FINDING CLARITY IN THE CLOUDS

Australian Privacy and Prudential Compliance of Cloud Services for Australian Business and Government Agencies

Peter Leonard

September 2016

GILBERT+TOBIN

SYDNEY | MELBOURNE | PERTH

CONTENTS

Finding Clarity in the Clouds

Australian privacy and prudential compliance of cloud services for Australian businesses and government agencies[1]

KEY POINTS

(a) This White Paper concerns the use of *as-a-service* offerings, also referred to as *cloud services* or *on-demand software services*. Our principal focus is how to ensure that this use is consistent with Australian privacy law and prudent practices. We also consider the standards and guidelines of the Australian Prudential Regulatory Authority as applied to regulated financial institutions and the Australian Government policies and guidelines affecting federal government departments and agencies. Because privacy and prudential regulation and good business practice requires data collectors to assess, manage and mitigate risk, we focus upon risk assessment and management relevant to evaluation and implementation of as-a-service offerings.

(b) As-a-service offerings have many benefits when compared to traditional software supply and integration into a customer's own systems. Properly implemented as-a-service should reduce, rather than enhance, risk. Relevant risk depends upon factors such as how an entity intends to use the service, the nature of that data (in particular, whether it is highly business sensitive whether personal information is being handled) and how the cloud service is implemented and managed. Where personal information or other sensitive information is being handled by a service provider, customers will wish to ensure appropriate transparency, accountability and proper governance measures are put in place, so that if there is a security incident, this incident is detected on a timely basis and response is prompt, managed and appropriate.

(c) Customers considering use of as-a-service need to consider the characteristics of data to be stored or processed and weigh information management and privacy risks against those associated with use of in-house computer systems. In-house systems may be poorly secured and monitored, have inadequate availability or be unable to flex and evolve with changing business requirements. Transition to as-a-service therefore has the potential to enhance privacy (including information security) safeguards available to protect personal information as compared to a customer's own (in-house) systems. The effectiveness of data lifecycle controls in the case of both outsourcing and offshoring must be evaluated to ensure that these controls remain appropriate, or are adapted or supplemented in order to be appropriate, so that information management processes are known and reliable and verifiable in practice (and auditable if required).

---

[1] **Important Notice and Disclaimer:** This White Paper provides a summary and general overview of Australian privacy compliance for cloud services. It is not intended to be comprehensive. This White Paper may not be current when read: it is published as at 1 September 2016. This White Paper does not deal with particular circumstances of any entity and it does not constitute legal advice. A reader should seek legal or other appropriate professional advice that takes account of the reader's particular circumstances.

(d) As-a-service is a particular form of outsourcing, often also including an offshoring element. Outsourcing or offshoring by an Australian entity, whether business or government agency, requires consideration of the effect of that outsourcing or offshoring upon the control of that entity over data, including personal information and confidential business information, collected and held by that entity.

(e) Offshoring of personal information has been the subject of concern for some prospective Australian customers of as-a-service offerings and of Australian regulators of those customers. The concern is principally attributable to several factors. The Australian 'accountability framework' that applies to offshore disclosure of personal information has only been in operation since March 2014. This framework is significantly different from cross-border data transfer regulation in most other highly regulated jurisdictions, so regulatory guidance from other jurisdictions is of little relevance. The initial guidance on cross-border disclosure from the Australian Privacy Commissioner was quite general in nature, although that guidance has since been clarified and supplemented. The operation of Australian privacy law has therefore not been well understood by some potential as-a-service customers.

(f) There are also legitimate questions that arise from any possibility of personal information collected about individuals moving out of the effective control of the data collector who those individuals rightly consider responsible for the stewardship of personal information about them. Some data collectors express concern that personal information collected by them might move beyond those jurisdictions that have effective privacy regulation and enforcement. Although secondary movement of data beyond nominated destinations is readily controllable through appropriate contractual restrictions, some global service providers have been slow or unwilling to make commitments as to global data handling practices or data destinations. Some service providers have also been unwilling to provide an appropriate level of transparency as to activities and misadventures, including reporting of material adverse events and their remediation, or to implement accountability and governance frameworks consistent with the level and materiality of privacy, prudential or perceived reputational risks and their mitigation.

(g) The key message of this paper is that provided data collectors assess, manage and mitigate risk (by applying now well-developed risk assessment methodologies and risk management frameworks and practices, Australian entities, including those in government, financial services and other significantly regulated sectors, can use as-a-service offerings, including such offerings with offshoring elements, in full compliance with privacy law and prudential regulation. This conclusion also applies to APRA regulated financial institutions, that following diligence and implementing information risk management and proper contractual safeguards mat use as-a-service offerings in compliance with APRA requirements. As-a-service customers should carefully evaluate each service provider and their offerings and ensure that certain contractual provisions are in place and that there is the appropriate transparency, accountability and governance to ensure that ongoing risk management is verifiably and reliably implemented.

(h) A checklist is included as an addendum to this paper.

Peter Leonard
Gilbert + Tobin Lawyers

1 Taking compliance seriously

Offshoring of personal information as associated with many as-a-service offerings[2] raises novel issues for customers, for regulators of customers, and for government in relation to government agency customers. In particular, 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.

For this reason, in this White Paper we first consider the relevant elements of Australian privacy law and how they operate in relation to providers of as-a-service offerings and their services.

We then turn to consider, from the viewpoint of the prospective customer, the broader questions of risk assessment and information risk management that should be addressed in the course of evaluation of as-a-service offerings and of contract terms offered by service providers.

As noted in the Australian Government's *Privacy and Cloud Computing for Australian Government Agencies: Better Practice Guide*, February 2013:

> "Despite common perceptions, cloud computing has the potential to enhance privacy safeguards used to protect personal information held by Government agencies. ….. Irrespective of choosing traditional methods of provisioning ICT [Information, Communications and Technology] requirements or cloud computing services, agencies need to be aware of their privacy and security obligations, conduct a risk-based analysis of

[2] The following discussion applies both to Software as a Service (**SaaS**) and Platform as a Service (**PaaS**) which in this White Paper are referred to collectively as 'as-a-service'' offerings. These offerings are also sometimes referred to as 'cloud services' or 'on-demand software services'. SaaS is usually defined as the capability provided to a customer to use a provider's applications running on private or public cloud infrastructure. These applications may be accessible from various client devices, through either a thin client interface such as a web browser (e.g. web-based email) or a program interface. In SaaS offerings the consumer does not own or operate the underlying cloud infrastructure including network, servers, operating systems, storage, or individual application capabilities, with the possible exception of limited, user-specific application configuration settings. PaaS is usually defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. In PaaS offerings the consumer does not own or operate the underlying cloud infrastructure including network, servers, operating systems, or storage, but controls the deployed applications and possibly configuration settings for the application-hosting environment.

their information, and ensure that the contractual arrangements they enter into with ICT providers adequately address their privacy obligations. It is important to note that the *Privacy Act* 1988 does not prohibit the use of cloud computing and an agency, having conducted appropriate due diligence, may contract for cloud computing services and comply with its Privacy Act obligations, as with current ICT contractual practice." [3]

Sections 6, 7 and 8 of this White Paper review the range of contractual, technical and operational safeguards that may be implemented to ensure that personal information always remains under the effective control of a customer notwithstanding the outsourcing and any offshoring aspects of use by a customer of as-a-service offerings.

Section 9 outlines the specific requirements that Australian governments impose upon use of as-a-service by government agencies.

Section 10 then deals with additional requirements that APRA prescribes for financial institutions that are regulated by APRA and that the ASX prescribes for ASX trading entities and other ASX market participants (including their trading and clearing functions).

Our conclusions are summarised above in the Key Points above and in section 11 of this White Paper.

2 Coverage of the *Federal Privacy* Act 1988 including the APPs

The Federal *Privacy Act* 1988[4] (**Privacy Act**) is the principal privacy statute in Australia. It operates across all sectors of the Australian economy. The Privacy Act regulates collection, use,

---

[3] Available at www.finance.gov.au/cloud. Perceived privacy and security related risks are well summarised in the Office of the Privacy Commissioner of Canada, *Reaching for the Clouds: Privacy Issues relating to Cloud Computing*, March 2010, available at https://www.priv.gc.ca/information/research-recherche/2010/cc_201003_e.asp.

[4] Available with consolidated amendments at http://www.comlaw.gov.au/Details/C2014C00757. Note that this consolidation is authoritative and it is regularly updated but it is not always current.

