'Australia's Privacy Principles and Cloud Computing: Another Way'

Kanin Lwin considers the application of the new APPs to the cloud computing industry.

Telecommunications advances, assisted by the development of the Internet, have spawned enormous opportunities for sophisticated data exchanges and has led to the proliferation of data outsourcing arrangements, especially cloud computing. These developments have, however, also made it easier for organisations to harvest and disseminate large quantities of personal information.

Privacy regimes in certain countries balance the interests of individuals in protecting their personal information with the economic efficiencies generated through data outsourcing, by distinguishing between entities that *control* how and what personal information is processed (***controllers***) and entities which merely process data on behalf of a controller (***processors***).

In many although not all situations, cloud providers will not be collectors or controllers of personal information

By contrast, the new Australian Privacy Principles (***APPs***), which will replace the National Privacy Principles (***NPPs***) and Information Privacy Principles (***IPPs***), do not purport to make such distinctions, despite applying to the lifecycle of collection, handling and destruction of personal information.[1] Consequently, the APPs have been criticized[2] for exposing cloud providers, in those instances where they act only as processors of personal information, to privacy obligations which may be beyond their capacity to comply.

This essay will contend, however, that the regulatory, economic and practical considerations surrounding cloud computing create a strong contextual impetus for reading the APPs in a way that recognises that providers and customers can and do have different roles in the processing of personal information. In particular, it will argue that many APPs, as a result of their operation, do in fact distinguish between (i) 'collectors' and 'non-collectors' of personal information and (ii) 'controllers' and 'processors'.

Background

Regulatory landscape

The marriage of computer and telecommunications technologies has spurred the evolution of automated message transmissions and enabled vast movements of data. In particular, the Internet has increased the possible scale and complexity of data interchange: already, internet traffic exceeds 1.5 billion gigabytes each day.[3] Whilst the opportunity for greater data flows has unlocked considerable economic benefits for society in general, it also poses significant privacy risks to individuals.

Economic Benefits

Businesses can now harness powerful communication networks to process their data externally, thereby tapping into an outsourcer's pool of resources along with the accompanying cost efficiencies. Cloud computing, for example, describes an arrangement wherein clients outsource some or all of their information technology (***IT***) workload by using the Internet to access, on demand, 'a shared pool of configurable computing resources (eg. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction'[4] (***cloud***).

The extent to which clients manage the underlying IT resources depends on the model selected; greatest control exists in an 'Infrastructure-as-a-Service' arrangement, and the least control in 'Software-as-a-Service' with 'Platform-as-a-Service' in between. One attraction of the cloud is that clients consume computing resources as a service, renting only as much of the provider's infrastructure as required, and thus can leverage off the considerable economies of scale consolidated within provider data centres.

Privacy challenges

However, the corresponding erosion of the individual's ability to control the circulation of information about themselves, a popular although not undisputed description of privacy,[5] threatens to offset these commercial benefits.

Communications and networking technology make it increasingly feasible for organisations to disseminate large quantities of personal information, often without an individual's knowledge or acceptance. Moreover, the 'Internet age' has spawned a situation where social interactions are fast becoming online affairs,[6] aggravating existing privacy concerns.

With growing amounts of information coursing through the Internet, it has become far easier for organisations to collect private information about customers and their personal habits, increasingly valuable commodities in today's information-driven economy[7]. By one estimate, the top 50 websites install on average 64 pieces of tracking software onto a person's computer, usually without warning, inhibiting an individual's control over their personal information.[8]

---

1 Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), 52 ***(Explanatory Memorandum).***

2 James North and Daniel Thompson, 'Privacy Laws Are Affecting Australia's Cloud Industry', *Corrs Chambers Westgarth Thinking,* http://www.corrs.com.au/thinking/insights/privacy-laws-are-affecting-australias-cloud-industry/ 7 March 2013

3 Jeff Jarvis, *The Guardian* (online), http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance 13 August 2013

4 Peter Mell and Timothy Grance, 'The NIST Definition of Cloud Computing', (Special Publication 800-145, National Institute of Standards and Technology, United States Department of Commerce, September 2011), 2.

