty order financially penalises an entity but does not compensate individuals adversely affected by the contravention. Each civil penalty provision specifies a maximum penalty for contravention of that provision. The penalty is expressed in terms of 'penalty units'. The value of a penalty unit from time to time is contained in s 4AA of the Crimes Act 1914 (Cth) and as of August 2018 is AU$210.

The 'civil penalty provisions' in the Privacy Act include:

- a serious or repeated interference with privacy (s 13G) – 2000 penalty units; and
- various civil penalty provisions set out in Part IIIA – Credit reporting of the Privacy Act - penalties of either 500, 1000 or 2000 penalty units.

An entity (or person) will also contravene a civil penalty provision, and be liable to pay a penalty, if it:

- attempts to contravene a civil penalty provision;
- aids, abets, counsels or procures a contravention of a civil penalty provision;
- induces a contravention of a civil penalty provision;
- is knowingly concerned in or a party to a contravention of a civil penalty provision; or
- conspires with others to effect a contravention of a civil penalty provision (s 80V).

Peter Leonard
Data Synergies
pleonard@datasynergies.com.au