Meeting privacy challenges – the ALRC & NSWLRC Privacy Reviews

Seminar, Faculty of Law, University of New South Wales, 2 October 2008

Panel Session 4: How well do the ALRC/NSWLRC proposals contribute to meeting international standards for cross-border data transfers?

Two approaches to cross-border data transfers

Introduction

The internet has created a global market for information handling and processing services. Major companies and government agencies, seeking more effective and efficient ways to store and process customer data, are often using overseas data processing services via the internet. However, global integration of information handling practices is concerning for affected individuals, be they 'consumers' or 'citizens'.

The Community Attitudes to Privacy 2007 survey conducted by the Office of the Privacy Commissioner showed that "the majority of Australians (90%) are concerned about businesses sending their personal information overseas, with 63% being very concerned".[1] Individuals want to know that when they hand over personal information it is protected by the organisation, or at least covered by laws that give them the right to have a complaint about misuse of their personal information investigated by a regulator. Uncertainty about whether this is the case when an organisation transfers overseas information about individuals introduces a 'country risk' for them.

What is the problem we are trying to resolve?

The objective is to eliminate the additional 'country risk' imposed on individuals when an organisation or government agency sends personal information about them to another country.

Two approaches to addressing the problem: Adequacy and Accountability

Around the world two approaches have emerged as most often applied to achieving the objective of eliminating this 'country risk' for the individual.

One approach is based on the concept of 'adequacy'. The 'adequacy' approach seeks to ensure that the receiving country or jurisdiction is perceived as having an 'adequate' privacy protection law in place. Most notably, this approach has been taken by *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (EU Directive). A very similar approach has been included in the *Privacy Act 1988 (Cwth)* as it applies to private sector organisations.

[1] See www.privacy.gov.au/publications/rcommunity07.pdf pg iv.

The other approach is based on the concept of 'accountability'. This approach, in its purest form, holds the original collector of the personal information accountable for compliance with the original privacy framework that applied when & where the data was collected, regardless of the other organisations or countries to which the personal data travels subsequently. This approach is included in the privacy frameworks of some overseas jurisdictions including Canada and the USA as well as the APEC Privacy Framework. It is also the basis of the recommendations by the ALRC in Chapter 31 of its recent report, *For Your information: Australian Privacy Law and Practice* (ALRC 108, 2008).

The adequacy of adequacy

The strongest proponent of the adequacy approach, the EU, has not developed a standardised and accepted way of assessing it. The EU has tended to determine adequacy through bilateral discussions with third party countries and to focus on the letter of the law, as they interpret it from a civil law perspective, to the exclusion of any other consideration such as the actual efficacy of the enforcement framework. This approach is reflected in the somewhat eclectic list of jurisdictions and programs which have achieved adequacy including: Canada, Switzerland, Argentina, Guernsey and the Isle of Man, Jersey, the US Department of Commerce's Safe Harbor Privacy Principles and the 'transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection'.

The adequacy approach is also hard for the consumer and regulator to work with. The adequacy approach does not provide them with a coordinated way of making and handling a complaint should a breach occur in another country. The adequacy approach provides the consumer with a number of accountability bodies to which they can complain. In effect, it leaves the responsibility on the consumer to do sufficient preliminary investigations, before they can make a formal complaint, to find the relevant accountability body in relevant jurisdictions where the alleged breach might have occurred. The regulator then takes over from there during the investigation

In short, the approach based on adequacy has not worked.

The adequacy of accountability

The accountability approach, properly applied, can address 'country risk' very simply. It eliminates the country risk by applying accountability to the organisation transferring the data. Organisations could be made accountable by law in Australia for compliance with the initial protections and privacy standards applying to personal information wherever in the world those organisations send it.

Like adequacy, the effectiveness of an accountability based regime depends critically on the legal powers and financial resources available to the regulator. Unlike the adequacy approach, the problem of chasing down where a problem happened in a chain of data movement is not left to the regulator or the affected individual. That problem is assigned to the original collector of the personal information. As such, it has a better chance of becoming an enforceable approach as well as placing a stronger incentive on the transferor to ensure that appropriate information handling practices are safe in the first place.

The ALRC approach – accountability as the foundation

In *For Your information: Australian Privacy Law and Practice*, the ALRC recommends that privacy laws should include a provision to ensure 'accountability follows the data'.

Recommendation 31-2 in particular (leading to Unified Privacy Principle 11) reads as follows:[2]

> **Recommendation 31-2** The 'Cross-border Data Flows' principle should provide that, 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 or 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 the model Unified Privacy 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.

Thus the ALRC has clearly decided, in light of further consideration after publishing its Discussion Paper, that the default should be based on the accountability concept. That said, in sub para (a) it also countenances adequacy arrangements similar to the current requirements of the Privacy Act.

Interestingly, compared with the exceptions to the adequacy arrangements in the EU Directive, the exceptions recommended by the ALRC are similar or tighter. In particular, Article 26 of the Directive makes an exception of the adequacy requirement in a number of instances including:

- there is unambiguous consent from the data subject (cf sub para (b) of Recommendation 31-2);
- the transfer is in the public interest or the vital interests of the data subject (cf the narrower exception in sub para (c))

As such, the ALRC recommendations appear to have been drafted to fit in with both of the predominant approaches and to contribute well to "meeting international standards for cross-border data transfers".

The remaining question is whether the ALRC approach will succeed in mitigating 'country risk'. However as mentioned earlier, this will be determined as much by the way that the laws are implemented and enforced as by the black letter words of the law. This in turn will depend as much on the level of resources provided to the regulator as on the powers it is given.

Resources will be a major consideration for government when responding to the ALRC report.

---

[2] *For Your information: Australian Privacy Law and Practice (ALRC 108, 2008)*, Chapter 31. See in particular www.austlii.edu.au/au/other/alrc/publications/reports/108/_3.html#Heading275