Deloitte.

Regulatory review

Keeping you informed of compliance developments

Financial Services

September 2008

Major changes to Australia's privacy law on the horizon

The Australian Law Reform Commission (ALRC) released its report *For Your Information: Australian Privacy Law and Practice* on its review of Australian Privacy Law on 11 August 2008. Its wide-ranging review considered if Australia's privacy framework is effective, for example, in the face of huge changes in technology since the *Privacy Act 1988* was first introduced and following its extension to the private sector in 2000. Key areas of the inquiry included the credit reporting system, interaction between federal state and territory privacy law, international trends in privacy protection, including data breach notification, and children's privacy.

The ALRC's report makes 295 recommendations which if adopted by the Government will make some very significant changes to Australia's privacy regime. For business, there are likely to be both wins and losses and certainly some opportunities, for example in the credit reporting changes and in the health area.

The Australian Government will now consider the ALRC's 295 recommendations and has said that it will do this in stages. The first stage response should be delivered in 12–18 months. It will focus on the recommendations relating to the Unified Privacy Principles, health regulation and the credit reporting sector and on improving education about the impact on privacy by new technologies. The government has not yet given a time frame for the second stage of its response, which will include some of the more contentious recommendations. In both stages there are likely to be further opportunities for business to put its views about proposed changes and the possible implications.

The first stage recommendations to be considered in the next 12–18 months include:

- introducing one set of 'Unified Privacy Principles' (UPPs), consolidating various sets of principles, for example the National Privacy Principles (NPPs) for the private sector, the Information Privacy Principles for the public sector, and credit reporting provisions into one, as part of measures aimed at simplifying the Privacy Act. More, or less, rigorous protections, for example for credit or health information, will be available through regulations
- expanding the current 'negative' credit reporting system, which focuses on credit defaults, to permit additional categories of 'positive' information to be added to an individual's credit file, including the type of credit, the credit limit and whether the account is current
- strengthening investigation and enforcement powers for the Privacy Commissioner including new power to audit private sector organisations or to impose civil penalties
- a focus on education and community awareness about the privacy implications of a range of new technologies.

In recommending a set of UPPs the ALRC has indicated a general approach, including high-level principles and technological neutrality and has noted some areas that would make significant changes to the current NPPs. These include:

- a separate direct marketing principle which would distinguish between direct marketing to existing customers and new customers or those under 15 years, and which would impose stricter requirements in the latter cases including telling people, when asked, the source of their contact details
- strengthening the transborder data flow provisions to take into account the work of APEC so that 'an agency or organisation that transfers personal information outside the country remains accountable for it, except in certain specified circumstances'
- a new requirement to notify individuals about avenues of complaint.

The ALRC has put forward developed sets of words for the UPPs. This is likely to be an area of considerable interest to business during any implementation process.

As noted earlier, the Government is proposing a two stage implementation process. Some of the more significant recommendations for business in this second stage include:

- removing the current employee records exemption meaning that private sector organisations would need to apply the Privacy Act to employee records
- removing the current small business exemption which applies to businesses with an annual turnover of $3m or less and where there is limited privacy risk
- introducing data breach notification similar to that currently applying in most United States jurisdictions but setting a reasonably high bar
- introducing a cause of action for a serious invasion of privacy where an individual has suffered a serious invasion of privacy, in circumstances in which the person had a reasonable expectation of privacy.

In making these recommendations the ALRC has recognised that there will be some considerable challenges for business. For example it recognises employers' concerns about when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee. The ALRC's view is that the current exceptions to the NPPs, which for example, permit organisations to deny access to personal information where access would reveal commercially-sensitive decision-making material, cover this situation. However, in this area, and a number of others, including the removal of the small business exemption the ALRC has also said that the Office of the Privacy Commissioner should develop and publish specific guidance.

This will be an important consideration in the Government's implementation process. For example, it is likely that there will be minimal impact on small businesses that do not handle much personal information but they will certainly need to be in a position to make a sensible risk assessment. Material from the Privacy Commissioner could help here. Recommendations relying on guidance and support will have less than the intended effect or could even prove to be problematic if the Privacy Commissioner among others is not properly resourced to discharge these responsibilities.

Another area which will need careful consideration by business is the concept of data breach notification. If this is introduced, organisations that suffer a security or other incident involving personal information will, in some circumstances, be required to notify the people affected. The ALRC is currently recommending that organisation be required to notify only when a data breach may give rise to serious harm to any affected individual.

Overall the ALRC's report provides a depth of insight into Australia's privacy landscape and raises significant challenges for governments and business. There will be important discussions ahead, starting with the first stage of the Government's response over the next 12–18 months.

The ALRC's report is available at **www.alrc.gov.au**.

The information in this article was provided by Chris Cowper, Principal Consultant with Information Integrity Solutions Pty Ltd (IIS). IIS is a specialist privacy consultancy.