COMPUTERS & LAW

Journal for the Australian and New Zealand Societies for Computers and the Law

Editors: Isaac Lin and Daniel Thompson

ISSN 08117225

Number: 84

January 2013

Privacy obligations of data processors

A conceptual gap affecting Australia's cloud industry

By James North and Daniel Thompson

James North *is a Partner at Corrs Chambers Westgarth.*

Daniel Thompson *is Lawyer at Corrs Chambers Westgarth.*

Introduction

As cloud computing continues to burgeon in Australia, Australian privacy laws remain poorly adapted to the cloud industry, notwithstanding the recently passed reforms to the *Privacy Act 1988* (Cth). This article discusses the difficulty faced by both onshore and offshore cloud providers in determining regulatory obligations under the Privacy Act, and argues that such regulatory uncertainty in data privacy may detriment Australia's prospects of becoming a data-hub in the Asian region.

As global technology heavyweights target Asia for deployment of data centre infrastructure and regional bases, the contest for best jurisdiction is heating up. Recently, Australian Minister for Broadband, Communications and the Digital Economy Stephen Conroy has been outspoken, both at home and abroad, as a proponent of Australia becoming a regional data hub. For some time Singapore has positioned itself to be the preferred data-host for the Asian region, including by pursing legal reforms amongst other government initiatives to develop a regulatory environment attractive to international data-hosts. While Singapore has succeeded in luring some of the world's largest technology companies and establishing itself as a front-runner for Asia's most attractive data-hub, growing interest and investment in Australian-based data centre infrastructure marks Australia as a viable alternative.

However, Australia suffers several disadvantages as a potential regional data-hub, including high telecommunications costs, its lack of connectivity abroad, and its location on the periphery of Asia, which results in higher network latency when servicing the Asian market than data centres in Singapore or Hong Kong. One factor trumpeted by the Australian Government as being in Australia's favour is the stable political and regulatory environment.

In this issue

From the editors...

In this issue, James North and Daniel Thompson consider the absence of the conceptual distinction between data controllers and data processors under Australian privacy law. Unlike many foreign privacy regimes, Australia does not distinguish between entities that control personal information and entities that process personal information on the behalf of a controlling entity. In the context of foreign investment in data centre infrastructure across Asia, James and Daniel consider the implications of this conceptual omission, both to Australia's growing cloud industry, and Australia's prospects of becoming a data-hub in the Asian region.

Monique Donato's article, '"Status Update", Liability for third party comments beyond Advertising Codes', discusses potential liability for third party comments on company Facebook pages in respect of both the Australian Association of National Advertisers Code of Ethics and under the law. In light of the recent decisions by the Australian Advertising Standards Board and the New Zealand Advertising Standards Authority's guidance note, the regulatory response is outlined together with a consideration of the means in which companies may cope with these newfound risks of liability.

The final part of Dr Pamela Gray's and Xenogene Gray's book review of Peter Hinssen's book, The New Normal, concludes their analysis of the implications of a changing social and technological landscape for the legal profession and the future of legal services.

Continued from page 1

Indeed, Australia's regulatory environment has been ranked fairly high against the 13 other jurisdictions in the Asia Cloud Computing Association's 2012 Cloud Readiness Index (as shown in the table below).

Data privacy has become a central regulatory issue for trans-border data residency and cloud computing, and numerous countries in the region (including Singapore and Australia) have recently introduced or reformed laws to meet the challenges of cloud computing. Legal regimes protecting privacy must ensure that suitable legal obligations exist to protect personal or sensitive information, but in a cloud environment, such regimes must ensure there is clarity as to who such obligations apply (for instance, do obligations apply to cloud service providers, or the cloud provider's customers who control personal information uploaded through the cloud service), and should also ensure that regulation does not unnecessarily impede the cross-border flow of information. The methodology applied to the 2012 Cloud Readiness Index with respect to data privacy considered not only the level of protection and enforcement for personal data, but also the harmonisation of national privacy regimes with regional best practice, including the principles set out in the APEC Privacy Principles.

Although Australia ranks fairly well against its neighbours in terms of data privacy, this article discusses the absence of a key conceptual distinction in Australian privacy law that exists in many foreign privacy regimes, including in Singapore's recently introduced *Personal Data Protection Act 2012*, and that is contained in the APEC Privacy Principles – namely, the distinction between a 'data controller', who has control over personal information and the purposes for which such information is used, and a 'data processor', who processes personal information at the direction and on the behalf of a 'data controller'.

The lack of this distinction in Australia's privacy regime makes it difficult for cloud computing providers (as processors of data) to determine their privacy obligations, and this regulatory uncertainty may potentially inhibit foreign investment in Australia's cloud industry and stymie Australian regional data-hub ambitions.