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 by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth). The amendments, which commenced on 12 March 2014, introduced (among other things) the Australian Privacy Principles[5] (**APPs**). The APPs replaced and substantially re-focussed the former National Privacy Principles (**NPPs**) that applied to private businesses, subject to a (continuing) small business exception, and the Information Privacy Principles (**IPPs**), which applied to Federal government agencies and contractors to such agencies. Most relevantly to this White Paper, the new accountability principle for cross-border disclosures was introduced by these amendments.

Key aspects of the APPs that are relevant to the use of as-a-service by Federal Government and business entities, being entities regulated by the Privacy Act (collectively referred to in the Act and this White Paper as '**APP entities**'), include requirements:

- to publish and comply with clearly expressed and up-to-date policies about the management of personal information by the entity (APP 1);
- to implement processes, procedures and governance that may reasonably be considered to give effect to those privacy policies and the requirements of the Privacy Act (APP 1.2). The Privacy Commissioner has emphasised the importance of readily understandable disclosure as to privacy practices and the match of policies to implemented practices.[6] This processes and procedures requirement has been characterised as an implementation into Australian privacy regulation of the principle of 'Privacy by Design'[7];
- to provide a relatively prescriptive notice when information is collected, including notice about likely disclosures to overseas recipients(APP 5);
- in some circumstances, before disclosing personal information to overseas recipients, to take reasonable steps to ensure that the overseas recipients do not breach the APPs in relation to that personal information (APP 8). Further, in some circumstances, an APP entity may be liable for a breach of the APPs by the overseas recipient (s 16C);

---

5. The 13 APPs are contained in schedule 1 of the *Privacy Act* 1988. They are separately available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles.

6 See Australian Privacy Commissioner, *Privacy management framework*, May 2015 as available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-management-framework; also *Guide to developing an APP privacy policy* and *Guide to undertaking privacy impact assessments,* each May 2014 and available at http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy.pdf and http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/guide-to-undertaking-pias.pdf.

7 Ibid. Privacy by design (PbD) is an important element of the Australian Privacy Commissioner's *Privacy management framework* of May 2015 at https://www.oaic.gov.au/agencies-and-organisations/guides/privacy-management-framework. See also *Privacy by Design (PbD),* http://www.oaic.gov.au/privacy/privacy-topics/privacy-by-design-pbd/.The Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill* 2012 states: "This inclusion of APP1 will keep the Privacy Act up-to-date with international trends that promote a 'privacy by design' approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception": page 72. Many publications of the Australian Privacy Commissioner explain and apply 'privacy by design' principles. See for example Office of the Australian Information Commissioner, *Guide to securing personal information*, January 2015, pages 7 and 8, available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-securing-personal-information.

- to take reasonable steps to destroy or de-identify information if the APP entity no longer needs the information for any authorised purpose (APP 11).

As is customary with Federal statutes, the *Privacy Amendment (Enhancing Privacy Protection) Bill* 2012 was accompanied by a lengthy Explanatory Memorandum.[8] An Explanatory Memorandum is a guide to the intended effect and operation of the Bill when enacted.

The amendments made by that Bill (as enacted) also included provisions empowering the Privacy Commissioner to issue guidelines as to the operation of the Privacy Act.[9] In February 2014 the Privacy Commissioner first released the *Australian Privacy Principles Guidelines* (**APP Guidelines**), as subsequently amended and updated in April 2015.[10] As stated by the Privacy Commissioner, "The APP guidelines outline the mandatory requirements of the APPs, how the Privacy Commissioner will interpret the APPs, and matters we may take into account when exercising functions and powers under the Privacy Act".[11]

The Explanatory Memorandum has legislative status as an aid to statutory interpretation if, among other things, provisions of an Act are not clear on their face.[12] The APP Guidelines do not have formal legislative status.[13] However, the APP Guidelines are of significant interest as an expression of the Privacy Commissioner's interpretation of key provisions of the Privacy Act. The APP Guidelines can reasonably be expected to be applied by the Commissioner as the enforcement authority for the Act. The Guidelines can be expected to be taken into account by the courts in any review of enforcement action taken by the Privacy Commissioner. The Guidelines are an important statement of authority as to interpretation of key provisions of the Privacy Act and may therefore be expected to be reviewed where relevant to any matter for judicial determination, while not binding the court.

---

8 Available at http://www.comlaw.gov.au/Details/C2012B00077/Explanatory%20Memorandum/Text.

9 The 'guidance related functions' of the Commissioner include "making guidelines for the avoidance of acts or practices that may or might be interferences with the privacy of individuals, or which may otherwise have any adverse effects on the privacy of individuals": section 28(1)(a).

10 Available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/. Note that the Guidelines were updated by the Australian Privacy Commissioner in March 2015 and some significant amendments were then made from the earlier (March 2014) edition of the Guidelines: see the Commissioner's *Summary of version changes to APP guidelines* at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/summary-of-version-changes-to-app-guidelines.

11 Section 15AB(1) of the *Acts Interpretation Act* 1901 (Cth) provides that (together with certain other material specified in section 15AB(3)) an explanatory memorandum relating to the Bill containing a provision may be taken into consideration to confirm that the meaning of the provision is the ordinary meaning conveyed by the text of the provision taking into account its context in the Act and the purpose or object underlying the Act, or to determine the meaning of the provision when the provision is ambiguous or obscure, or the ordinary meaning conveyed by the text of the provision taking into account its context in the Act and the purpose or object underlying the Act leads to a result that is manifestly absurd or is unreasonable.

12 Available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/.

13 Guidelines made under paragraph (1)(a) are not a legislative instrument: section 28(4) of the Privacy Act.

3 Personal Information

The Privacy Act regulates the handling (collection, use, disclosure and retention) of 'personal information' about individuals (natural persons). Some sub-categories of personal information, such as sensitive information and credit information, are also subject to additional requirements.

Information is 'personal information' if an individual is identified or reasonably identifiable, whether from the information in question or the combination or analysis of that information together with other reasonably available information.[14] Whether a person is 'reasonably identifiable' requires an exercise of objective judgement about the likelihood of an individual's identity being re-ascertained. Once information is effectively de-identified, it is no longer regulated as 'personal information'. If information is purportedly de-identified but an individual could be re-identified using other information that is available, then that purportedly de-identified information is still personal information and must be handled as personal information. The act of de-identification is not of itself a use of personal information and accordingly does not require notice to, or consent of the individual to whom the information relates.[15]

The APP Guidelines suggest that whether an individual is 'reasonably identifiable' from particular information will depend on considerations:

> "that include:
>
> - the nature and amount of information

---

[14] Definition of 'personal information' in section 6 of the Privacy Act. The circumstances in which an individual may reasonably be identified were considered in the context of the former definition of personal information in the Australian Privacy Commissioner's determination in *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35 (1 May 2015), available through http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-determinations, and in a number of earlier decisions applying analogous definitions in State privacy statutes as cited in that determination . This determination was over-turned in the Administrative Appeals Tribunal and then went on appeal to the Full Federal Court of Australia. As at the date of writing of this White Paper the decision of the Full Federal Court of Australia was pending.

[15] Australian Privacy Commissioner, *Privacy business resource 4: De-identification of data and information*, available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information. See further OAIC, *Guide to big data and the Australian Privacy Principles*, Consultation Draft May 2016, https://www.oaic.gov.au/engage-with-us/consultations/guide-to-big-data-and-the-australian-privacy-principles/consultation-draft-guide-to-big-data-and-the-australian-privacy-principles.

