Commentary on the ALRC Recommendations for Cross Border Transfers (2008)

Chris Connolly, Galexia

1. Proposed UPP 11

UPP 11. Cross-border Data Flows

If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to these principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

Note: Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.

2. Very brief comments

2.1. The new accountability principle

This is a very attractive development as it has the potential to ensure that organisations are motivated to take care when transferring data to other jurisdictions, and it provides consumers with some rights against collecting organisations when breaches occur.

Web: www.galexia.com Ph: +612 9660 1111 Fax: +612 9660 7611
Post: Suite 95 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

However, the ALRC recommendation on accountability suffers from two weaknesses:

Firstly, it does not apply to every transfer of data, as a series of exceptions apply (discussed below). It is difficult to see why the accountability principles does not apply to all transfers. The exception for circumstances where a consumer *insists* on the transfer is understandable – the other exceptions make no sense.

Secondly, the accountability principle does not assist consumers *rectify* a breach that occurs in another jurisdiction. Although they may have a valid complaint against a local organisation, the damage will occur in a foreign location and will not be subject to remedial action (such as the removal, correction or destruction of information). In privacy law, remedial action is often more important to consumers than compensation. The proposed UPP 11 appears to rely heavily on the accountability principle, without recognising this limitation for consumers.

2.2. The 'adequacy' exception – laws

The continued presence of an adequacy test in Australian privacy law (in the face of strong opposition) is welcome. However, it is very poorly implemented in the proposed UPP 11.

It is a mistake to combine laws and contracts in the one provision, as they have little in common and the combination may have resulted in a watering down of protections. These notes therefore divide the adequacy test between laws and contracts.

The key problems with the adequacy test for laws, as proposed in UPP 11 (a) are:

2.2.1. Reasonable belief

The test relies on the 'reasonable belief' of the sending party. This is a weak test and is doomed to become a wide loop-hole for transfers that weaken privacy, either through error or deliberate action.

This test may be unnecessary for laws, as elsewhere in the ALRC Report they have recommended that Australia develop a list of countries who provide privacy protection that is substantially similar to the UPPs **[Recommendation 31–6].** If a country is on that list, the reasonable belief test will be so easily met that the test is irrelevant.

However, if a country is not on that list, the sender can still 'develop' a reasonable belief and send the data anyway. This is highly dangerous.

There are numerous examples where a sender may have a reasonable belief that data will be safe in the foreign jurisdiction. For example the CPO of Google has stated that Japan has adequate privacy laws and he questions why the EU have not added Japan to their white-list. Many people may develop a reasonable belief that data is protected by reading the Japanese Act quickly and reading blogs and other online materials (e.g. the Google statements).

In fact, great care needs to be taken when sending data to Japan. Privacy protection could be zero in many circumstances. For example, many key exceptions to the Japanese law are not contained in the Act itself (they are contained in Cabinet orders) and some have not even been officially translated into English.

There are numerous other similar examples in the region. Korea and Taiwan both have strong privacy laws, but they only apply to certain industries and categories of data. Hong Kong and New Zealand have strong privacy laws, but protection for onward transfer of data is weak.

There is a current trend to criticise the EU white list – and it is true that they appear to have made some mistakes (e.g. approval of Argentina). However, in our region they appear to have made sound decisions – including rejecting Australia.

A significant problem with the EU white list is that it has an all or nothing approach. Australia is either on or off the list. It would be more useful and realistic to allow a conditional white list to develop that reflected the known gaps in domestic laws (e.g. the small business and employee exemptions in Australia, the small records exemption in Japan, the category limitations in Korea and Taiwan…). There is an opportunity to do this in Australia but it is not mentioned in the ALRC report.

If we are going to have a white list for adequate laws we should force reliance on that list and abandon the weak 'reasonable belief' test. We should also develop a conditional white list that reflects known gaps, but still allows the transfer of data where it is safe to do so. The resources required to do this once will be less than the combined costs of numerous businesses in obtaining legal advice, and less prone to mistakes.

2.2.2. Restriction to UPPs

The proposed test is whether a foreign law is substantially similar to 'the principles'. This restricts protection to a fraction of the potential breaches of Privacy contained in 'the Act' and it should be amended.

The current text would exclude data breach rules, health and credit reporting regulations and other protections scattered through the Act. Many of these are important protections.

2.3. The 'adequacy' exception – contracts

This should be set out as a separate principle.

As it stands, UPP 11 (a), when used in conjunction with a contract, is probably the weakest exception. It combines the reasonable belief test (very weak) with an untested / non- standard contract (weak) and removes the accountability principle. It is difficult to imagine how you would construct a complaint for a breach – it is probably easier to have an argument about reasonable belief in relation to a law than a contract. And contracts will be confidential and difficult to debate in the open, as opposed to laws.

However, contracts are a common form of protecting privacy in cross-border transfers and they are unlikely to disappear. Other jurisdictions recognise contracts as providing a layer of protection, and publish model contract terms in order to enhance privacy standards. Australia should adopt the same approach.

The EU model contract terms were the subject of harsh (and justified) criticism throughout the late nineties and the early part of this decade. However, they have been revised and re-issued in consultation with stakeholders (including business groups). The new contract terms represent a significant improvement and there do not appear to be any remaining criticisms from business.

Australia could learn from this experience and publish model contract terms that help organisations to incorporate the UPPs and other Privacy Act requirements into their cross-border contracts. This would provide a higher level of protection than the 'reasonable belief' test.

In practice, a combination of the accountability principle and model contracts could be a very popular mechanism for protecting privacy in cross-border transactions. It avoids the onerous 'registration' requirements of other proposals (eg BCRs and CBPRs) at a time when businesses face a strain on privacy/legal resources.

2.4. Consent

The consent exception is open to abuse – but this is not a problem restricted to UPP 11. It imports all of the problems with consent that are discussed elsewhere in the ALRC report. Significantly, the consent for cross-border transfers could be 'bundled' with the consent for the use of personal information at the local level – making it impossible for a consumer to approve local use and oppose foreign use.

2.5. Required or authorised

This exception – UPP 11 (c) – is necessary, although the term 'under law' is quite broad.

2.6. The 'Note" re Use and Disclosure

This is a bizarre addition to the Principle that is open to misinterpretation by an organisations who might believe that, as the note only refers to 'Use and Disclosure', they are not bound by the other Principles.

2.7. Notice

The inclusion of cross border transfers in the Openness Principle in UPP 4 is welcome. Presumably it is also required in specific notices, but this is strangely absent from the proposed UPP 3. This is a significant error / gap.

2.8. Binding schemes

There is a strange reference to binding schemes in UPP 11 (a). It is not defined or otherwise mentioned in the ALRC report or DP 72. It was included in the NPPs but is not defined. The ALRC rejects BCRs, CBPRs and trustmarks in other sections so it can't refer to those. Perhaps it refers to registered codes of conduct? The term 'binding schemes' would benefit from either deletion or a definition.

2.9. Related bodies corporate

Related bodies corporate who transfer data across borders within the corporate group will have to comply with UPP 11. This is very close to a direct rejection of BCRs and CBPRs for intra-company transfers. **[Para 31.201 to 31.206].** It is also an excellent clarification of an issue that is confusing in the current Act.