INTRODUCTION

In Australia, as in many jurisdictions, there have been questions as to whether cloud services that involve offshoring of personal information can be provided from outside Australia in compliance with Australian privacy law and the requirements of regulators. Australian privacy regulation is charting a new course to deal with trans-border privacy, including as-a-service (cloud computing) offerings. This new approach requires regulated entities to apply information management methodologies to evaluate privacy risk and its mitigation on an end-to-end basis, including handling by sub-contractors such as providers of as-a-service offerings. The Australian approach to trans-border data flows also reflects the simplified accountability framework under the 2013 revisions to the OECD Privacy Guidelines, and in particular Article 16: “a data controller remain

THE PRIVACY ACT 1988

The Federal Privacy Act 1988 (Privacy Act) is the principal privacy statute in Australia. It operates across all sectors of the Australian economy. The Privacy Act regulates collection, use, disclosure and retention of ‘personal information’ that is collected for inclusion in any form of print or electronic ‘record’ or in a ‘generally available publication’. The Privacy Act was amended in March 2014. These amendments introduced (among other changes) the Australian Privacy Principles (APPs). Regulated entities are now required to implement processes, procedures and governance that may reasonably be considered to give effect to the entity’s privacy policies and the requirements of the Privacy Act (APP 1.2). This new processes focus has rightly been characterised as an implementation into Australian privacy regulation of the principle of ‘Privacy by Design’.

APPLICATION TO APP ENTITIES

The Privacy Act has extraterritorial reach. Individuals whose personal information is protected by the Privacy Act need not be Australian citizens or Australian residents. The operation of the Privacy Act is generally tied to two factors: the status of the entity engaging in a particular act or practice, and the location in which an entity engages in that act or practice. Where an entity regulated by the Act (an ‘APP entity’) is regulated in relation to its acts or practices outside Australia, those acts or practices must conform with the requirements of the Privacy Act, regardless of requirements of local law in the jurisdiction where the act or practice occurs. Each entity within a corporate group is generally considered separately, although related bodies corporate are treated together for limited purposes.

Generally, compliance with local law in a foreign country where the act or practice occurs, does not excuse non-compliance by an APP entity with the Privacy Act. By specific exception, an act or practice outside Australia will not breach the APPs if the act or practice is both engaged in outside Australia and required by an applicable law of a foreign country. This exception requires legal compulsion: the APP entity cannot elect to make a voluntary disclosure under a foreign law, even if voluntary disclosure is expressly permitted by a relevant foreign law.
Australia’s unique approach to trans-border privacy and cloud computing

Australian Federal Government and its agencies are APP entities regulated in respect of relevant acts or practices as to personal information both within and outside Australia, regardless of whether the personal information was collected in Australia or held in Australia.

Organisations constituted in Australia, such as Australian corporations, partnerships and trusts, are APP entities regulated in respect of relevant acts or practices as to personal information both within and outside Australia regardless of whether the personal information was collected in Australia or held in Australia.

Other organisations and small business operators that are not Australian constituted bodies but that have ‘an Australian link’ are regulated in respect of any act or practice as to personal information outside Australia. Each of two elements must be present before an organisation or a small business operator that operates outside Australia and is not an Australian constituted body ‘has an Australian link’:

+ relevant personal information must be collected or held by the organisation or operator in Australia or an external Territory, either before or at the time of the act or practice; and

+ the organisation or operator must ‘carry on business in Australia’.

Personal information may be ‘collected in Australia’ by the act of collection from an Australian resident even though the collector of that personal information has no physical infrastructure or other activities in Australia. This is because the Act considers a collection to occur where the personal information is collected from, not the place from which the solicitation for collection is made.

The second element (‘carries on business in Australia’) is more contended. The phrase ‘carries on business in Australia’ is not defined in the Privacy Act and the guidance afforded through interpretation of that phrase as used in other areas of Australian law is limited and not consistent. Applying principles as developed in the context of other laws, the provision of services by an overseas entity from outside Australia that does not itself maintain any business presence in Australia, to customers that are APP entities that conduct business within Australia and that themselves collect personal information within Australia, is probably not sufficient to constitute an ‘Australian link’ for the overseas entity providing those services to the APP entity that collects such personal information. It follows that a provider of as-a-service that is not itself an APP entity and that does not conduct its business (including entering into contracts for provision of services) in Australia, and that provides as-a-service to customers in Australia and to customers in other countries respectively wholly from outside Australia, probably does not have a sufficient ‘Australian link’ to fall within the extra-territorial operation of the Privacy Act and thereby be directly regulated in relation to its acts and practices as to personal information outside Australia.