- the circumstances of its receipt
- who will have access to the information and 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'
- if the information is publically released, whether a reasonable member of the public who accesses that information would be able to identify the individual."[16]

4 Extraterritorial reach of the Privacy Act

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 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. For example, where 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.[17]

Generally, compliance with local law in a foreign country where the act or practice occurs, including pursuant to any law of that foreign country, does not excuse non-compliance by an APP

---

16 At paragraph B.91, available at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/.

17 Sections 6(8) and 13B(1) of the Privacy Act. Those limited purposes are not relevant to the discussion in this White Paper.

entity with the Privacy Act. However, 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.[18] In the (different but directly analogous) context of considering when an act or practice 'is required by an Australian law or a court/tribunal order', the Privacy Commissioner in the APP Guidelines draws a distinction between 'required' and 'authorised', as follows:

> "An APP entity that is 'required' by an Australian law or a court/tribunal order to handle information in a particular way has a legal obligation to do so, and cannot choose to act differently. The obligation will usually be indicated by words such as 'must' or 'shall', and may be accompanied by a sanction for non-compliance.
>
> 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. The entity is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as 'may', but may also be implied rather than expressed in the law or order."[19]

This analysis should apply equally to an applicable law of a foreign country which applies of its own force to oblige an entity to handle information outside Australia in a particular way, where that entity in that place cannot lawfully elect to act differently. The Privacy Act does not expressly require that the legal compulsion created by an applicable law of a foreign country to be the law of the jurisdiction in which the act or practice is required to take place. Thus, the Privacy Act appears to allow laws of foreign countries to have extra-territorial application to APP entities in other foreign countries, provided in all cases that the purported extra-territorial operation of that applicable law does not mandate or compel a breach of the Privacy Act by requiring an act or practice to take place within Australia and its external Territories that would be a breach of the Privacy Act. Accordingly, the Privacy Act does not preclude so-called 'long-arm reach' or 'extended extra-territorial reach' foreign statutes in some circumstances operating to require disclosures to be made outside Australia to foreign government agencies, courts or tribunals where an APP entity or other person making the disclosure is obliged by a foreign law effective in that place to require that disclosure.

The APP Guidelines state in relation to section 6A(4) as follows:

> "8.61 The effect of this provision is that where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the APPs. The APP entity will also not be responsible for the act or practice under the accountability provision.[20]
>
> 8.62 For example, the USA PATRIOT Act[21] may require the overseas recipient to disclose personal information to the Government of the United States of America. In these circumstances, the APP entity would not be responsible under the accountability provision for the disclosure required by that Act.

---

18 See the note to each of sections 5B(1) and 5B(1A) and section 6A(4) of the Privacy Act.

19 *APP Guidelines* paragraphs B.129 and B.130, page 26.

20 The so-called 'accountability provision' is section 16C of the Privacy Act, as discussed below.

21 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* Act of 2001 (USA).

8.63 An APP entity could consider notifying an individual, if applicable, that the overseas recipient may be required to disclose their personal information under a foreign law. The entity could also explain that the disclosure will not breach the APPs. This information could be included in the APP entity's APP 5 notice, particularly if the entity usually discloses personal information to overseas recipients (see APP 5.2(i), Chapter 5), or in its APP Privacy Policy (see Chapter 1 (APP 1)).”[22]

However, the APP entity cannot elect to make a voluntary disclosure, even if that voluntary disclosure is expressly permitted by a relevant foreign law.

5 Which entities are 'APP entities' and therefore directly regulated by the Privacy Act?

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,[23] 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,[24] 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.[25] Each of the following two elements must be present before an

---

22 *APP Guidelines* Chapter 8 paragraphs 8.61, 8.62 and 8.63, page 16.

23 Section 5B(1) of the Privacy Act.

24 Sections 5B(2) and 6C of the Privacy Act.

25 Sections 5B(1A) and 5B(2) of the Privacy Act.

organisation or a small business operator that operates outside Australia and that is not an Australian constituted body 'has an Australian link':

- The 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'.

- The organisation or operator must 'carry on business in Australia'. [26]

Personal information may be 'collected in Australia' by the act of collection from an Australia 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.[27]

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. The guidance afforded through interpretation of that phrase as used in other areas of Australian law is limited and not consistent.[28] Clearly, there must be some relevant ongoing activity relating to Australia by that entity itself (or an agent acting directly on behalf of that entity and able to exercise its authority) that forms part of the entity's business. The Privacy Act treats members of a corporate group as separate entities for this purpose, so the position of each company within a group must be separately considered. A common view is that some form of ongoing or regular physical activity of an entity in Australia, either through persons conducting the business of that entity in Australia, or through that entity owning or operating infrastructure in Australia, may be enough for an entity to be regarded as carrying on business in Australia. This may be the case even though such activities may fall well short of constituting a 'permanent establishment in Australia' under Australian international tax law. However, a multi-factorial test is applied having regard to the objects of the relevant legislation, which in the case of the Privacy Act is to "promote the protection of the privacy of individuals".[29]

Applying these 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, does not appear sufficient of itself 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, does not appear to have a

---

26 Section 5B(3)(c) of the Privacy Act.

27 Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill* 2012, Item 6 - Subsection 5B(3), page 218. See also APP Guidelines, paragraph B.22, page 7.

28 See Australian Securities and Investments Commission (ASIC), *Regulatory Guide 121: Doing financial services business in Australia*, July 2013, at paras RG121.47 to RG121.50 and the cases listed at page 53 of that Guide. Available at http://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-121-doing-financial-services-business-in-australia/. See further *Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196 per Edelman J at [158] to [205].

29 Section 2A(a) of the Privacy Act; *APP Guidelines* paragraphs B.17 to B.21, pages 6 and 7.

sufficient ‘Australian link’ to fall within the extra-territorial operation of section 5B(3) of the Privacy Act and thereby be directly regulated in relation to its acts and practices as to personal information outside Australia.

6 Disclosure to overseas recipients and indirect regulation by the Privacy Act

As discussed above, many global providers of as-a-service offerings will not have a relevant ‘Australian link’ and will not be directly regulated in relation to their acts and practices as to personal information outside Australia in the course of provision of those services.

Such 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 may lead to concerns of an APP entity as to its ‘accountability’ under section 16C of the Privacy Act in relation to any act or practice of that external service provider handling personal information that is ‘disclosed’ to that external service provider in the course of (or arising out of) provision of services to the APP entity, where that act or practice would be a contravention of the Privacy Act were the act or practice that of the APP entity itself.

A prudent APP entity will also wish to ensure end-to-end effectiveness and reliability of the APP entity’s data lifecycle controls that form part of the entity’s information management processes. End-to-end effectiveness and reliability requires transparency and accountability of sub-contractors in relation to any sub-contracted services or sub-processes where personal information is handled, including as as-a-service offerings provided by external service providers that handle personal information. Transparency and accountability will prudently be required regardless of whether an external service provider is directly regulated by the Privacy Act. To ensure that contractual commitments are in fact implemented, a prudent APP entity will also seek to ensure that compliance to Australian privacy standards in relation to handling of personal information by external service providers is verifiable and auditable if required.

The relevant provisions in the Privacy Act as to ‘disclosures’ to ‘overseas recipients’ 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.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

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;

(ii) after being so informed, the individual consents to the disclosure;… ."

The accountability provision, section 16C (*Acts and practices of overseas recipients of personal information*), 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."

The key relevant terms, being 'overseas recipient' and 'disclose', are not defined in the Privacy Act. The APP Guidelines relevantly state:

> "Under APP 8.1, an 'overseas recipient' is a person who receives personal information from an APP entity and is:
>
> - not in Australia or an external Territory
> - not the APP entity disclosing the personal information, and
> - not the individual to whom the personal information relates."[30]

Where personal information is disclosed to an overseas recipient with an 'Australian link', an APP entity is not accountable, as the exception within section 16(1)(c) operates.[31] 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 a particular factual scenario. 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' is not defined in the Privacy Act but is used in contradistinction to 'use' and 'holds'.

'Holds' is particularly relevant in the case of access rights of affected individuals to personal information 'held' by APP entities about those individuals. The APP Guidelines state:

> "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. Whether an APP entity 'holds' a particular item of personal information may therefore depend on the particular information collection, management and storage arrangements it has adopted. For example, an APP entity 'holds' personal information where:
>
> - it physically possesses a record containing the personal information and can access that information physically or by use of an electronic device (such as decryption software)
> - it has the right or power to deal with the personal information, even if it does not physically possess or own the medium on which the personal information is stored. For example, the entity has outsourced the storage of personal information to a third

---

30 APP *Guidelines* paragraph 8.5, page 4.

31 Section 16C will only apply where, in addition to the other conditions stated in section 16C, paragraph (c) is satisfied, namely, 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." If the Act has extraterritorial operation pursuant to section 5B to the overseas entity, then paragraph (c) is not satisfied.

party but it retains the right to deal with it, including to access and amend that information."[32]

'Use' is also not defined in the Privacy Act. The 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. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another
- unauthorised access by an employee of the entity.

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 (see paragraph B.63–B.68). 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."[33]

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

---

[32] *APP Guidelines* paragraph B.81, page 18.

[33] *APP Guidelines* paragraphs B.143 and B.144, pages 28 and 29; see also Chapter 8, paragraph 8.14.

the actions or knowledge of the recipient. Disclosure, in the context of the Privacy Act, can occur even where the personal information is already known to the recipient.

