

No. 19: 23 December 2009

### Government releases first-stage response to ALRC report

On 14 October 2009, the Government released its first stage response to the ALRC report in a document entitled *Enhancing National Privacy Protection – Australian Government First Stage Response to the Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice* (October 2009). Among other things, the document sets out each relevant ALRC recommendation and the Government's associated response. The Government proposes to release exposure draft legislation implementing the first stage response in early 2010, at which time the precise scope and content of the proposed reforms will become evident. In the words of Senator Ludwig, the proposed changes will "... effectively rewrite the Commonwealth *Privacy Act 1988* for the 21st Century, the most significant reform to it since its inception" (Senator Ludwig, "Privacy – the way ahead", speech delivered to the International Association of Privacy Professionals – Australia/New Zealand, Melbourne, Wednesday 14 October 2009).

#### *First stage*

In general terms, the first stage response outlines the Government's position on 197 recommendations relating to:

- developing a single set of Privacy Principles for the handling of personal information by federal Government agencies and private sector organisations (which are currently separately regulated by the Information Privacy Principles and National Privacy Principles respectively) – the ALRC report recommended that the new Privacy Principles should address the following issues: Anonymity and Pseudonymity; Collection; Notification; Openness; Use and Disclosure; Direct Marketing; Data Quality; Data Security; Access and Correction; Identifiers; and Cross-Border Data Flows;
- redrafting and updating the structure of the Privacy Act;
- establishing a three-tiered scheme for binding Privacy Codes – this scheme will allow for the following three types of codes: codes voluntarily developed by organisations; mandatory codes developed by organisations at the request of the Commissioner; and mandatory codes developed by the Privacy Commissioner;
- addressing the impact of new technologies on privacy;
- strengthening and clarifying the Privacy Commissioner's powers and functions;
- introducing comprehensive credit reporting and enhanced protections for credit reporting information – this will allow five positive datasets to be included on an individual's credit report (eg repayment history) but will only apply once obligations proposed under the National Consumer Credit Protection Bill 2009 are in force; and
- enhancing and clarifying the protections regarding the sharing of health information and the ability to use personal information to facilitate research in the public interest.

Out of the ALRC's 197 recommendations, the Government accepted 141 (either in full or in principle), accepted 34 with qualification, noted 2 and rejected 20.

For an overview of key recommendations made by the ALRC, see at [37-7954] in the *Comprehensive Guide to Privacy Law – Private Sector*. The Office of the Privacy Commissioner has published a series of documents regarding key aspects of the Government's response (viewed 23 December 2009):

- summary of the Government's main responses, available at <[www.privacy.gov.au/images/stories/privacy-law/synopsis.pdf](http://www.privacy.gov.au/images/stories/privacy-law/synopsis.pdf)>;
- overview of proposals for a new binding credit code as part of credit reporting reforms, available at <[www.privacy.gov.au/materials/types/other/view/6959](http://www.privacy.gov.au/materials/types/other/view/6959)>;
- summary table outlining the effect of the Government's response regarding health privacy, available at <[www.privacy.gov.au/materials/types/other/view/6958](http://www.privacy.gov.au/materials/types/other/view/6958)>.

#### *Second stage*

Stage two of the Government's response will consider the 98 recommendations in the ALRC report not addressed in the first stage, which focus on:

- proposals to clarify or remove certain exemptions from the Privacy Act;
- introducing a statutory cause of action for serious invasion of privacy;

- serious data breach notifications;
- privacy and decision making issues for children and authorised representatives;
- handling of personal information under the *Telecommunications Act 1997*; and
- national harmonisation of privacy laws (partially considered in stage one).

The Government has not set a specific time-frame within which these recommendations will be addressed.