APPLICATION TO OVERSEAS CLOUD SERVICE PROVIDERS

Providers of cloud services may however be ‘overseas recipients’ to whom personal information is ‘disclosed’ in the course of provision of as-a-service to APP entities. This in turn leads to concerns about the operation of an ‘accountability’ requirement in section 16C of the Privacy Act. The relevant provisions read as follows:

“APP 8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual,

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

APP 8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information 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 in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure; and

(ii) after being so informed, the individual consents to the disclosure: ‘…’

The accountability provision, section 16C., provides:

“(1) This section applies if:

(a) an APP entity discloses personal information about an individual to an overseas recipient; and

(b) Australian Privacy Principle 8.1 applies to the disclosure of the information; and

(c) the Australian Privacy Principles do not apply, under this Act, to an act done, or a practice engaged in, by the overseas recipient in relation to the information; and

(d) the overseas recipient does an act, or engages in a practice, in relation to the information that would be a breach of the Australian Privacy Principles (other than Australian Privacy Principle 1) if those Australian Privacy Principles so applied to that act or practice.
(2) The act done, or the practice engaged in, by the overseas recipient is taken, for the purposes of this Act:

(a) to have been done, or engaged in, by the APP entity; and

(b) to be a breach of those Australian Privacy Principles by the APP entity.”

Where personal information is disclosed to an overseas recipient with an ‘Australian link’, an APP entity is not accountable, as the exception in section 16(1)(c) operates. In one possible fact scenario, an overseas entity may itself be a directly regulated APP entity due to the operation of section 5B in relation to some of its activities, while also being an overseas recipient of personal information in other circumstances. The operation of the regulation is not clear in this case: it may be that in this scenario lesser steps under APP 8.1 might be “reasonable” in respect of any disclosure to that overseas entity.

The interpretation of ‘disclose’ is potentially more contentious. ‘Disclosure’ and ‘use’ are not defined in the Privacy Act. The Australian Privacy Commissioner’s (the Commissioner) APP Guidelines state: “B.143 Generally, an APP entity uses personal information when it handles and manages that information within the entity’s effective control. … B.144 In limited circumstances, providing personal information to a contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. For example, if an entity provides personal information to a cloud service provider for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a ‘use’ by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes

- the contract requires any subcontractors to agree to the same obligations, and

- the contract gives the entity effective control of how the information is handled by the provider. Issues to consider include whether the entity retains the right or power to access, change or retrieve the information, who else will be able to access the information and for what purposes, the security measures that will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.”

In relation to ‘disclosure’, the APP Guidelines state “B.64 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. This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient.”

Many Australian businesses have been concerned that entrusting personal information to an offshore cloud service provider is a ‘disclosure’ rather than a ‘use’ and thereby leads to strict liability under section 16C of that customer in the event of any act or practice by the service provider that is contrary to the APPs. The Commissioner recently cautioned against over-stating the distinction: in Sending Personal Information Overseas, May 2015, Privacy business resource 8 and Privacy agency resource 4, the Commissioner stated:

“…the OAIC recognises that in some instances, it can be difficult to determine whether the information is being ‘used’ or whether it is being ‘disclosed’. In such cases, the practical effect of distinguishing a ‘use’ from a ‘disclosure’ should not be overstated. Whether an APP entity sends personal information to an overseas recipient as a ‘use’ or as a ‘disclosure’, it may still be held accountable for mishandling of that information by the overseas recipient. In practice, the steps that an APP entity takes and their accountability when sending personal information overseas can be similar regardless of whether the information is being used or disclosed. For this reason, where it is unclear whether the personal information is being used or disclosed, the best approach is to take reasonable steps to ensure the APP are complied with. An APP entity that sends personal information overseas may be liable if the personal information is mishandled.”

AN INFORMATION MANAGEMENT APPROACH TO DISCLOSURE

The Privacy Act does not expressly address whether maintaining effective control should be regarded as the indicia of ‘use’ rather than ‘disclosure’. Australian privacy law generally does not use concepts of ‘control’ over data: in this respect the Australian law differs substantially from jurisdictions that use concepts such as ‘data controller’ and ‘data processor’. So the concept of ‘effective control’ is somewhat contentious. The Commissioner has not expressed a definitive view as to whether any form of controlled access by a service provider might constitute a disclosure by the customer to the service provider. However, the Commissioner appears to be developing an information management based approach to regulatory enforcement of APP 8.1. Applying an information management based approach, ‘effective control’ could be considered to be maintained by a customer if access by the service provider to personal information is controlled by technical, operational and contractual safeguards that are appropriate in all the circumstances, in particular having regard to the sensitivity of the personal information and the risk of further use or uncontrolled disclosure.