5 Daniel Solove, *Understanding Privacy* Harvard University Press, (1st ed, 2008) 24-29.

6 McKay Cunningham, 'Diminishing Sovereignty: How European Privacy Law Became International Norm' (2012) 11 *Santa Clara Journal of International Law* 423.

7 Horace Anderson, 'The Privacy Gambit: Toward a Game Theoretic Approach to International Data Protection' (2006) 9(1) *Vanderbilt Journal of Entertainment and Technology Law* 5.

8 Cunningham, above n6, 426.

Furthermore, much of the value in personal information lies as part of larger value-added assets like the database of customer payment information facilitating Amazon.com's '1-Click' payment system wherein customers can make online purchases through a single mouse click, without needing to re-enter their billing details.[9] Organisations are thus incentivised to accumulate ever expanding dossiers on individuals, perpetuating ever greater intrusions into the private sphere.

Reaching a balance

To accommodate both the economic benefits of allowing greater data traffic and providing adequate protections against organisations mining this data traffic for personal information certain privacy regimes distinguish between controllers and processors. Singaporean legislation for instance exempts 'data intermediaries' (effectively another name for 'processor') from most privacy law responsibilities.[10]

The reason for this functional distinction is twofold. First, the concept of 'controller' gives individuals an entity against whom they can enforce their privacy rights, thereby re-asserting some control over the circulation of their personal information. The European Union, as an example, requires controllers to ensure an individual's right of correction is delivered in practice.[11] Secondly, the existence of 'processors' as separate entities handling information on the controller's behalf recognises that the controller's responsibility for the processing of personal data does not mean controllers must always physically handle personal information. Thus it accommodates for the practical reality of data outsourcing.

APPs

The APPs purport to recognise that 'protection of the privacy of individuals is balanced with the interests of entities carrying out their functions'[12], therefore they address to some extent the competing considerations influencing privacy protection design. However, the APPs seem to allocate responsibilities irrespective of the functional differences between data processing participants and so might not in fact effectively balance between securing the privacy interests of individuals and the economic benefits inherent to outsourcing arrangements.

With respect to the private sector, the APPs will apply to any 'organisation' depending on whether that entity:

- 'Collects',[13] 'holds',[14] 'collects and holds'[15] ,'receives',[16] or 'discloses',[17] personal information;
- 'Adopts' or 'uses/discloses' a government-related identifier;[18]
- 'Deals'[19] with an individual; or
- Is an 'APP entity'.[20]

One possible explanation of this approach could be a desire to shift the focus away, in many instances, from what entities are and onto what entities do with personal information, especially given entities can alternate between acting as controllers or processors when processing data[21]. Nevertheless, from the standpoint of cloud arrangements, the APPs, on face value, encounter significant practical, regulatory and commercial difficulties.

Cloud providers as processors & non-collectors

In many although not all situations, cloud providers will not be collectors or controllers of personal information. For example, clients who leverage a cloud solution to scan their emails for malware are usually responsible for setting, via the management console under their control, the directions according to which that data is processed.[22] With such solutions, the cloud provider should also generally have administrative and process locks in place to help ensure they remain, on a day to day basis, at arm's length from the data running through their infrastructure.[23]

Even if cloud providers can be said to hold data that resides on their servers, insofar as entities 'hold' personal information under their possession or control,[28] they often lack the capacity to provide access

The Australian Information Commissioner (***Commissioner***) has also released guidelines for the APPs (***Guidelines***) which state that, subject to certain conditions, clients may be regarded as controlling personal information where their cloud agreement empowers them to determine how data is processed[24].

The Guidelines are not legally binding, however, the Commissioner will take the Guidelines into account when applying the APPs.[25] And the Commissioner's guidance in relation to control by contract replicates earlier guidance regarding the IPPs.[26]

In certain situations, however, cloud providers will act as collectors and controllers, such as where a provider harvests personal information from emails stored on their cloud solution.[27]

Practical

One practical problem of applying all the APPs to each data processing participant is that given cloud providers often act as processors and non-collectors, they would frequently need to adhere to many

9 Anderson, above n7.

10 *Personal Data Protection Act 2012* (Singapore) ss2(1) and 4(2).