### Federal Privacy Commissioner's latest case notes

The Commissioner has released the following case notes relevant to the private sector:

- **Inappropriate collection from third party:** C and their partner (P) held a joint bank account with a financial institution (FI). After a family dispute, P advised FI of the dispute and amended the signature authority on the joint account. Several weeks later, a relative of P contacted FI to amend another account and provided further information about the dispute. FI further modified the joint account to block all withdrawals not signed by both C and P and later contacted C about the modification. *Outcome:* FI had breached NPP 1.4 as it was reasonable and practicable to collect C's personal information directly from C rather than from the third party. Further, FI had breached NPP 3 as, given the information was not provided by the account holders, it was subject to change and had an effect on C's finances, FI had not taken reasonable steps to check the accuracy of the information it collected from the third party. FI paid financial compensation to C: *M v Financial Institution* [2009] PrivCmrA 16.
- **Denial of access to confidential referee information:** C made an application to acquire a car dealership from an automotive company (AC). When assessing the application, AC contacted C's referees who provided information about C on condition that the information be treated confidentially. AC rejected C's application. C subsequently requested access to the information AC held about them. AC denied access on the grounds that to provide access would constitute a breach of its duty of confidence to the referees. *Outcome:* As C's information was subject to an equitable duty of confidence, AC was entitled to deny access under NPP 6.1(g) (providing access would be unlawful). AC could also rely on NPP 6.1(h) (denying access is required or authorised by or under law) to deny access as denying access was required by the law of confidence: *O v Automotive Company* [2009] PrivCmrA 18.
- **Disclosure of confidential client information:** C left their marital home due to domestic violence. C moved to a residence which was subject to break-ins and a violent attack. Because of safety fears, C moved again. To diminish the risk of harm, C changed their name by deed poll and concealed the new address from the ex-partner. C was a client of a Commonwealth agency (CA). C advised CA of the new address and change of name, requesting the information remain confidential. CA sent a letter to C, containing references to C's new name and address, at C's marital home. C's ex-partner viewed this information and contacted C. CA acknowledged the disclosure was not permitted under IPP 11 (similar to NPP 2.1), apologised and offered to pay an amount in compensation, which C rejected. *Outcome:* C sought compensation for health treatment and other costs incurred after the disclosure and for injury to feelings. CA agreed to pay some compensation but not the amount requested by C. C provided further evidence to support their claim for compensation. CA offered an increased monetary sum which C accepted in settlement of the matter: *P v Commonwealth Agency* [2009] PrivCmrA 19.
- **Misuse of customer information by staff:** An individual found a scrapbook in a shopping centre car park which contained an account of grievances and humorous incidents compiled by staff at a call centre of a retailer (R). Many of the accounts contained personal information about R's customers. R was unaware of the existence of the scrapbook prior to the investigation. Following an internal investigation by R, R stated that the existence of the scrapbook and its subsequent loss was an anomaly. R had in place measures to ensure the security of its customers' personal information, including: induction and ongoing privacy training for its employees, with particular focus on the use of, and access to, customer information; a quality control team which regularly monitored customer calls; and restricted staff access to customer information on a need-to-know basis. *Outcome:* Following its investigation, R took the following steps: employees responsible for the scrapbook were counselled about the proper use of customer information; these employees received a written warning advising that if they misused customers' personal information again their employment would be terminated; and additional privacy training was implemented with all customer service staff which emphasised how to correctly handle customers' personal

information. The Commissioner was satisfied that R had processes in place to meet its obligations under NPP 4.1 at the commencement of the investigation and that it took appropriate steps once it became aware of the incident – the Commissioner ceased the investigation: *Own Motion Investigation v Retailer* [2009] PrivCmrA 25.