B.65 The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee.

B.66 Examples include where an APP entity:

- shares a copy of personal information with another entity or individual
- discloses personal information to themselves, but in their capacity as a different entity
- publishes personal information whether intentionally or not and it is accessible to another entity or individual.
- accidentally provides personal information to an unintended recipient
- displays a computer screen so that the personal information can be read by another entity or individual, for example at a reception counter or in an office.

B.67 Where an APP entity engages a contractor to perform services on its behalf, the provision of personal information to that contractor will in most circumstances be a disclosure (see paragraph B.144 for the limited circumstances where it will be a 'use')."[34]

The Privacy Act also imposes specific restrictions on the disclosure of personal 'credit eligibility information' to entities that do not have an Australian link. These rules are arguably more restrictive than those that relate to the cross-border disclosure of general personal information under APP 8, as they seek to limit disclosures of credit eligibility information to certain categories of recipients, namely related bodies corporate of the credit provider, its credit managers and debt collectors.

The Privacy Act also expressly requires the credit provider to take reasonable steps to limit the recipient in its use and disclosure of the credit eligibility information, and ensure the recipient's compliance with certain, but not all, APPs. An accountability principle, in similar terms to the provisions under s 16C, also applies to the credit provider in respect of any breaches by the recipient in relation to the information.

While the APP Guidelines do not expressly apply to the offshoring of credit eligibility information, the principles we discuss below as to the 'use' or disclosure' of personal information are directly analogous to the 'use' or 'disclosure' of credit eligibility information for the purposes of the Privacy Act.

In considering the distinction between 'use' and 'disclosure', it is important to not overstate the significance of that distinction when applying a privacy risk management. As recently stated by the Australian Privacy Commissioner:

---

[34] *APP Guidelines* paragraphs B.64 to B.67, pages 14 and 15; see also Chapter 8, paragraph 8.14.

"…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."[35]

7 Effective control by the customer as an indicia of use rather than disclosure

Notwithstanding the Privacy Commissioner's analysis in the APP Guidelines, 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'. The only reasonably analogous law is the Canadian Federal PIPEDA. [36] In administering PIPEDA, the Privacy Commissioner of Canada has had to consider 'use' versus 'disclosure' in the course of issuing a number of detailed determinations. The Privacy Commissioner of Canada concluded that a transfer for processing is a 'use' of the information and not a 'disclosure' and that assuming the information is being used for the purpose it was originally collected, additional consent for the transfer is not required. The transferring organization is accountable for the information in the hands of the organization to

---

35 *Australian* Privacy Commissioner, Privacy business resource 8 and Privacy agency resource 4,*Sending Personal Information Overseas*, May 2105, available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-agency-resources/privacy-agency-resource-4-sending-personal-information-overseas and http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-8..

36 *Personal Information Protection and Electronic Documents Act* S.C. 2000, c. 5

which it has been transferred. Organizations must protect the personal information in the hands of processors. The primary means by which this is accomplished is through contract.[37]

The *EU Data Protection Directive*, the *OECD Privacy Guidelines* and the *Asia Pacific Economic Cooperative (APEC) Privacy Principles* each differ from Australian law by drawing a distinction between 'data controllers' and 'data processors'. Data controllers, including customers acquiring as-a-service, carry the primary data protection obligations. Providers of as-a-service generally would be considered data processors and subject to more limited obligations. The regulatory logic is that the obligations on data controllers are higher as data controllers collect the data for their own purposes, have the ability to access, update and use the data, and generally have a direct relationship with the individual who is the subject of the personal information. The more limited range of obligations applicable to data processors principally focus upon ensuring adequate security of personal information.

While the test put forward by the Australian Privacy Commissioner is one of 'effective control', the Australian Privacy 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. The breadth of the circumstances in which the effective control test is intended to apply by the Australian Privacy Commissioner is somewhat unclear from reading some Guidelines on their face: for example paragraph B.66 of the APP Guidelines states that disclosure occurs when an APP entity "shares a copy of personal information with another entity". Paragraph 8.13 states it is "generally considered" a disclosure where "an Australian organisation relies on its overseas parent company to provide technical and billing support, and as part of this, provides the overseas parent company with access to its Australian customer database (which includes personal information)". The mere fact that a customer has a contract with a service provider with appropriate restrictions as to the handling of personal information is not of itself determinative (otherwise APP 8.1 would not apply to any business process outsourcing or similar service), because other examples provided by the Privacy Commissioner where disclosure occurs include the engagement of contractors to "process" online purchases or to perform reference checks on the customer's behalf.[38]

However, the Australian Privacy Commissioner subsequently clarified the Commissioner's preferred interpretation of the term 'disclose'. The March 2015 amendments to the APP Guidelines changed what is now paragraph B.64 to state that "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". The addition of "or visible" as an additional element (separate from release from effective control) strengthens support for the interpretation that view access by an as-a-service provider in circumstances where effective control of the information so viewed is maintained by the customer should not (without more) be a 'disclosure' under APP 8.1.

---

37 The decisions are conveniently summarised in Office of the Privacy Commissioner of Canada, *Reaching for the Clouds: Privacy Issues relating to Cloud Computing*, March 2010, available at https://www.priv.gc.ca/information/research-recherche/2010/cc_201003_e.asp. See also Office of the Privacy Commissioner of Canada, *Guidelines for Processing Personal Data Across Borders,* available at https://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp.

38 *APP Guidelines* paragraph 8.13, page 6.

It is unfortunate that the Privacy Act does not on its face put this matter beyond argument, given the fast growing take-up by Australian businesses of as-a-service offerings made available by global providers. Even though the Privacy Commissioner's view is highly persuasive, a risk remains that another regulator or a tribunal might reach a different conclusion if called upon to consider, for example, an allegation by an end user that an as-a service customer had not complied with a statement made to affected individuals that the customer will fully comply with the Privacy Act when the customer allowed an as-a-service provider limited and controlled access to personal information in the course of provision of technical support. Preferably, the Australian Parliament should amend the Privacy Act to give greater clarity and support to the Privacy Commissioner's view, particularly as the effective control test adopted by the Australian Privacy Commissioner is somewhat distanced from what might be said to be an ordinary English language meaning of the term "disclosure". However, in the interim the interpretation now supported by the Australian Privacy Commissioner appears to be a sensible, information management based approach to regulatory enforcement of APP 8.1, consistent with the information management principles-based nature of the legislation. On this basis effective control ought properly be considered to be maintained if access to and use of personal information is controlled by implementation of technical, operational and contractual safeguards that are appropriate having regard to the sensitivity of the personal information and the risk of further use or uncontrolled disclosure.

Effective controls, through appropriate information management safeguards, clearly will mitigate risk of subsequent or unauthorised disclosure. 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 de-identification guidance[39] may provide an appropriate 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.[40] Applying this analogy, for effective controls as to acts and practices of the service provider to be indicia of 'use' 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. 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. This is why transparency, accountability and governance mechanisms

---

[39] Australian Privacy Commissioner, *Business Resource 4: De-identification-of-data-and-information*, available at http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information and the other resources referenced therein. See also UK Information Commissioner's Office *Anonymisation: managing data protection risk code of practice* 2012, Appendix 2, particularly at p 53, available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.

[40] Ibid., see text under sub-heading *Assessing the risks of re-identification*.

are 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. 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. 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 and therefore should not be regarded as disclosed by the customer to the service provider.

Another advantage of the 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,[41]
- 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 and may include such things as:

- quarantining of data;
- access controls that have the effect of quarantining the particular personnel granted access to particular data;
- training, e.g. on security and data minimisation principles;
- personnel background checks;

[41] APP Guidelines, paragraph 8.14, page 6. See also the useful discussion in Australian Privacy Commissioner, Privacy business/agency resource 4: *Sending personal information overseas*, op cit.

- other arrangements for technical and organisational security e.g. staff confidentiality agreements;
- controls over other data brought into the environment;
- limitation to particular project(s);
- restriction on disclosure;
- prohibition on attempts at re-identification;
- measures for destruction of any accidentally re-identified personal data; and
- encryption and key management.[42]

In summary, 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 that 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.

Of course, privacy risk management is but one aspect of prudent information management for outsourcing and offshoring aspects of as-a-service. We now turn to information management as an aspect of information technology risk, including assessment of materiality of risks, associated with as-a-service and traditional (in-house) software supply and integration.