Table 1 – 2012 Australia and Singapore regulatory rankings

	Data Privacy	Data Sovereignty	IP Protection	Freedom of Information Access	Regulatory ranking
Australia	7.5 (equal 3rd)	7.3 (4th)	7.6 (equal 3rd)	8.6 (5th)	4th
Singapore	4.5 (11th)	8.1 (1st)	8.7 (1st)	7.1 (equal 11th)	7th
Top score / average score	9.0 / 6.3	8.1 / 5.3	8.7 / 6.3	8.9 / 7.8	

Data controllers and data processors

Cloud providers as data processors

Organisations that collect personal information for their own use, for instance, from their customers, are generally subject to a broad range of privacy obligations, both under the Privacy Act and under foreign privacy laws. These organisations 'control' personal information, in that they collect the information for their own purposes, may access, update and use the information, and generally have some level of relationship with the individuals concerned.

In contrast, a cloud services provider will not have control over personal information stored or processed by customers on its servers, and will likely not have visibility into the data to determine whether it contains personal information. A cloud provider may provide cloud based software, platforms or infrastructure as a service to customers, who then may use such services to upload or handle personal information. The cloud provider does not determine the purpose for which the personal information will be used, will not generally access, use, or alter such personal information themselves (indeed they may not be able to access such information due to encryption of the data), and will not have a direct relationship with any of the individuals concerned. Rather, cloud providers process their customer's data in accordance with the directions of the customer.

Many foreign privacy regimes differ from Australia's Privacy Act in that they distinguish between data controllers and processors, and under such foreign regimes a cloud provider would be considered a 'data processor' and exempted from most privacy obligations relating to data processed on behalf of its customers.

Foreign privacy regimes

The concept of a data controller, as distinct from a data processor, is a common concept in privacy regimes around the world, including in Europe and Asia. Under such foreign regimes, 'data controllers' are subject to the full range of legal obligations with respect to personal information (including with respect to collection, use, disclosure, accuracy etc.), and only very limited obligations are placed on 'data processors' (which are generally limited to ensuring that personal information is secure from unauthorised access or disclosure).

Foreign privacy laws that distinguish data controllers from data processors hinge the distinction on an entity's ability to control the relevant personal information. Some examples include:

- under the UK *Data Protection Act 1998*, a data controller is determined by an organisation's autonomy to determine the purpose for which the personal information will be processed or used;
- the *APEC Privacy Principles* define a data controller as an organisation controlling the collection, holding, processing or use of personal information, including by instructing another organisation to collect, hold, process or use personal information, but excluding collecting, holding, processing or using personal information in accordance with instructions received from another person or organisation: and
- Singapore's *Personal Data Protection Act 2012* does not define 'data controller', but excludes 'data intermediaries' from the majority of privacy obligations under the act, who are defined as organisations that process personal data on behalf of another organisation.

When will the Privacy Act apply to cloud providers?

The Privacy Act will apply to Australian-based cloud providers who collect or hold personal information in Australia, but may also apply directly to foreign cloud vendors that store personal information in offshore data centres:

- the foreign cloud provider is found to be "carrying on business in Australia" (indicia for which includes repeatedly transacting with Australian customers, and marketing specifically to customers in Australia); and
- personal information was collected or held by the cloud provider in Australia before or at the time of an act or practice to which the Privacy Act applies (which could include where personal information is stored in Australia, even transiently, on infrastructure owned or controlled by the offshore cloud provider).

Additionally, Australian customers are likely to require foreign cloud providers to contractually undertake to comply with the Privacy Act, as the Privacy Act prohibits organisations sending personal information outside Australia unless certain exceptions apply, including that the organisation has ensured that the foreign entity receiving the information will comply with the Privacy Act.

Where a cloud provider (or its customer) determines that the cloud provider must comply with the Privacy Act, they are then faced with the difficult task of determining which obligations are applicable.

What Privacy Act obligations apply to cloud providers?

Data processor obligations under many foreign privacy regimes are clearly set out in legislation. For instance. Singapore's privacy regime excludes 'data intermediaries' from all obligations other than to protect personal information from unauthorised access or disclosure.

The Privacy Act makes no distinction between a data controller and a data processor in the privacy obligations contained in the National Privacy Principles (the "**NPPs**", which apply to private companies), Information Privacy Principles (the "**IPPs**", which apply to

government agencies and their contractors) and the Australian Privacy Principles ("**APPs**", which unify the NPPs and IPPs under recently passed privacy reforms that will come into effect in 2014).

Rather, the application of most of the obligations contained in the NPPs, IPPs and APPs apply to organisations depending on whether they 'collect', 'use or disclose', 'hold', or 'possess or control' personal information, or 'transfer' or 'disclose' personal information to an overseas recipient. These terms, other than the term 'collect' (see below), are not defined in the Privacy Act,[1] and cloud providers must determine on a case-by-case basis whether their processing of customer data triggers the application of an NPP, IPP or APP under the Privacy Act.