- **Health service provider not entitled to make default payment listing:** C underwent a medical procedure and received an invoice from the health service provider (HSP), which remained unpaid. HSP sent follow up invoices and a final letter of demand advising that it would list a payment default on C's credit file if the invoice was not paid within 14 days. HSP subsequently listed the payment default. Later, C paid the debt. C alleged the payment default did not relate to credit as defined by the Act. HSP argued it was a "credit provider" within the meaning of the Act because it provided a loan and that loan was not paid within 7 days. HSP did not provide any payment terms or methods prior to surgery, but argued that, given the invoice did not explicitly state that immediate payment was required, a lack of payment terms should be construed as allowing a reasonable time, in excess of 7 days, for payment. *Outcome:* In rejecting HSP's argument, the Commissioner found that HSP did not have a sufficient credit relationship with C and was not a credit provider and, subsequently, breached the Act by listing the payment default. HSP apologised, removed the listing, ceased its practice of reporting overdue accounts to a credit reporting agency and made a financial settlement: *L v Health Service Provider* [2009] PrivCmrA 15.
- **Failure to update mailing address:** An individual advised the Commissioner that a financial institution (FI) had been sending bank account statements to their previous residential address for several years, despite these statements consistently being returned, marked "return to sender – address unknown". The Commissioner commenced an own motion investigation. FI had in place a process to deal with such mail. The process was set out in a manual of which all staff had been made aware. The process entailed FI checking for issues such as duplication, and then working through its customers' mailing records to ensure they were up-to-date. This involved attempting to contact the relevant customer using all available contact information. If the financial institution was not able to establish contact with the customer, it changed the customer's mailing address to FI's address and placed a "stop" on the customer's account. FI had placed a "stop" on the relevant customer's account. *Outcome:* There was no breach of NPP 3. FI's processes were sufficient: *Own Motion Investigation v Financial Institution* [2009] PrivCmrA 12.
- **Disclosure of employee information to assessing doctor:** (*editor's note:* employee records are exempt from the NPPs; however, this case note will be relevant to employers who generally seek to treat employee records in accordance with the NPPs) C was an employee of a Commonwealth agency (CA). CA had undertaken an investigation into C's conduct. C submitted a workers' compensation claim and CA arranged for a doctor to assess C to determine their fitness for duties and any barriers to their return to work. CA provided the doctor with personal information about C, including information relating to the investigation. C claimed CA had no need to disclose such information. IPP 11.1(a) (similar to NPP 2.1(a)) permits an agency to make a disclosure to a person other than the individual concerned – otherwise prohibited under IPP 11 – if the individual is reasonably likely to have been aware that information of that kind is usually passed on to the recipient. *Outcome:* C was reasonably likely to have been aware (even if not actually aware) that the information would be passed to the doctor because: CA had notified C that the purpose of the doctor's appointment was to assess their ability to return to the workplace; and CA notified C beforehand of the disclosure. CA subsequently provided C with a copy of the information it supplied to the doctor. It is usual practice in workers compensation matters for an employer to provide an assessing doctor with all relevant information about the employee. As the subject matter of the agency's investigation may have presented a barrier to C returning to work, the information was relevant to the assessment of C's condition. The disclosure was permitted under IPP 11.1(a): *J v Commonwealth Agency* [2009] PrivCmrA 13.
- **Surveillance of incorrect person:** C was placed under surveillance by a company (CO) that had mistaken C for one of its employees. C had a relative who worked for CO and who had been on leave for an extended period. C wrote to CO requesting access to any recordings or photographs it had of them. Four weeks passed without a response. C complained to the Commissioner requesting that CO destroy any recordings or photographs of C or, alternatively, provide C with access to their personal information. *Outcome:* CO advised it had not received C's letter but was willing to destroy all personal information it had about C, including that held by its solicitor, which it later did and confirmed in writing. C was

satisfied with CO's actions and the Commissioner closed the complaint: *R v Company* [2009] PrivCmrA 21.