11 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of 'controller' and 'processor',* EU Doc 00264/10 EN WP 169 (adopted 16 February 2010) 4 (***Opinion 1/2010***).

12 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) sch4 s2A (***Privacy Amendment***).

13 Australian Privacy Principles 3, 5, 10.1.

14 APP 6, 7, 11, 12 and 13.

15 APPs 1.3-1.6.

16 APP 4.

17 APP 8.

18 APP 9.

19 APP 2.

20 APP 1.2.

21 *Opinion 1/2010,* above n11, 29.

22 Email correspondence from Basil Newnham, Symantec Corporate Counsel, to Kanin Lwin, 26 November 2013.

23 Ibid.

24 APP Guidelines, Ch B, 'Use'.

25 APP Guidelines, 'Preface'.

26 IPP Guidelines, Ch 8, 'Relationship between use and disclosure'.

27 *Opinion 1/2010,* above n11, 29.

privacy obligations outside their capability to comply. For example, APP 12 requires entities holding personal information to grant access to that data upon request. Even if cloud providers can be said to hold data that resides on their servers, insofar as entities 'hold' personal information under their possession or control,[28] they often lack the capacity to provide access. Where a client has chosen to secure their data through a method like multi-blind key encryption, wherein they essentially retain both the encryption and de-encryption keys,[29] a provider would depend entirely on the customer's assistance to comply with APP 12. Likewise, APP 6 obliges entities to use personal information only for the purpose(s) for which it was collected. However, cloud providers who process data which the client collects are unlikely to know this purpose or share the same purpose as the original collector.

Regulatory

Any reading of the APPs which reduces the number of entities to whom they apply might be said to favour practicality at too great a cost to privacy. However, making providers accountable for obligations with which they cannot feasibly comply does not necessarily stimulate better compliance with the APPs. Instead, expanding the number of entities that have privacy obligations may unnecessarily dilute privacy responsibility[30] and reduce the cost and burden of compliance for cloud computing customers who are both the controller and collector, given liability may now be shared with the provider.

Any reading of the APPs which reduces the number of entities to whom they apply might be said to favour practicality at too great a cost to privacy

Commercial

A favourable and more targeted application of the APPs to cloud computing is also more consistent with a drive to develop Australia as a consumer and vendor of digital services through a mixture of 'conducive' regulations and 'digital infrastructure' like the NBN[31]. In particular, interpreting the APPs in a manner that avoids fragmenting privacy responsibility would allay consumer concerns and permit Australian businesses to expand their use of outsourcing arrangements like cloud computing. Furthermore, more realistic distinctions in the application of privacy obligations would enhance Australia's attractiveness as a regional data-hub and potentially, be more consistent with the approach taken in other jurisdictions including the EU[32] whose privacy regime recognises the functional differences between data processing participants.[33].

Preferred approach

Collectors & controllers

As described above, there is a contextual impetus for interpreting the APPs in a way that acknowledges the different roles various entities play when processing data. One possibility is to recognise that several APPs distinguish between (i) controllers and processors and (ii) collectors and non-collectors, given concepts of 'control' or 'collection' underpin most APPs.