The remainder of this article considers privacy requirements that may apply to cloud providers in relation to personal information contained within their customer's data.

Collecting personal information

"Collection" of personal information is defined under the Privacy Act as collection for the purpose of "inclusion in a record or a generally available publication". As a matter of statutory interpretation, it is unlikely that this definition of collection applies to cloud providers, which receive personal information only as a result of customer's uploading data containing personal information onto the cloud provider's systems in the course of using the cloud services.

Accordingly, it is unlikely that NPP 1, IPPs 1-3 or APP 3, which set out obligations in relation to the collection of personal information (for instance, collection by fair and reasonable methods), apply.

Holding Personal Information

By virtue of personal information being physically stored on a cloud provider's servers, such providers arguably have 'possession', or 'hold' the personal information, which triggers obligations including:

- ensuring personal information is secure from unauthorised access or disclosure (NPP4, IPP4, and APP 11); and
- on request of individuals concerned, providing access to personal information and, if requested by such individual, make any corrections to the personal information (NPP 6, IPPs 6 and 7, and APP 12 and 13).

These obligations are considered in further detail below.

Data security

NPP4, IPP4, and APP 11 place obligations on organisations that hold or have possession of personal information to take reasonable steps to protect personal information from unauthorised access or disclosure, and to destroy or de-identify personal information if it is no longer needed for any purpose for which it was collected.

A cloud provider may contractually undertake to its customers to take reasonable steps to ensure that customer data is secure from unauthorised access or disclosure – for instance, by securing the cloud platform and/or software applications that are provided to a customer.

The extent of a cloud provider's obligation to keep personal information secure becomes less clear when it is providing a cloud platform on which the customer builds its own software applications (for instance, where a cloud provider provides the platform for a customer's website, but the customer develops their own applications and functions for the operation of the website). In this situation, a cloud provider can only take steps to secure the platform, and will not be able to ensure that the applications developed by the customer appropriately secures the customer's data. In agreements for the provision of cloud services of this kind, the common contractual position is that the customer is responsible for securing its information, and the cloud platform provider is responsible for securing its platform. It is unlikely that a cloud provider could be found to be in breach of its obligation to 'take reasonable steps' to protect personal information in the event of a data breach caused by the customer's failure to use encryption adequately to protect its information. Nevertheless, in this scenario it is not clear.

Access and correction

NPP 6, IPPs 6 and 7, and APP 12 and 13 set out obligations in relation to providing individuals access to their personal information, and correction of such information at the request of individuals.

Although these obligations apply by virtue of the cloud provider holding a customer's data, cloud providers will find it difficult to comply as they will not have control or visibility over the personal information within customer data or knowledge of which individual the data relates to. As such, these obligations are a good example of the regulatory uncertainty resulting from the absence of a data processor / data controller distinction. These obligations are more appropriately discharged by a data controller (i.e. the cloud services provider's customer). To mitigate the risk of non-compliance, data processors must resort to seeking contractual assurances from the data controller, such as that the customer be obliged to discharge the cloud provider's obligation to grant access to individuals concerned and make any corrections to their personal information, and to indemnify the cloud provider for any breach.

Use and disclosure

NPP2, IPPs 9-11, and APP 6 restrict how a company may use or disclose personal information, and may apply to a cloud provider depending on whether there is any scope for the use or disclosure of personal information by the cloud provider.

In most cases, a cloud provider will not 'use' personal information contained in customer data (for instance,

where a cloud provider provides platform-as-a-service, or infrastructure-as-a-service). In some cases, a cloud provider might be required to directly handle or "use" customer data (including personal information) in relation to providing a cloud software service (for instance, where online applications process customer data including personal information). Where this is the case, a cloud provider may be subject to privacy obligations governing use of personal information, including that such use is consistent with the primary purpose for which the personal information was collected. As the cloud provider has not collected the personal information, and will not be aware of the purpose of collection, or whether an individual has consented to a particular use of their personal information, they will be unable to ensure compliance with such obligations. Cloud providers will again be left to negotiate contractual measures to protect themselves from possible breaches of the Privacy Act by their processing of customer data – for instance, by requiring customers to obtain all necessary consents from individuals for the cloud provider to process the information.

With respect to disclosure, a data processor may be required to disclose customer data pursuant to a court order, or request from a government agency. NPP2 and IPP11 contain an exception to the obligation not to disclose personal information where such disclosure is 'required by law'. Although this exception will clearly cover situations where Australian law compels disclosure, it is questionable whether the exception will apply to foreign laws that require the disclosure of customer data stored in Australia (for instance, US cloud providers are subject to the U.S. PATRIOT Act, which may require U.S. companies to hand over data stored anywhere in the world).[2] However, APP6 has clarified this exception to apply only to disclosure required by Australian law.