- **Credit reporting – listing statute barred debt.** A credit provider (CP) listed a default on C's consumer credit information file after the debt became statute barred. CP subsequently identified C's debt as statute-barred, and sent a notice to the credit reporting agency. However, the notification did not indicate that the listing was inaccurate, and did not request that the listing be removed. *Outcome*: CP breached para. 2.8 of the *Credit Reporting Code of Conduct* by listing a default on C's consumer credit information file after the debt became statute barred. CP had also breached para. 2.5 of the Code (which relates to rectifying inaccurate or non-permissible information): *Q v Credit Provider* [2009] PrivCmrA 20.
- **Credit reporting – data quality.** A debt collection agency (DCA) listed a debt on C's consumer credit information file. C claimed the debt was a "provable debt" on C's bankruptcy Statement of Affairs and therefore should not have been disclosed to the credit reporting agency. C also alleged that DCA failed to advise the credit reporting agency on becoming aware that the debt was incorrectly listed. Before providing C's details to the credit reporting agency, DCA had sent a written Notice of Assignment to C stating that the debt had been assigned to DCA, that payment was requested and that C's details may be passed on to a credit reporting agency. C did not dispute the debt until after it had been listed. If a debtor disputed their debt, DCA's normal process was to verify the debt with the original credit provider before passing the debtor's details to a credit reporting agency. *Outcome*: DCA's process constituted reasonable steps under both NPP 3 and s 18(G)(a) of the credit reporting provisions. DCA also had "reasonable grounds" for considering the information it passed to the credit reporting agency was correct for the purposes of s 18E(8)(b): *S v Debt Collection Agency* [2009] PrivCmrA 22.
- **Welcome letter erroneously sent to non-customer.** C received a letter from a telecommunications company (TC) welcoming them as a new customer. C was not, and never had been, a customer of TC. TC had obtained C's personal information from a related telecommunications company (in accordance with the related body corporate exemption under s 13B) after a corporate acquisition and had sent the letter by mistake. *Outcome*: The use of C's personal information was consistent with the primary purpose for which it was originally collected (namely, providing a telecommunications service to C), even though the welcome letter was sent in error. Further, TC had reasonable processes in place to ensure data quality, as required by NPP 3: *U v Telecommunications Company* [2009] PrivCmrA 24.
- General annotations from case notes:
  - **Collection of unsolicited information:** An organisation collects personal information if it gathers, acquires, or obtains information from any source and by any means (irrespective of whether the information was sought by the organisation): *M v Financial Institution* [2009] PrivCmrA 16.
  - **Employee records exemption:** Disclosure by an employer of an employee's personnel and related files to a contractor to enable the contractor to investigate the handling of complaints made by the employee will generally be "directly related" to the employment relationship: *N v Commonwealth Agency* [2009] PrivCmrA 17.

### **VSC: Statutory right of access not "possession" for discovery purposes**

In *Psolidis v Norwich Union Life Australia Limited* [2009] VSC 417, Cavanough J considered the relationship between a right of access under the *Health Records Act 2001* (Vic) and possession of documents for the purposes of discovery. In doing so, his Honour summarised a series of Western Australian cases which have considered the same issue in the context of the *Privacy Act 1988* (Cth). His Honour effectively concluded that a right of access under the Victorian statute does not amount to "possession" for discovery purposes, although a different conclusion has been reached in relation to the Commonwealth Act.

In *Psolidis*, the defendant sought orders enabling it to inspect records held by a plaintiff's doctors. The principal question in the case was whether the doctors' records were in the patient's "possession, custody or power" following the enactment of the *Health Records Act 2001* (Vic). If so, the defendant could have been entitled to an order for discovery. The defendant argued that the Act gives Victorians a "legal right to access their medical records". In rejecting the submission, Cavanough J stated (at [38]):

That proposition is overstated ... [T]here are significant exceptions to the right of access. And it is a "legal" right in a limited sense only. The right cannot be directly enforced in the usual way in which legal rights are enforced, namely in the ordinary courts. In some cases it may

not be able to be enforced at all, much less immediately. Overall, in my opinion, it does not answer the *Lonrho* [*v Shell Petroleum Co Ltd* [1980] 1 WLR 627] description of a “presently enforceable legal right (of access to medical records)”. Nor does it provide to Victorians “an actual and immediate ability to examine (their medical records)”, in the sense referred to by Doyle CJ in *Taylor v Santos* [(1998) 71 SASR 434].