Many obligations in the APPs apply only to controllers or collectors. As a result, processors who are not involved in data collection are answerable for just APPs 1.2 and 11.1 (summarised by the table below) which do not require collection or control. Controllers remain different from collectors given processors can collect personal information on a controller's behalf.[34]

APP	Focus	Lifecycle stage	Appropriate entity
1.2	Compliance procedures	Entire	All
11.1	Security	Handling	
1.3-1.6	Privacy Policies	Collection	Collector
2	Anonymity/ pseudonymity	Collection	
3	Solicited personal information	Collection	
5	Notification of collection	Collection	
9.1	Adoption of government related identifiers	Collection	
10.1	Quality of personal information collected	Collection	
4	Unsolicited personal information	Collection/ Destruction	Controller
6	Use or disclosure	Handling	
7	Marketing	Handling	
8	Cross-border disclosures	Handling	
9.2	Use or disclosure of government-related identifiers	Handling	
10.2	Quality of personal information used or disclosed	Handling	
11.2	Destruction/ de-identification	Destruction	
12	Access	Handling	
13	Correction	Handling	

Rationale

Although this approach adds a collector/non-collector classification to the controller/processor distinction of other privacy regimes, it still balances, more effectively, the economic and privacy implications of the growth in data traffic. A regulatory focus on 'collectors' and 'controllers' enables individuals to exercise their privacy rights against those entities and thereby retain some control over their personal information throughout the lifecycle of processing. This approach of allocating the bulk of privacy obligations according to whether entities 'collect' or 'control' personal information also takes into account the functional differences between data processing participants and so promotes privacy protection without inhibiting outsourcing arrangements like cloud computing.

Cloud providers, in the many situations where they neither collect nor control personal information, would not need to comply with unfeasible obligations like granting access to information outside their control.[35] Instead, they would be exposed only to APPs 1.2 and

28 *Privacy Amendment* sch 1 s24.

29 Symantec Corporation, 'Patent for Systems and Methods for Secure Third-Party Data Storage' (26 September 2013) http://www.faqs.org/patents/app/20130254558

30 *Opinion 1/2010,* above n11, 29.

31 Department of Broadband, Communications and the Digital Economy, Australia's Digital Economy: Future Directions, 2009, 8.

32 Australian Law Reform Commission, *Review of Australian Privacy Law,* Discussion Paper 72 vol 1, 850-854.

33 *Opinion 1/2010,* above n11, 4.

34 *Opinion 1/2010,* above n11, 27.

11.1, obligations providers *can* and *should* comply with at all times. APP 1.2 simply requires that organisations have procedures in place to comply with the relevant APPs. Whilst APP 11.1 obliges entities to take such steps as are reasonable in the circumstances to protect personal information they hold from risks such as 'misuse' and 'unauthorised disclosure', providers need not control or collect data to be able to comply with this obligation.

By virtue of partly or wholly managing the underlying IT infrastructure for an organisation, cloud providers have considerable influence over the protection of personal information within their environment, irrespective of whether they control data collection and handling. Even under an 'Infrastructure-as-a-Service' arrangement, where providers manage only the physical IT resources, providers still have a responsibility to ensure their hardware is not misused to compromise a client's environment: one customer, for example, could run malicious code from the 'cloud' leveraging the solution's considerable physical resources to intensify their attack against other customers.

Controller/processor

The idea of control appears in many APPs either through the proxies of 'use' and 'disclosure' or because there is an assumption that the type of entity to which that particular APP applies has a capacity to deal with personal information that only a controller would have.

- **Use or disclosure – APPs 6-8, 9.2, 10.2 and 11.2.** APPs which incorporate 'use' and/or 'disclosure' of personal information into their scope can only apply if the entity has control over data. APPs 6, 7, 8, 9.2 and 10.2 regulate how an entity may 'use' and/or 'disclose' personal information. APP 11.2 requires entities to destroy/de-identify personal information they can no longer use or disclose. Although 'use' and 'disclosure' are not defined,[36] the Guidelines state that information is 'disclosed' where an entity releases it from its 'effective control'[37] and 'used' if the entity maintains control.[38] This is consistent with the earlier NPP guidelines[39] and mirrors the previous IPP guidelines wherein, for example, disclosure is regarded as a release of effective control.[40]
- **Capacity to decide which data to process – APP 4.** APP 4 obliges entities to decide either to destroy/de-identify or 'collect' unsolicited personal information, depending on whether it could have been legitimately collected. The decision is ultimately one about which data to process (i.e. is it to be collected and processed or destroyed/de-identified), a determination only the controller can make.[41] Consequently, APP 4 should normally only concern those entities acting as controllers.
- **Capacity to grant access – APP 12.** Likewise, the requirement in APP 12 that individuals generally be given access to their personal information implies that an entity has the capacity to grant such access, an ability usually regarded as an exclusive power of controllers.[42]
- **Level of control – APP 13.** APP 13 provides that entities must, under certain circumstances, correct the personal information they hold. The Explanatory Memorandum notes that APP 13 is designed to normally force entities into assessing the quality of personal information they hold 'at the time of use or disclosure',[43] indicating that APP 13 is primarily directed at controllers.