[42] UK Information Commissioner's Office *Anonymisation: managing data protection risk code of practice* 2012, Appendix 2, particularly at p 53, available at https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf, as cited with approval by the Australian Privacy Commissioner, at http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/privacy-business-resource-4-de-identification-of-data-and-information.

8 Identifying risks: as-a-service compared to traditional (in-house) software supply and integration

Although some of the risks associated with outsourcing and offshoring components of cloud services are relatively new, there is already a large and rapidly expanding literature on how to apply various already well accepted risk frameworks to as-a-service offerings.[43] Of course, any assessment of risk must also assess the materiality of identified risks. Often a decision as to the materiality of an identified risk to a business will be determined by three factors: first, the impact of the risk if it eventuates (which often is associated with the business process facilitated by the application being a core business process), secondly, the likelihood or remoteness of the risk, and thirdly, whether the risk is as to non-compliance with applicable laws.

Many organisations consider that any risk of illegality is a material risk, regardless of business impact or remoteness. This is why concerns as to compliance with privacy laws figure so prominently in discussions of risk associated with outsourcing and offshoring: even if the impact of a breach of privacy law may sometimes be assessed as low, many organisations strive to achieve 100 percent risk mitigation as to compliance with all relevant laws, including privacy law.

Given that well accepted risk frameworks have now been adapted to address as-a-service as well as traditional software deployment, many organisations should be able to undertake an objective comparison of the level of risk associated with as-a-service deployment as compared to the level

---

[43] As to privacy information security generally, see U.S. NISTIR 8062 *Privacy Risk Management for Federal Information Systems*, Draft July 2015, available at http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf. As to information security in the cloud, *ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 *Information technology -- Security techniques -- Privacy framework* but adapted for the public cloud computing environment. As to risk management principles, see further AS/NZS ISO 31000:2009 *Risk management - Principles and guidelines* (an equivalent standard to *ISO 31000:2009 Risk management - Principles and guidelines*). There is also useful work by the Cloud Accountability Project of the A4Cloud to create an Accountability Framework "that will be a comprehensive specification for how to create accountability for cloud services, spanning regulatory, legal, technical, business and user issues. See www.a4cloud.eu/cloud-accountability and the many publications available or referenced at that site.

of risk associated with in-house deployments. However, many business customers today are concerned about using as-a-service across national borders. Concerns are sometimes significantly greater than is the case with traditional software supply and integration into a customer's in-house systems.

On its face, this is surprising.

Software integration is often complex and expensive, requiring customisation, integration and interfacing of applications, platform and other systems. Project management of data migration and system switchover is complex and often time-critical. Establishment of disaster recovery capabilities and maintenance of back-ups requires duplication of effort and often expensive outsourcing arrangements that must also be monitored and managed. System security, including from hacking and other external intrusions, must be ensured and maintained in the face of unpredictable and increasingly sophisticated threats. The in-house deployment must be supported and updated, with the risk that a highly customised deployment may be 'orphaned' or otherwise require expensive upgrade and re-architecting of system platform or databases to maintain service levels or compatibility and integration into other systems. The business must project its future business requirements and predict the likely geographical needs of the business over the life of the software deployment. The business must also ensure that its software licences reflect those projections (or can be adjusted at known cost to accommodate them) and that it has a pathway to upgrade and expansion.

As-a-service offerings address many of the risks and concerns associated with software supply and integration into a customer's own systems. As noted in the Australian Government's *Information Security Management Guidelines*, "Outsourcing ICT arrangements can offer a host of benefits, including scalability, elasticity, high performance, resilience and security together with cost efficiency. The range of technology options available through outsourcing of ICT is extensive. It is [however] important to recognise that any ICT arrangements delivered by the agency have a range of risks that an agency is responsible for identifying, assessing and managing. Outsourcing of agencies ICT arrangements can in some circumstances reduce the overall risk associated with delivering these services in house".[44] The Australian Department of Defence notes that the risk assessment of as-a-service deployments depends "on factors such as the sensitivity and criticality of data to be stored or processed, how the cloud service is implemented and managed, how the organisation intends to use the cloud service, and challenges associated with the organisation performing timely incident detection and response. Organisations need to compare these risks against an objective risk assessment of using in-house computer systems which might: be poorly secured; have inadequate availability; or, be unable to meet modern business requirements".[45]

---

[44] Australian Government, *Information Security Management Guidelines*, August 2014 as amended April 2015, page 5 paragraphs 25 and 26, available at http://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentInformationSecurityManagementGuidelines.pdf. See also *Attorney-General's Department, Protective Security Policy Framework: Security risk management* at https://www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Security-risk-management.aspx.

[45] Australian Signals Directorate of the Department of Defence, *Cloud Computing Security for Tenants*, April 2015, available at http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf. See further materials at http://www.asd.gov.au/infosec/cloudsecurity.htm, including for cloud service providers *Cloud Computing Security for Cloud Service Providers* http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Cloud_Service_Providers.pdf.

Implementation Risk

One clear advantage of as-a-service over traditional software supply and integration is significant mitigation of implementation risk. A customer should be able to complete a full evaluation to determine the materiality of these risks and, where determined to be material risks, confirm that an as-a-service offering under consideration fully addresses these material risks before the customer commits to contract with the service provider or commences implementation.

Project management of as-a-service implementation is almost invariably less complex and usually not time critical: the service provider's offering, its integration into the customer's other systems and processes and the expected operation of disaster recovery and other resilience features, can all be fully tested before live processing of customer data. Integration interfaces are defined and stable. If the implementation appears to be compromised in any way, the customer can elect not to proceed to switch-over.

Operating and ongoing risk

As-a-service usually also has clear advantages in mitigating risks of operation during the service term and future-proofing the customer. Security and resilience is usually available at significantly higher levels of assurance than can be readily achieved and maintained in-house deployments. If a service provider does not upgrade its offering over the service term to assure good practice security and reliability of service, the issue is likely to affect and be known across that service provider's customer base and put the service provider's business reputation at risk. Good practice in relation to ongoing security, privacy and resilience management is essential for trust of customers in a service provider and its service offerings. Put simply, a service provider must ensure that services are available, reliable and consistent, including by protection against evolved and escalated forms and levels of intrusion and other security threats.[46]

Flexibility is another key aspect of future-proofing the customer. One feature of attractive as-a-service offerings should be ability for the customer to adjust its system requirements, while maintaining service levels and allowing full scalability and forward and backwards compatibility. As-a-service offerings are often priced on an on-demand or utilisation model: a customer does not need to reliably project its forward business requirements and can flex its requirements up or down without additional capital cost and with significant savings in the event of the customer electing to downsize or reduce scope. Many as-a-service offerings are available globally, thereby enabling business expansion or contraction to meet changes in a customer's operations but with continuation of assured security, resilience and service quality across national borders. The service provider also carries risks of support and upgrade, including management of upgrades or changes to all third party software and platform components and third party vendor relationships. Of course, in the case of traditional software deployments all these other components must be managed by the customer: a significant hidden cost of many in-house implementations.

---

[46] Many on-demand software service providers undergo stringent security procedures such as independent expert verification and certification of controls over information technology and related processes in accordance with the *Service Organization Control (SOC) reporting framework* (SOC 1, 2, 3) pursuant to the Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*, of the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), January 2010. See further the 'SSAE 16 Overview' at http://ssae16.com/SSAE16_overview.html. A global equivalent, International Standards for Assurance Engagements (ISAE) No. 3402, *Assurance Reports on Controls at a Service Organization*, became effective as of 15 June 2011 and is available through http://isae3402.com/ISAE3402_overview.html.

In summary, the deployment of an on-demand software application should be as straightforward as acquisition and integration of many other utility services that are acquired by businesses and that already offer flexibility, reliability, scalability and adaptability: power, communications carriage services, water, banking and payroll services and so on.

Given the re-distribution of many project, implementation and ongoing service risks away from the customer to the service provider, it may be difficult to see why some businesses and government agencies express concern as to the growing trend away from in-house software system implementations towards use of as-a-service. Some concerns relate to unfamiliarity with the business models, commercial terms and technical aspects of this still new way of doing business. Sometimes an issue arises from a perception of loss of control, or loss of transparency, over how a customer's data is handled and secured by the service provider. This issue is particularly heightened with government agencies. Government agencies will reasonably require a high level of assurance that their stewardship of data about citizens will not be compromised through the agency losing control of, and visibility as to, any use or disclosure of that data. The stewardship concern is particularly heightened where as-a-service is provided from outside the jurisdiction of that government. Sometimes concern is expressed as to the relatively simple forms of contract offered by the various providers of as-a-service offerings and limited willingness to negotiate these terms - often the result of a desire to control transaction costs and ensure standardisation of offerings across the customer base.