Cavanough J continued (at [110]-[116]):

In support of its arguments on “power”, [the defendant] cited the very brief decision of Registrar Wallace of the Western Australian District Court in *Royal v Alcoa of Australia Limited* [[2005] WADC 170]. Registrar Wallace held that relevant medical records relating to the plaintiff in the possession of a medical centre and a hospital were within the power of the plaintiff by virtue of the *Privacy Act 1988* (Cth) and the Guidelines thereunder published by the Office of the Privacy Commissioner. The Privacy Act (in Schedule 3) incorporates the National Privacy Principles. They are similar in format to the Health Privacy Principles set out in the (Victorian) Act. The exceptions and exemptions are similar in content. However, Registrar Wallace did not set any of them out or examine any of them individually in the Court’s reasons. The Registrar simply said that “none of [them], on their face, apply in the present case”. The Registrar was satisfied that the statutory right to “access”, as administered in practice under the Privacy Commissioner’s Guidelines, amounted to a right to inspect the documents in one way or another, as the relevant organisation saw fit. Without more, he concluded that the plaintiff had a presently enforceable legal right to obtain inspection of the documents and that, on the authority of *Lonrho*, the documents were therefore in the plaintiff’s power.

As is apparent from the above, I take a different view of the requisite approach to the corresponding exceptions and exemptions in the Act.

Registrar Wallace apparently found it unnecessary to examine the review or enforcement provisions in the Privacy Act. One reason for this may be that s 98 of the Privacy Act enables any person to apply (directly) to the Federal Magistrates Court or to the Federal Court for an injunction to restrain a contravention of the Act. It has been determined that this avenue of enforcement is free-standing and is not diminished by other provisions in the Act, such as the provisions for complaints to and determinations by the Privacy Commissioner. There is no provision equivalent to s 98 in the Health Records Act. Partly for that reason, I have characterised the complaint and enforcement provisions of the Health Records Act in a way different from the way in which Registrar Wallace apparently viewed the corresponding provisions of the Privacy Act in *Alcoa*.

Accordingly, nothing in *Alcoa* persuades me to depart from what I have said above.

[The plaintiff] points out that in *Chavarría v Rodman* [[2006] WADC 42] Principal Registrar Gething of the District Court of Western Australia declined to follow *Alcoa*. However, with respect, I have difficulties with the reasoning in *Chavarría* as well. The Principal Registrar expressly departed from the approach taken in *Alcoa* in one respect only. He found that the right to have “access” to a document under the *Privacy Act 1988* (Cth) did not amount to a right to obtain a copy or to a right to allow a third party (such as an adversary in litigation) to inspect the original, and concluded that, in consequence, the relevant documents were not in the “power” of the party for discovery purposes. The Principal Registrar apparently considered that this reasoning was in line with *Taylor v Santos and Theodore* [(1998) 71 SASR 434] But, as I have indicated, in my view it was not.

The proposition that, for discovery purposes, the Privacy Act probably does not give individuals “power” over documents in the possession of organisations was put forward recently by a Judge of the District Court of Western Australia, Davis DCJ, in *Integrated Management Services Pty Ltd v Inches* [[2009] WADC 41]. However Davis DCJ made this comment relying principally on the reasoning in *Chavarría*, with which, as indicated above, I do not agree.

*Chavarría* and *Integrated Management Services* may implicitly stand for the proposition that, absent the problem about obtaining copies, the *Privacy Act 1988* (Cth) would generally give “power” over documents to individuals for discovery purposes. However, if so, I would simply not be persuaded by that to depart from my analysis of the effect of the Victorian Act (notwithstanding that, under the Victorian Act, copies are available at the election of individuals who are entitled to access). (footnotes omitted)

Cavanough J also considered *Nixon v Channel 4* [1997] EWCA Civ 1117. In that case, the Court of Appeal of England and Wales briefly considered the relationship between discovery and the *Access to Health Records Act 1990* (UK). The court considered that the Act did not render a patient's medical records in the possession of a third party discoverable by the patient. However, the reason given by the Court of Appeal for that conclusion was that the patient had no right to demand possession or custody of the original documents. Cavanough J concluded (at [106]):

Similarly, there is no right under the Victorian Act to demand possession or custody of original medical records. However the weight of authority, at least in Australia, indicates that a mere right to inspect documents (or actual and immediate ability to do so) is generally sufficient to generate an obligation to make discovery of them.

...

