Time to get off cloud 9 and start thinking about privacy

Caroline James *LEWIS HOLDWAY LAWYERS*

In an ever-evolving global and IT based market, active participants must understand privacy law considerations for Australian businesses which seek to store data, including personal information about individuals, in a cloud operated by an external cloud computing provider.

Key takeaways

- Storing personal information in an externally operated cloud computing service is generally considered to be disclosure for the purposes of Australian Privacy Principles (APPs) 6 and 8. APP entities should obtain consent from the individuals concerned before seeking to store data in this way.
- APP entities should consider APP 11 when negotiating an engagement agreement with a cloud computing provider, to ensure that storage methods are adequately secure and that personal information is destroyed or de-identified after use.
- The mandatory notification provisions under the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (Privacy Amendment Act) may apply to both APP entities and cloud computing providers, but ideally the APP entity should be the party that determines whether a reasonable person would conclude that serious harm will likely result from an eligible data breach.

Background

The Privacy Act 1988 (Cth) (Privacy Act) and the APPs regulate the collection, use and storage of personal information about individuals with whom APP entities deal. The recent ubiquitous use of cloud computing has gained the attention of businesses who are anxious to maintain legislative compliance in this area. Many business operators are familiar with their privacy obligations where they relate to information that is stored on-site. However, the waters can become murky when operators seek to store data, including personal information about individuals, in an externally based cloud. In practice, we have found a number of matters helpful for a business's key personnel to consider when seeking to engage cloud computing providers. Some of these areas are:

- the type of cloud system to be used and how this differs from other systems;
- the types of information that the business wishes to store in the cloud;
- the locations in which the data is stored in the cloud and any foreign laws that apply;
- the security measures in place to protect information;
- the right to be notified in the event of any unauthorised access to or disclosure of personal information; and
- the right to have personal information returned once the agreement with the provider has concluded.

What is cloud computing?

"Cloud computing" is used to describe the use of third party services for managing computing systems online. In the past, organisations often managed computer networks in-house, but it was frequently the case that they lacked the necessary technological expertise to do so successfully.[1] Cloud computing companies identified a need in the market for businesses to be freed of computer network concerns and developed appropriate storage and management services.

There are three basic types of services offered by cloud providers — Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Generally, the term "cloud computing" refers to SaaS, the most popular cloud computing system.

Each system requires users to manage the computer hardware and software with varying levels of engagement, as set out below:[2]

- The SaaS system provides both the server hardware and software to an organisation, relieving it of the complications of managing an IT system. It is considered to be "the top of the cloud stack".[3]
- The PaaS system provides the business with a platform, such as Microsoft Office 365, to run applications. The PaaS cloud service provider manages and upkeeps the system and provides tools such as Java, but it is the business's responsibility to select applications that run on the platform.

- The IaaS system provides a business with the same features as PaaS, but the business is fully responsible for the control of the leased infrastructure. IaaS is often seen as the computing system of the business that is not actually owned by the business. Using IaaS generally requires significant technical expertise.

The level of control that the cloud provider has over the information depends on the system used. For example, under the IaaS model, information is simply stored in the cloud. In contrast, the SaaS model allows the service provider to access and retain the information provided by a business.[4] Naturally, privacy implications also vary depending on the model used.

Disclosure

A question frequently asked by APP entities is whether the storage of data on a third party cloud is "disclosure" for the purposes of the Privacy Act. Although some organisations that transfer information to third party contractors are not deemed to have disclosed that information (because the contractor is considered to be a part of that organisation), the Office of the Australian Information Commissioner (OAIC) generally considers cloud service providers to be separate organisations.[5] Whether disclosure has occurred will depend on the type of cloud model used. For example, the IaaS model does not require the transfer of information to a third party provider because the information usually remains under the control of the business. In contrast, information is disclosed under the SaaS model because of the control given to the service provider over the information.