We now turn to consider further the particular concerns of government agencies.

9 Government agencies: cloud simple, cloud first

The benefits of as-a-service as compared to traditional software supply are reflected in the Federal Government's 'cloud first' policy, first implemented by the former Labor Government and then expanded by the current Coalition Government. The *Australian Government Cloud*

Computing Policy – Smarter ICT Investment states[47]: "non-corporate Commonwealth entities are required to use cloud services for new ICT services and when replacing any existing ICT services, whenever the cloud services are fit for purpose; offer the best value for money, as defined by the *Commonwealth Procurement Rules*[48]; and provide adequate management of risk to information and ICT assets as defined by the *Protective Security Policy Framework"*[49].

The Federal Government's preference for cloud has led to a progressive lightening of review and approval requirements imposed by the Australian Federal Government upon Federal Government agencies before those agencies enter into arrangements for offshoring of provision of services and processing of personal information. New South Wales, Victoria and Queensland State governments have also implemented 'cloud first' policies as mandatory directives for their agencies.[50] A series of 'better practice guides'[51] have been developed at both the Federal and State levels to assist Government agencies to evaluate vendors, service offerings and service agreements for as-a-service offerings.

Government has also emphasised that as-a-service brings new risks that need to be considered and assessed. As stated by the Australian Signals Directorate of the Department of Defence in its *Cloud Computing Security for Tenants*:

> "Organisations need to perform a risk assessment and implement associated mitigations before using cloud services. Risks vary depending on factors such as the sensitivity and criticality of data to be stored or processed, how the cloud service is implemented and managed, how the organisation intends to use the cloud service, and challenges associated with the organisation performing timely incident detection and response. Organisations need to compare these risks against an objective risk assessment of using in-house computer systems which might: be poorly secured; have inadequate availability; or, be unable to meet modern business requirements."[52]

The Australian Government's *Information Security Management Guidelines* summarises new risks of outsourced services as follows:

> "… contracting an outsourced provider for the storage and handling of Australian Government information introduces new risks that must be considered and assessed before

---

47 As to Australian Government cloud policy and guidelines, see https://www.finance.gov.au/cloud/, See *Australian Government Cloud Computing Policy – Smarter ICT Investment Version 3.0*, October 2014 as available at http://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf

48 As available at http://www.finance.gov.au/procurement/procurement-policy-and-guidance/commonwealth-procurement-rules/.

49 As available at https://www.protectivesecurity.gov.au/Pages/default.aspx.

50 See for example NSW Government Cloud Policy 2015 https://www.finance.nsw.gov.au/ict/resources/nsw-government-cloud-policy, For Queensland, see the *Cloud Computing Strategy* available at https://www.qgcio.qld.gov.au/initiatives/cloud-computing. For Victoria, see *Information Technology Strategy, Victorian Government 2016–2020*, available at http://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2016/05/Information-Technology-Strategy-for-the-Victorian-Government-2016-to-2020.pdf. The Victorian Commissioner for Privacy and Data Protection has also released a detailed discussion paper *Cloud Computing in the Victorian Public Sector*, May 2015, available at https://www.cpdp.vic.gov.au/images/content/pdf/Cloud_Computing_in_the_Victorian_Public_sector.pdf; also Victorian Government Solicitor's Office, *Cloud Computing in a Government Context*, at http://vgso.vic.gov.au/sites/default/files/Cloud%20Computing%20in%20a%20Government%20Context%20-%20Speakers%20Notes.pdf.

51 See Australian Government materials at https://www.finance.gov.au/cloud/.

52 Australian Signals Directorate of the Department of Defence, *Cloud Computing Security for Tenants*, April 2015, available at http://www.asd.gov.au/publications/protect/Cloud_Computing_Security_for_Tenants.pdf.

a decision is made to engage a provider. The physical location of stored information also represents a series of new risks and vulnerabilities.

Entering into an ICT arrangement in which information is held offshore, either by the contractor or subcontractor, can have additional risks. For example, while the term 'Cloud' implies that the information is 'not fixed'; all information stored in a Cloud service is physically located somewhere in a data centre or multiple data centres. Below is a list of factors that should be considered prior to entering into an offshore ICT arrangement.

- the nature of the legal powers to access or restrict access to data
- complications arising from data being simultaneously subject to multiple legal jurisdictions
- the lack of transparency (and reduced ability to directly monitor operations), and
- the difference in the business and legal cultures in other nations."

Like Australia, most foreign jurisdictions have legislative powers that allow access to communications and stored information for the purposes of law enforcement and national security. In some cases these laws allow international law enforcement and national security agencies to access information held overseas or in Australia."[53]

Government agency customers may also have specific statutory obligations that must be met.[54] For example (and together with the *Privacy Act 1988* (Cth)), a number of Federal laws affect how Australian Government agencies create and manage records and information. Some of these laws, including the *Privacy Act 1988* itself, the *Archives Act 1983*, the *Australia Information Commissioner Act 2010* and the *Freedom of Information Act 1982*, apply to most Australian Government agencies. Other laws are agency specific or information specific. Agency-specific legislation can cover diverse requirements. For example, a statute may require certain information to be created, specify the format in which it is to be kept, how or where it is to be captured, and how and to whom it may be disclosed. State and Territory laws affect how Government agencies of the particular State and Territory create and manage records and information and in some (relatively rare) cases create geographical or territorial limits as to where data may be processed or stored.

For example, the *My Health Records Act* 2012 (Cth)[55] limits key participants in the MyHealth Record system that record information for the purposes of that system, or that have access to information relating to such records, from processing or handling information relating to the records outside Australia or causing or permitting another person to process or handle information relating to the records outside Australia. However, the MyHealth Record system operator (but not other participants) is specifically authorised, for the purposes of the operation or administration of

---

53 Australian Government, *Information Security Management Guidelines*, August 2014 amended April 2015, page 5 paragraphs 27 and 28.

54 For a useful and quite comprehensive review of the regulatory environment affecting implementation of cloud services by Australia businesses and government agencies, see Australian Government Department of Communications, *Cloud Computing Regulatory Stocktake Report Version 1*, June 2014, available at https://www.communications.gov.au/publications/cloud-computing-regulatory-stock-take-report.

55 Section 77, available at https://www.legislation.gov.au/Series/C2012A00063..

that system, to process and handle such information outside Australia, provided that the information is not personal information in relation to a consumer or a participant in the MyHealth Record system or otherwise identifying information of an individual or entity.

By comparison, private sector entities are generally less regulated. With the exception of relatively few sector specific rules, the operation of the *Privacy Act 1988* and any contractual restrictions that an entity has accepted, Australian corporations and other private sector entities that conduct business in Australia may exercise their respective business discretion as to where, how and by whom their business information, including any personal information about individuals that is collected and held either by them or on their behalf, is processed and stored.

In summary, although the application of the Privacy Act requirements is broadly the same, the requirements applying to use of as-a-service offerings government agencies are generally more prescriptive and more extensive than the requirements applying to businesses. There are also a range of agency specific restrictions that need to be addressed. However, relevant requirements and restrictions have now been extensively analysed in whole of government and sector-specific guidelines and support materials from the Federal government and from individual State and Territory governments.[56]

Provision of banking, insurance and other financial services is probably the most highly regulated business sector in Australia (outside environmentally sensitive projects). Given the particular, higher level of restrictions that apply to the financial services sector, we now turn to consider those requirements.

10 APRA regulated institutions: compliance with requirements for 'material business activities'

In section 8 of this White Paper we noted that although some of the risks associated with outsourcing and offshoring components of cloud services are relatively new, there is extensive literature on how to apply already well accepted risk frameworks to as-a-service. However,

[56] See the materials as available at www.finance.gov.au/cloud and those referred to in footnote 50 above.

looking beyond strict compliance with law to rate the materiality of non-legal risk, often there will be legitimate disagreement and debate as to how to set a materiality threshold.