Effective controls clearly can mitigate risk of subsequent or unauthorised disclosure. But what is the appropriate standard of mitigation of risk? - The Australian Privacy Commissioner has not expressed a definitive view as to the point at which the controls can be objectively evaluated to be effective such that there should be considered to be no ‘disclosure’. However, the Commissioner’s Business Resource 4: De-identification of data and information provides a useful analogy. For deidentification techniques to be considered to have appropriately addressed reidentification risk, the objective assessment of reidentification risk ‘in-the-round’ must be that it is low. Applying this analogy, for effective controls as to acts and practices of the service provider to be indicia of ‘use’
Australia’s unique approach to trans-border privacy and cloud computing

rather than ‘disclosure’, the risk of an act or practice by the service provider that is an unauthorised use or disclosure, or otherwise contrary to the Privacy Act, must be mitigated through appropriate safeguards to the point where that risk is reliably and verifiably low.

An information management approach to disclosure essentially places the obligation upon the APP entity to ensure the effectiveness and reliability of the APP entity’s data lifecycle controls on an end-to-end basis by bringing contracted services or sub-processes (such as on demand software services provided by external service providers) within the APP entity’s information management processes. But where handling of personal information held by an offshore service provider is a ‘use’ and not a ‘disclosure’ by the APP entity, that APP entity will remain responsible for ensuring that the service provider’s use of that personal information does not cause the APP entity to breach the APPs: hence the Commissioner’s caution as to the distinction between ‘use’ and ‘disclosure’ in this context. Regardless of whether there is ‘use’ and ‘disclosure’, transparency, accountability and governance mechanisms will usually be important aspects of the terms of provision of contracted service arrangements and of ongoing administration of outsourcing and offshoring arrangements to assure compliance with the contractual terms. But if these mechanisms and the contractual terms meet the appropriate standard, it is reasonable to conclude that the personal information of individuals that is collected by the customer and held and processed by the service provider is ‘used’ and ‘held’ by the customer and not ‘disclosed’ to the service provider and therefore that section 16C does not apply. This should remain the case even if that personal information is able to be viewed under limited and defined circumstances by the service provider; because the personal information never leaves the effective control of the customer.

Another advantage of an information management approach is that it may also be applied to management of commercially sensitive customer information that is not personal information about individuals. Many customers will require a high level of assurance of protection of their confidential business information. This approach applies that same high level of assurance to personal information, while also giving effect to privacy regulation of personal information as a distinct information asset.

In summary, the information management approach requires:

+ a binding contract between the APP entity as customer and the service provider that commits the service provider only to handle the personal information for the limited purposes of provision of as-a-service to the customer; and
+ the contract requires any subcontractors to agree to the same obligations;
+ contractual provisions that ensure reliable and verifiable implementation of technical, operational and contractual safeguards that are effective controls that mitigate risk of disclosure to third parties (whether advertent or by hacking or other intrusions) to the point where there should be considered to be no ‘disclosure’ because the risk of an act or practice by the service provider that is contrary to the Privacy Act is low.

The technical, operational or contractual safeguards that are appropriate to a particular as-a-service offering should be determined having regard to the sensitivity of the information asset.

Entities in some sectors are subject to a higher level of regulation. The Australian Prudential Regulatory Authority has released detailed requirements for financial institutions using cloud services. APRA’s July 2015 Information Paper Outsourcing Involving Share Computing Services (including Cloud) recognises that public cloud is inevitable for financial services. It provides constructive guidelines for managing risks in a cloud world. By way of exception, APRA questions the appropriateness of migrating critical systems of record to the public cloud. APRA’s approach to risk is very broad, encompassing traditional areas of risk assessment (including security and business disruption) and also:

+ the up-front selection process;
+ key factors to be addressed in contracts;
+ governance requirements;
+ the challenges around transition; and
+ innovative and pragmatic approaches to ongoing assurance.

APRA focuses on ‘observed weaknesses’ in current practices and sets out useful checklists for best practice migration of APRA-regulated entities to cloud services. APRA also encourages financial sector entities to consult with APRA before entering into cloud services arrangements with a “heightened inherent risk”.

Other regulatory and standards bodies have also expressed opinions as to outsourced and offshoring services. For example, the Australian Accounting Professional & Ethical Standards Board, has issued a Guidance Note, APES GN 30 Outsourced Services (March 2013), which also states ‘subject matter that should be considered for inclusion in an Outsourcing Agreement’. Federal Government has issued extensive guidance and some mandatory requirements, which must be met by Federal Government agencies.

In conclusion, APP entities, including government agencies, can use as-a-service offerings that include an offshoring element in full compliance with privacy law. Risk assessment needs to be conducted. Information management steps must be determined to take into account of the requirements of the APPs. Customers should carefully evaluate each service provider and ensure that certain contractual provisions are in place and that there are the appropriate transparency, accountability and governance mechanisms to ensure that privacy risk management is verifiably and reliably implemented.

August 2015