The APP Guidelines specify that although disclosure does not occur under the IaaS model, the third party cloud computing provider is still "using" the information for the purposes of the Privacy Act. In these circumstances, APP entities should be aware that any actions undertaken by the cloud provider on behalf of the APP entity will generally be treated as having been undertaken by the actual APP entity.[6]

APP 6 provides that APP entities must not disclose personal information that was collected about an individual for a particular purpose unless the individual concerned has consented to that disclosure, or the purpose for which the information is being disclosed is related to the purpose for which it was collected (the original purpose), and the individual would reasonably expect the entity to use or disclose the information in this way. If the personal information was collected for the original purpose of obtaining an individual's contact details, for example, it is questionable whether disclosing it for the purpose of data storage management is significantly related to the original purpose. In any event, it is recommended that consent is obtained prior to the disclosure of information to a third party cloud computing provider.

A further obligation is imposed on APP entities that seek to disclose personal information outside Australia: APP 8 requires them to take reasonable steps to ensure that the overseas recipient does not breach the APPs. APP 8.2 provides exemptions to this fairly onerous obligation, one of which being if the entity reasonably believes that the recipient of the information is subject to a law that will protect the information in a way that is substantially similar to the APPs and the individual is able to take action to enforce that law, and another being if the individual consents to the disclosure after being informed that this protection does not apply.

This means that an APP entity seeking to *disclose* information to a cloud computing provider should:

- check the locations in which the data is stored; and
- if the cloud computing provider is located in Australia, obtain consent from the individual to the disclosure; or
- if the information is sought to be disclosed to countries whose privacy laws do not afford similar protection to the Privacy Act, ensure that that appropriate privacy related obligations are placed on the service provider or its affiliates, or obtain consent from the individual after notifying them that equivalent protections do not apply.

Many APP entities obtain consent for both national and international disclosure via their privacy policy.

Security

APP 11.1 provides that if an APP entity holds personal information, it must take reasonable steps to protect the information from:

- misuse, interference and loss; and
- unauthorised access, modification or disclosure.

Businesses should have security of personal information at the forefront of their considerations when seeking to engage a cloud computing provider. The much publicised hackings of various celebrities' mobile telephones in and around 2014 generated significant concern about the security of information in the cloud. However, Apple maintained that the "accounts were compromised by a very targeted attack on usernames, passwords and security questions", rather than the cloud itself actually being hacked.[7] One of the advantages of cloud computing is the way in which it is said to better protect personal information. For example, the SaaS system is reported to manage information securely by implementing network monitoring and anti-virus software,[8] and many cloud

systems use encryption methods to convert information into a code which can only be identified through the use of the encryption key. However, cloud computing servers use the same operating systems and applications as physical servers and may similarly be subject to hacking.[9] It is not guaranteed that all providers have proper security arrangements, so key personnel should undertake their own due diligence to satisfy themselves that the information is adequately protected.

APP 11.2 requires an APP entity which no longer needs the information for the purpose for which the information was used or disclosed to take reasonable steps to destroy or de-identify the information. The OAIC outlines that reasonable steps depend on a number of factors such as the nature of the information, the data handling practices and the ease with which a security measure can be implemented. Although an advantage of cloud computing is its provision of multiple backups and the way it helps protect against data loss, this can make it more difficult for APP entities to confirm that all copies of the information have been permanently destroyed or de-identified after their required use.[10]

Ideally, APP entities should request access to the information while it is stored in the cloud, and that the cloud provider returns the information when the engagement terminates, in addition to requesting that any backups are destroyed. APP Guideline 11.37 provides that if an APP entity has instructed a third party cloud provider to irretrievably destroy the personal information it holds on behalf of that organisation, taking reasonable steps to destroy or de-identify the information could include verifying that this has occurred. However, APP entities should be aware that negotiating such a provision with the provider may not be possible, and if this is the case, the APP entity risks breaching APP 11.2. APP entities could attempt to mitigate the risk by notifying individuals that remaining copies of documents may persist for a certain period of time due to the backup systems used, which is the approach taken by Google Docs.[11]

Mandatory notification (eligible data breaches)

On 13 February 2017, the Commonwealth Government passed the Privacy Amendment Act which takes effect on 22 February 2018. This new law will require entities governed by the Privacy Act to notify affected persons and the Privacy Commissioner if an "eligible data breach" occurs. This happens where there is either:

- unauthorised access to, or unauthorised disclosure of, personal information, and a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to which it relates; or
- loss of personal information, making unauthorised access to or unauthorised disclosure of the information likely to occur, and if it were to occur, it would be likely to result in serious harm.