Collector/non-collector

- **APPs 3, 5 and 10.1.** Some of the APPs bear little relevance for non-collectors. For instance, APP 3 restricts when entities can collect personal information whilst APPs 5 and 10.1 regulate how collection can occur. Other provisions like APPs 1.3 to 1.6, 2 and 9.1 presume the entity is a collector notwithstanding language which might read as applying to non-collectors as well.
- **APPs 1.3 to 1.6.** These APPs require entities to develop and disseminate privacy policies according to specific standards. Although 'APP entity' encompasses collectors and non-collectors, APP 1.4 states that privacy policies must declare what personal information that entity 'collects and holds' and so makes little sense for non-collectors.
- **APP 2.** This principle grants individuals a right to anonymity or pseudonymity when 'dealing' with entities. As such a right ensures entities seek only the minimum amount of personal information necessary, APP 2 potentially applies to two stages in the lifecycle of information processing: (i) when an entity collects personal information from the data subject or (ii) holds that information beyond what is necessary.[44] However, it is unlikely APP 2 extends to encompass non-collectors. APP 11.2 already deals with the de-identification of personal information which has ceased to be relevant to the purpose for which such data could be legitimately used or disclosed. Furthermore, the Explanatory Memorandum rationalises APP 2 primarily on the basis 'the privacy of individuals will be enhanced if their personal information is not *collected* unnecessarily'.[45]
- **APP 9.1.** APP 9.1 generally prohibits organisations from 'adopting' government related identifiers. Given the Guidelines define adoption in terms of the collection and organisation of personal information[46], this prohibition seems geared toward collectors.

Conclusion

Opportunities for vast movements of data offer considerable economic benefits but pose serious privacy concerns, in particular the growing incentive and ability to harvest this traffic for valuable private data. To accommodate this tension without inhibiting outsourcing arrangements like cloud computing, certain privacy regimes take into account the functional differences between data processing participants, usually in terms of control. The APPs strike a similar balance between privacy and practicality, albeit by allocating many obligations to 'controllers' or 'collectors'. As the market and value proposition for cloud services grows, these classifications offer a means of interpreting the APPs in a manner which avoids burdening providers (where they act as processors and non-collectors) with unfeasible obligations that unnecessarily fragment privacy responsibility. Furthermore, the focus on controllers and collectors also better aligns Australia's regulations with the emerging 'digital economy' both in terms of capturing a slice of the growing cloud services market and encouraging Australian businesses to drive productivity gains by embracing the 'cloud'.

Kanin Lwin is a graduate at Ashurst Australia and was a finalist in the 2014 CAMLA Young Lawyers Essay Competition for an earlier version of this essay.

35 APP 12.
36 *Privacy Act 1988* (Cth) s6.
37 APP Guidelines, Ch B, 'Disclosure'.
38 APP Guidelines, Ch B, 'Use'.
39 NPP Guidelines, 35-42, 'Use and disclosure'.
40 IPP Guidelines, Ch 8, 'The meaning of use and disclosure of information'.
41 *Opinion 1/2010,* above n11, 16.
42 *Opinion 1/2010,* above n11, 17.
43 Explanatory Memorandum, 88.
44 Anneliese Roos, 'Core Principles of Data Protection Law' (2006) 39 *Competition and International Law Journal,* 113-114.
45 *Explanatory Memorandum* 74.
46 APP Guidelines, Ch 9, 'Adoption'.