Sometimes materiality of as-a-service applications is assessed having regard to whether a business process facilitated by a particular as-a-service application is a 'core business process'. The Australian Prudential Regulation Authority (**APRA**) applies its *Prudential Standard CPS 231 Outsourcing* (last revised January 2015) to any material business activity' of a regulated institution, being:

> "….[a business activity] that has the potential, if disrupted, to have a significant impact on the APRA-regulated institution's or group's business operations or its ability to manage risks effectively, having regard to such factors as:
>
> (a) the financial, operational and reputational impact of a failure of the service provider to perform over a given period of time;
>
> (b) the cost of the outsourcing arrangement as a share of total costs;
>
> (c) the degree of difficulty, including the time taken, in finding an alternative service provider or bringing the business activity in-house;
>
> (d) the ability of the regulated institution or member of the group to meet regulatory requirements if there are problems with the service provider;
>
> (e) potential losses to the regulated institution's customers and other affected parties in the event of a service provider failure; and
>
> (f) affiliation or other relationship between the institution or group and the service provider."[57]

Many activities of institutions regulated by APRA will therefore not be 'material business activities'. But how do you identify which activities are or are not material? Sometimes it will be obvious that a particular activity is core to the activities of a regulated institution: clearing and settlement of payments by or on behalf of banks is one example. But one customer's proposed use of an as-a-service application in a particular business process may be a 'material business activity' for that customer but not for another customer. Text editing, formatting and content publishing capabilities are clearly a 'material business activity' for a publishing house, but probably are not for a bank. Customer relationship management (CRM) capabilities will be

---

[57] Australian Prudential Regulation Authority Prudential Standard CPS 231 *Outsourcing* January 2015, paragraph 14, available at http://www.apra.gov.au/CrossIndustry/Documents/141120-CPS-231.pdf. See also APRA Prudential Practice Guide CPG 235 *Managing Data Risk* September 2013 (http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Practice-Guide-CPG-235-Managing-Data-Risk.pdf); Prudential Practice Guide PPG 234 *Management of security risk in information and information technology* (http://www.apra.gov.au/crossindustry/documents/ppg_ppg234_msrit_012010_v7.pdf) and *CPS 220 Risk Management* and *Prudential Practice Guide* http://www.apra.gov.au/CrossIndustry/Documents/Prudential-Standard-CPS-220-Risk-Management-January-2015.pdf; SPG 231 *Outsourcing, July 2013*. Although Prudential Standard *CPS 231 Outsourcing* is now the primary regulatory instrument, Prudential Practice Guide 235 remains a current APRA published instrument and provides guidance and examples of what APRA considered to be material for the purpose of (then) APS 231 and further details on many other aspects of then APS 231, now CPS 231. As to financial services institution (FSI) regulations impacting FSI take-up of cloud services in other Asia Pacific jurisdictions, see Asian Cloud Computing Association, *Asia's Financial Services: Ready for the Cloud*, March 2015, available at http://www.asiacloudcomputing.org/research/fsi2015.

material for some applications of CRM in some businesses, such as customer response contractors and direct marketing houses, but may not be material for a bank. The scale of the deployment and the degree of dependency will each be relevant. A pilot or limited implementation may not have sufficient scale to be material. Further, one use of an as-a-service offering by a customer may be a 'material business activity' while another is not. For example, a CRM application may be used for vendor management or customer response or both: one use might be a material business activity and other not.

It is appropriate to pause here to reflect on what this additional level of prudential regulation is endeavouring to achieve. In section 7 of this White Paper we concluded all 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. We noted that privacy risk management is but one aspect of prudent information management for outsourcing and offshoring aspects of as-a-service. In section 8 we noted that many organisations consider that any risk of illegality is a material risk, regardless of business impact or remoteness, and rightly strive to achieve 100 percent risk mitigation as to compliance with all relevant laws, including privacy law. So the question now under consideration is when the additional layer of prudential regulation of material business activities of regulated institutions should apply, not whether all businesses should achieve compliance with all laws, including privacy regulation.

The inherently business-process-specific nature of any assessment of whether an activity is a 'material business activity' is also illustrated by ASX Clear Operating Rules *Guidance Note 9 – Offshoring and Outsourcing.*[58] This guidance note applies to impose particular requirements as to outsourcing and offshoring by ASX market participants such as trading houses and clearing houses operating in the ASX electronic securities exchange. The ASX states its "higher expectations around the documentation and supervision of material offshoring and outsourcings arrangements, relative to those that are not material" and that offshoring and outsourcings of a "material business activity" are material.[59] The ASX states that a "material business activity" of a trading house or clearing house is one that has the potential, if disrupted, to have a material impact on the ability of that participant to comply with its obligations under the relevant ASX Operating Rules. The ASX continues:

> Examples of arrangements that ASX would regard as material offshoring or outsourcing arrangements (as the case may be) include:
>
> - the offshoring or outsourcing of the operation of core IT systems used in a participant's clearing activities;
> - the offshoring or outsourcing of core clearing functions and processes; and
> - the offshoring or outsourcing of a participant's business continuity and disaster recovery arrangements.

---

[58] ASX Clear Operating Rules June 2015, *Guidance Note 9 Offshoring and Outsourcing*, February 2015. http://www.asx.com.au/documents/rules/asx_clear_guidance_note_09.pdf.

[59] *Ibid.*, at section 6, page 5.

Examples of offshoring or outsourcing arrangements that ASX generally would not regard as material include:

- the engagement of an external identity verification service or credit service to verify the identity or creditworthiness of new clients on an ongoing basis;
- the provision of accounting, legal or compliance services on an ongoing basis by staff located offshore and employed by an overseas related body corporate;
- the engagement of a professional adviser (such as an accountant, lawyer or management consultant) to provide professional advice on an ongoing basis; and
- the engagement of a specialist compliance consulting firm to provide compliance services on an ongoing basis.[60]

So what is the higher level of regulation that is applied by the prudential regulator to those cases where there is an outsourcing of a material business?

Some of the requirements are those that we have already identified as applying to any prudent customer: in particular, proper assessment of data risk and implementation of good information management. Some requirements are additional and specific to outsourcing and offshoring respectively of a material business activity by an APRA-regulated institution. An APRA regulated institution must consult with APRA prior to entering into any offshoring agreement involving a material business activity so that APRA may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the regulated institution's risk management framework.[61] The institution must notify APRA of any outsourcing agreement relating to material business activities "as soon as possible after entering into an outsourcing agreement, and in any event no later than 20 business days after execution of the outsourcing agreement".[62] A regulated institution must ensure it has sufficient and appropriate resources to manage and monitor an outsourcing involving a material business activity, including "at a minimum" maintaining appropriate levels of regular contact with the service provider (ranging from daily operational contact to senior management involvement) and a process for regular monitoring of performance under the agreement, including meeting criteria concerning service levels.[63] The outsourcing agreement in relation to a material business activity of a regulated institution must address:

(a) the scope of the arrangement and services to be supplied;

(b) commencement and end dates;

(c) review provisions;

(d) pricing and fee structure;

---

60 Ibid, section 6, page 5.

61 APRA Prudential Standard CPS 231 *Outsourcing*, January 2015, paragraph 36.

62 APRA Prudential Standard CPS 231 *Outsourcing*, January 2015, paragraphs 34 and 35.

63 APRA Prudential Standard CPS 231 *Outsourcing*, January 2015, paragraph 38.

(e) service levels and performance requirements;

(f) audit and monitoring procedures;

(g) business continuity management;

(h) confidentiality, privacy and security of information;

(i) default arrangements and termination provisions;

(j) dispute resolution arrangements;

(k) liability and indemnity;

(l) sub-contracting;

(m) insurance; and

(n) where applicable, offshoring arrangements (including through sub-contracting)[64].