In *Nixon v Channel 4* ... the Court of Appeal apparently saw no occasion to consider whether there were other reasons why the *Access to Health Records Act 1990* (UK) did not put medical records within the "power" of the individual. So it seems that, in the end, *Nixon v Channel 4* ... does little to illuminate the questions before me. (footnotes omitted)

### **SCNSW: position as to development of tort of privacy "a little unclear"**

In *Chan v Sellwood* [2009] NSWSC 1335, Davie J observed that the position regarding the development of a tort of invasion of privacy in Australia is "a little unclear". His Honour stated (at [37]):

Whether the law of Australia recognises a tort for breach of privacy is a little unclear. What the High Court said about it in *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63; (2001) 208 CLR 199 at [40]- [42] and [106]-[132] and [189]-[190] would not appear to preclude the emergence of such a tort. In *Grosse v Purvis* (2003) Aus Torts Reports 81-706 Skoien J of the Queensland District Court found that there was such a tort (see at [421]-[447]). Heerey J in *Kalaba v The Commonwealth* [2004] FCA 763 thought that the weight of authority was, at that time, against the proposition that there was such a tort but in *Gee v Burger* [2009] NSWSC 149 McLaughlin AsJ thought at [53] that the matter was arguable.

### **Health services: new guidelines for disclosure of genetic information**

Guidelines entitled *Use and disclosure of genetic information to a patient's genetic relatives under section 95AA of the Privacy Act 1988 (Cth) – Guidelines for health practitioners in the private sector* (December 2009) have been issued by the National Health and Medical Research Council and approved by the Privacy Commissioner under s 95AA of the Privacy Act. The Guidelines specify the requirements that must be met by health practitioners in the private sector if they choose to use or disclose genetic information without patient consent under NPP 2.1(ea).

Further, the Privacy Commissioner has also issued Temporary Public Interest Determination (TPID) No 2009-1A (which gives general effect to TPID No 2009-1) allowing health practitioners to collect or use the contact details of a patient's genetic relatives in situations where the s 95AA Guidelines permit the disclosure of information (the Government has indicated in its recent first stage response to the ALRC Report 108 that it intends to amend the Privacy Act to allow this collection or use). TPID 2009-1A provides:

Under TPID 2009-1, a health service provider can only collect or use the contact details of a patient's genetic relatives if they are satisfied that:

- a) it is impractical to gain the consent of the genetic relative and
- b) the applicant intends to use the contact details to inform the relative of the potential consequences, to their own health, of genetic information obtained from the patient for the relative's own health and
- c) the applicant has a reasonable belief that this is necessary to lessen or prevent a serious threat to the life, health or safety of the genetic relative and
- d) where consent has not been obtained from the patient for the disclosure of their genetic information, the disclosure will be made in accordance Guidelines issued under section 95AA of the Privacy Act.

### **Do Not Call Register to be extended to cover business numbers**

The Do Not Call Register Legislation Amendment Bill 2009 was introduced into the House of Representatives on 26 November 2009. The Bill is a response to concerns regarding the rate at which unsolicited marketing faxes have grown in recent years. It will extend the Do Not Call Register to enable all persons, including individuals, businesses, government and organisations, to register telephone and fax numbers on the Register. At present, telephone numbers used primarily for business or public use, emergency service numbers and fax numbers cannot be listed on the Register.

The main elements contained in the Bill are:

- a provision that makes all Australian telephone and fax numbers eligible to register on the Register;
- a prohibition on sending unsolicited marketing faxes to an Australian number which is registered on the Register, subject to certain exemptions;
- a requirement that agreements for the sending of unsolicited marketing faxes must require compliance with the Act (this requirement is aimed at organisations which may contract with another party to provide fax marketing services on their behalf);
- civil penalty provisions for breaches of the new provisions;
- the introduction of “registered consent” which will give all new registrants the option of consenting to receive telemarketing calls or marketing faxes relating to particular industry classifications at the time of listing their number on the Register (the default position will continue to be that registrants are opting-out of all telemarketing calls and marketing faxes);
- conferring powers on the Australian Communications and Media Authority (ACMA) to make determinations about the circumstances in which consent will be inferred for unsolicited telemarketing calls and marketing faxes to business numbers (this is a reserve power and there will be no change to the existing inferred consent provisions under the Act); and
- consequential amendment to Part 6 of the *Telecommunications Act 1997*, to allow the fax marketing industry to make industry codes, and the ACMA to make industry standards for the fax marketing industry, consistent with the existing arrangements which allow codes and standards to be made for the telemarketing industry. The ACMA will have the power to make an industry standard relating to the fax marketing industry.