'Transferring' or 'disclosing' personal information overseas

Similar to many foreign privacy regimes, Australia has restrictions on the transfer of personal information overseas. However, unlike foreign regimes that adopt a data controller / data processer distinction, the Privacy Act does not limit the obligation to comply with data sovereignty restrictions to data controllers, and a cloud provider may be liable where it sends customer data offshore, even where it does so at the direction of a customer. NPP 9 and APP 8 prohibit the transfer (or the 'disclosure', under APP 8) of personal information to an overseas recipient, subject to certain exceptions including where the foreign jurisdiction has comparable privacy laws, where the overseas recipient is contractually bound to comply with privacy requirements, or where the relevant individuals have consented to their personal information being sent offshore.

Where a cloud vendor is located overseas and does not hold customer data in Australia, they will not be transferring or disclosing personal information outside of Australia – rather, it will be the Australian based customer that will be the entity that is sending the personal information overseas. Rather, it is where a cloud provider has data centre facilities in Australia and is likely to transfer data to overseas data centres that they will need to comply with NPP 9 (or APP 8, once it comes into effect). Such cloud providers may be in breach of NPP 9 or APP 8 if they disclose customer data containing personal information overseas to a foreign entity that is different to the Australian cloud provider (including, for instance a related entity of the cloud provider) unless one of the exceptions noted above apply.

To avoid the risk of breaching data-sovereignty obligations, cloud vendors may insist that all risk for breach of data sovereignty restrictions must lie with the customer (other than as a result of a cloud provider's breach of contract), and accordingly, agree not to move customer data offshore other than at the direction of the customer. Additionally, cloud providers may insist that customers obtain the consent of any relevant individuals for the cloud provider to send personal information offshore.

One difficult issue that arises in the context of data sovereignty restrictions concerns foreign national security laws such as the U.S. PATRIOT Act. Using this example, U.S. companies operating in Australia may be compelled by U.S. law to disclose data in its possession. In a situation where a customer requires that data be stored only within Australia, a U.S. cloud provider may be compelled to disclose such information to U.S. government authorities in breach of contract and potentially in breach of the Privacy Act. There is no easy resolution to this situation between cloud providers and their customers. A cloud provider will seek to ensure that its contractual obligations with respect to data residency are subject to any applicable legal requirement (including applicable foreign legal requirement) to send such data offshore. However, such positions on the part of the cloud provider may be unacceptable for customers depending on their requirements. Notably, customers that hold sensitive information such as health or credit information, that are a government agency, or that are a regulated financial entity may be prohibited from offshoring data, regardless of whether such offshoring is required by a foreign law.

Privacy policy

NPP5 and APP1 require organisations to have a readily available policy document setting out how personal information is handled, and, in respect of APP1, whether personal information is sent offshore, and if so, to which jurisdictions.

Cloud providers or data processors generally possess a privacy policy with respect to personal information they collect directly (eg. from their customers), but such

policies often do not cover personal information stored in customer data. In these circumstances, it may be appropriate for cloud providers to incorporate a general statement with respect to customer data stating that the customer is responsible for all personal information that it collects and uses in conjunction with the cloud provider's services, and that personal information contained in customer data will only be used, transferred or otherwise processed at the direction of the customer.

Conclusion

The absence of the distinction between a data processor / data controller in Australia's privacy framework creates uncertainty as to the extent that privacy obligations apply to personal information stored or processed by cloud providers on behalf of their customers. Whereas foreign privacy regimes specifically identify the limits on data processor obligations, Australia's law is silent. This regulatory uncertainty makes Australia less attractive to cloud vendors, who are confronted with a greater risk of contravening the Privacy Act through processing customer data in Australia than in regimes where their role as a data processor specifically excludes compliance with most privacy obligations. Additionally, it complicates negotiations for customers, as cloud providers are forced to seek contractual indemnities and other protections to offset the risk of regulatory breach.

While Australia's cloud industry is in its infancy, it has demonstrated strong potential by attracting the attention of some of the world's largest technology companies. To realise this potential, Australia must play to the perceived strengths in its regulatory environment and ensure that clarity is given to the privacy obligations of cloud providers.

---

[1] The concept of having "possession or control" or "holding" personal information was not defined under the Privacy Act prior to the reforms. The reforms have not added clarity to these terms, but have made their use more consistent – the term "possession or control", wherever it appears in the Privacy Act has been replaced with the term "hold", and the term "hold" has been defined as having "possession or control".

[2] Where customer data is held in servers outside of Australia, a disclosure that is compelled by foreign law will not breach the NPPs or the proposed APPs by virtue of section 6A(4) of the Privacy Act.