A sometimes difficult to implement requirement in relation to as-a-service arrangements is that to ensure transparency to APRA, an outsourcing agreement involving a material business activity must include a clause that allows APRA access to documentation and information related to the outsourcing arrangement, including the right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor. The standard also states that APRA expects service providers to cooperate with APRA's requests for information and assistance.[65]

All but the last of the above requirements apply to any outsourcing of a material business activity by a regulated institution, whether or not there is any offshoring element. In the case of offshoring, a regulated institution must also consult with APRA prior to entering into any offshoring agreement involving a material business activity "so that APRA may satisfy itself that the impact of the offshoring arrangement has been adequately addressed as part of the regulated institution's risk management framework".[66] For regulated entities, that risk management framework should be developed in accordance with APRA prudential guidance for data management and in particular Prudential Practice Guide *PPG 234 - Management of security risk in information and information technology*[67] and Prudential Practice Guide *CPG 235 – Managing Data Risk*.[68]

Most of the risks that APRA identifies for regulated entities to manage through control processes are common to both in-house implementations and outsourcing in relation to a material business activity and therefore not unique to either outsourcing generally or outsourcing with an off shore element. However, APRA also identifies certain additional possible risks of outsourcing or

---

64 APRA Prudential Standard CPS 231 *Outsourcing*, January 2015, paragraph 26.

65 APRA Prudential Standard CPS 231 *Outsourcing*, January 2015, paragraphs 31 to 33.

66 APRA Prudential Standard CPS 231 *Outsourcing* January 2015, paragraph 36.

67 See footnote 57 above.

68 See footnote 57 above.

offshoring that are associated with any diminution of data life-cycle controls. APRA therefore states that a regulated entity should "apply a cautious and measured approach when considering retaining data outside the jurisdiction it pertains to", in particular focussing upon any change in the effectiveness of data lifecycle controls.[69] In the case of both outsourcing and offshoring, these controls may be diminished through "control framework variations, lack of proximity, reduced corporate allegiance, geopolitical risks and jurisdictional-specific requirements".[70] APRA suggests various ways in which regulated entities may ensure that these controls are maintained, including APRA's expectations that to ensure appropriate lifecycle controls are in place in an outsourced or offshored environment, a regulated entity should be able to demonstrate:

(a) ability to continue operations and meet core obligations following a loss of services;

(b) maintenance of the quality of critical or sensitive data;

(c) compliance with legislative and prudential requirements; and

(d) a lack of impediments (from jurisdictional hurdles or technical complications) to APRA being able to fulfil its duties as prudential regulator (including timely access to data in a usable form). In the normal course, APRA will seek to obtain whatever information it requires from the regulated institution; however, the outsourcing agreement must include the right for APRA to conduct on-site visits to the service provider if APRA considers this necessary in its role as prudential supervisor. APRA expects service providers to cooperate with APRA's requests for information and assistance. If APRA intends to undertake an on-site visit to a service provider, APRA will normally inform the regulated entity of its intention to do so.[71]

---

69 Prudential Practice Guide *PPG 234 - Management of security risk in information and information technology*, at paragraph 48, page 13.

70 Prudential Practice Guide *CPG 235 – Managing Data Risk* at paragraph 47.

71 Prudential Standard *CPS 231 Outsourcing* January 2015, at paragraph 31.

11 Conclusions

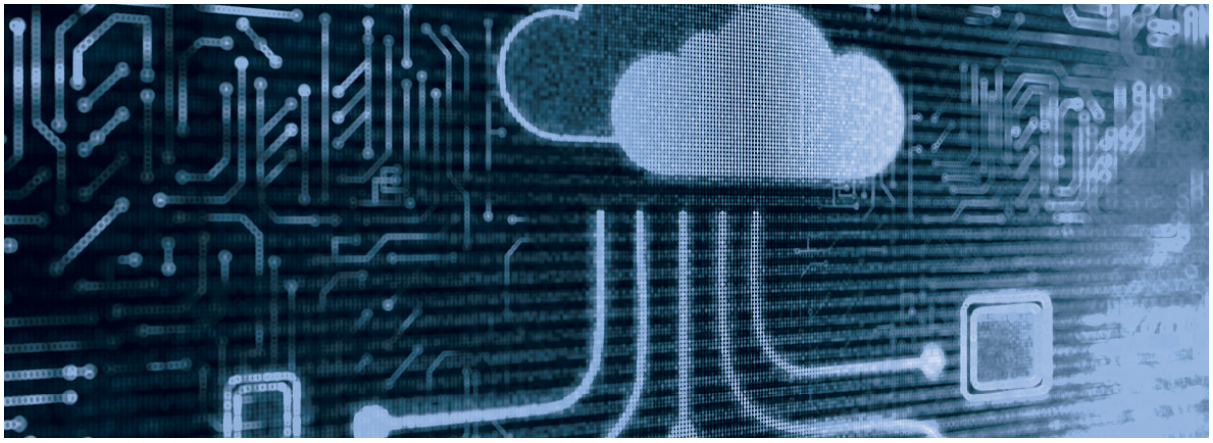
This White Paper has examined why, properly implemented, use of as-a-service by a customer should reduce, rather than enhance, risk as compared to traditional software in-house deployment. However, there are legitimate questions that arise from any possibility of personal information moving out of the effective control of the customer who remains responsible for the stewardship of personal information that it collected. There are also legitimate questions that arise from the possibility that personal information collected by a customer might move out of jurisdictions that have effective privacy regulation and enforcement. Although these questions can be addressed through appropriate contractual restrictions and accompanying transparency, accountability and governance mechanisms, some service providers appear to be unwilling to make these commitments, to provide appropriate transparency as to their activities, including as to reporting of any relevant incidents and as to their remediation, or to implement accountability and governance frameworks consistent with the level and materiality of privacy risk.

All customers should carefully evaluate each service provider and ensure that certain contractual provisions are put in place and that there are the appropriate transparency, accountability and governance mechanisms to ensure that privacy risk management is verifiably and reliably implemented, and to ensure that those customers are able to continue to comply with their obligations under the Privacy Act notwithstanding the use of a contracted service provider. Privacy risk management is but one aspect of prudent information management for outsourcing and offshoring aspects of as-a-service. Many organisations consider that any risk of illegality is a material risk, regardless of business impact or remoteness, and rightly strive to achieve 100 percent risk mitigation as to compliance with all relevant laws, including privacy law. With appropriate diligence, compliance with relevant Australian laws can be achieved, except for those unusual customers where offshoring of their activities is expressly prohibited.

Government agencies, and regulated institutions outsourcing material business activities, are subject to additional requirements (discussed in sections 9 and 10 respectively of this White Paper). These additional requirements can also be addressed by many well designed as-a-service offerings and service providers that are willing to provide the required transparency, accountability and governance commitments.

Our conclusions are also summarised in the Key Points section at the front of this White Paper.

Peter Leonard
Gilbert + Tobin Lawyers
1 September 2016



ANNEXURE: AS-A-SERVICE CONTRACTS: PRIVACY RELATED PROVISIONS FOR CONSIDERATION

1	Privacy commitments	Service provider (SP) commits to meet specific privacy obligations as expressly stated in the contract or by reference to the APPs. SP commits to access personal information (PI) only for the permitted purpose (as clearly stated on the contract – e.g. at the specific request of a customer representative view only access of specific information for the purpose of provision of customer support requested by the customer). SP agrees to not separately copy, use or disclose the same in any unencrypted form, such use to be only during the term and for the benefit of the customer.
2	Security	SP to permit access to PI only be authorised support personnel and to secure PI against external intrusions and access by unauthorised personnel of service provider. Encryption requirements understood and assurance that decryption tools appropriately managed. Monitoring of access to PI to be in accordance with good service provider practice. Access controls to be updated during the term in accordance with good service provider standards.
3	Transparency	Any relevant unauthorised access to PI or disclosure of PI is to be reported promptly when reasonably suspected or discovered. Countries where data is to be stored (including back-ups and resilience sites) are specified and always known.

4	Governance, accountability and verification	If any unauthorised access or disclosure of PI is reasonably suspected or discovered, root cause analysis is to be performed and remediation pathway to be agreed after consultation with customer. Contractual controls as to PI are supported by reporting and certifications as required. Check match of reporting and certifications and other governance and accountability measures to the customer's internal information management processes, as appropriate to ensure prudent end-to-end information management
5	Business continuing management	Resilience measures and back-up procedures are known and defined, so PI is secured in all forms in which it is held.
6	Sub-contracting	Any sub-contracts that might involve sub-contractor access to PI are known and appropriately controlled, so that the customer's risk assessment is end-to-end and not compromised through a service provider's use of subcontractors that might use or disclose PI.
7	Confidentiality of other commercial-in-confidence customer information and privacy of PI	Does the coverage of the contract provisions dealing with confidential information (including non PI) give the protection the customer needs for commercial-in-confidence customer information, in addition to the specific privacy protective provisions addressing handling of PI?
8	Tailoring	Are there sector-specific, data-specific or customer-specific restrictions that should be included as contract terms? If so, tailor terms to suit.

GILBERT+TOBIN

Sydney
Level 35, Tower 2
International Towers Sydney
200 Barangaroo Ave
Barangaroo NSW 2000

Melbourne
Level 22, 101 Collins Street
Melbourne VIC 3000

Perth
1202 Hay Street
West Perth WA 6005

GTLAW.COM.AU