### **National Human Rights Committee recommends Human Rights Act**

On 30 September 2009, the National Human Rights Committee reported to the Attorney-General on its review of human rights in Australia, which commenced in December 2008. Among a raft of other reforms, the report recommended the enactment of a federal Human Rights Act. The Act would only impose obligations on federal public authorities. The Committee recommended that the Act adopt a “dialogue model”, which has been implemented in New Zealand, the United Kingdom, the ACT and Victoria. Under this model, the Act would set out a list of human rights and accord the three branches of government – the executive, the legislature and the judiciary – specific roles in relation to protection and promotion of those rights. This model was recommended in favour of alternative models, including the Canadian legislative model (which would allow courts to declare legislation inoperative if it is found to be inconsistent with human rights), a “parliamentary” model (which would seek to protect human rights through democratic institutions and independent oversight mechanisms, rather than through judicial review) and an “entrenched” model (which would involve amending the *Australia Act 1986* to include a list of rights). The Government has indicated that it will issue a formal response once it has considered the report.

### **New rules for NSW residential tenancy databases**

A draft Residential Tenancies Bill 2009 (NSW), released on 4 November 2009, proposes to update and reform the NSW residential tenancy laws. Among other things, the draft Bill proposes new rules for using tenancy databases and for resolving disputes about the information on such databases. The Bill incorporates and reforms the existing requirements of the *Property, Stock and Business Agents Regulation 2003* that deal with residential tenancy databases. The draft Bill limits the information that can be listed in a database, the period of time information can be kept and allows for access to the information by persons named on a database. The draft Bill also provides for disputes to be heard and resolved in the Consumer, Trader and Tenancy Tribunal. The provisions are consistent with draft national provisions

regarding residential tenancy databases being prepared by the Ministerial Council on Consumer Affairs. The public consultation period ended on 18 December 2009.

### **APEC Ministers endorse Pathfinder documents**

On 12 November 2009, APEC Ministers endorsed the following Pathfinder projects documents which had been finalised at the APEC Data Privacy meetings held in Singapore on 27 and 28 July 2009:

- a template Cooperation Arrangement for Cross-Border Enforcement to facilitate assistance and information sharing between data protection authorities;
- a template cross-border complaint handling form; and
- a directory of data protection authorities.

The documents form key parts of the voluntary system of cross-border privacy rules based on the APEC Framework.

### **Information Commissioner Bill and FOI Amendment (Reform) Bill introduced**

The Government introduced the *Information Commissioner Bill 2009* and the *Freedom of Information Amendment (Reform) Bill 2009* into the Parliament on 26 November 2009. The Bills have since been referred to the Senate Finance and Public Administration Legislation Committee for inquiry and report by 16 March 2010. Public submissions close 28 January 2010.

Among other things, key proposals in the Bills include establishing two new statutory positions of Information Commissioner and FOI Commissioner and, further, bringing them together with the Office of the Privacy Commissioner (OPC) in a new Office of the Information Commissioner (OIC). As such, the OIC will be headed by the Information Commissioner (being a new office holder) who will be supported by the Privacy Commissioner (being an existing office holder) and the FOI Commissioner (being a new office holder). The Information Commissioner would be solely responsible for the Information Commissioner functions and for the production and tabling of the OIC's annual report. The Privacy Commissioner will be largely responsible for the privacy functions and the FOI Commissioner for the FOI functions.

**DISCLAIMER:** This publication is intended solely to keep readers up-to-date with developments in privacy law. It is not intended to be, nor constitutes, legal or other professional advice and should not be used or relied upon as a substitute for such advice. Before relying on the contents of this publication, users should verify its currency and accuracy with primary sources or seek professional advice as required. The publishers and every other person involved with the production of this publication disclaim all liability for any form of loss or damage suffered by any person as a result of any error or omission within, or use of or reliance on, this publication.