The notice must include recommendations about the steps individuals should take in response to the data breach. However, if the information holder acts quickly to mitigate an eligible data breach, and the breach is not likely to result in serious harm, no notification needs to be made.

Section 26WC of the Privacy Amendment Act says that if an APP entity has disclosed personal information to an overseas entity, the overseas entity is deemed to hold the information for the purposes of the notification section. A relevant consideration is whether information that is disclosed for the purposes of cloud computing is still "held" by the APP entity. In practice, the OAIC recognises the difficulty around the terms "hold", "disclosure" and "use", and says that the best approach is for the APP entity to take reasonable steps to ensure the APPs and the Privacy Act are complied with.[12]

Section 26WJ of the Privacy Amendment Act states that where more than one entity holds the same personal information, only one of those entities need to make the requisite notification. APP entities should negotiate with cloud providers to determine who will make the notification, which should occur well in advance of a breach where possible. APP entities should also seek to ensure that the provider notifies them as soon as possible if there is unauthorised access to or disclosure of personal information stored in the cloud, or if any personal information is lost from the service provider's possession. This places the onus on the APP entity to determine whether a reasonable person would conclude that serious harm is a likely result from the unauthorised access or disclosure of personal information. Issues could arise if the cloud provider is responsible for determining whether a breach is likely to result in serious harm and elects not to alert the APP entity, but the APP entity would have considered that the data breach actually warranted notification. In this case, the APP entity would be liable for the failure to notify and could incur significant civil penalties.

Conclusion

The huge volume of data that many businesses collect makes the storage of that information in a third party cloud an attractive option. It does, however, necessitate the consideration of how privacy laws apply to businesses that choose to store information in this way. This article has outlined some of the matters which Australian businesses should be aware of when seeking to engage a cloud computing provider.

Caroline James
Lawyer
Lewis Holdway Lawyers
CarolineJ@lewisholdway.com.au
www.lewisholdway.com.au

Footnotes

1. S Srinivasan *Cloud Computing Basics* Springer 2014 p vii.
2. Above n 1, at p 11.
3. B Furht and A Escalante (eds) *Handbook of Cloud Computing* Springer, USA 2010 p 12.
4. R Buyya, J Broberg and A Goscinski (eds) *Cloud Computing Principles and Paradigms* A John Wiley & Sons Inc, New Jersey 2011.
5. A Solomon, "Privacy and the cloud" speech delivered at the Cloud Computing Conference and Expo (9 September 2010) www.oaic.gov.au/privacy-law/privacy-archive/privacy-speeches-archive/privacy-and-the-cloud.
6. Office of the Australian Information Commissioner *Australian Privacy Principles Guidelines* (1 April 2015) Chs 8.14 and 8.15.
7. D Love, *Apple on iCloud Breach: It's Not Our Fault Hackers Guessed Celebrity Passwords*, 9 February 2014, www.ibtimes.com/apple-icloud-breach-its-not-our-fault-hackers-guessed-celebrity-passwords-1676268.
8. Above n 1, at p 12.
9. Above n 3, at p 12.
10. Office of the Australian Information Commissioner "Guide to information security: 'reasonable steps' to protect personal information" (April 2013) www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf.
11. Above n 5.
12. Office of the Australian Information Commissioner, *Privacy Business Resource 8: Sending Personal Information Overseas*, May 2015, www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-8.