COMPARATIVE STUDY
ON
DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES,
IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS


COUNTRY STUDIES
(Douwe Korff, Editor)

B.2 – AUSTRALIA

BY

Graham Greenleaf

Submitted by:

LRDP KANTOR Ltd (Leader)
In association with

Centre for Public Reform

(Final edit – May 2010)
AUSTRALIA
By Graham Greenleaf

I. Context of information privacy in Australia

1. Introduction: The current state of Australian privacy reform

The Commission has previously received two expert reports by Bygrave and Greenleaf on the adequacy of Australia’s privacy protection, in 2005 and 2006 (Bygrave and Greenleaf, 2005, 2006). This report draws on that previous work, abbreviating it or referring to it as appropriate for this briefer report, and bringing it up to date where needed.

From 2006 privacy issues in Australia have been dominated by the reference given by the Australian federal government to the Australian Law Reform Commission (ALRC) to comprehensively review Australia’s Privacy Act 1988 (which covers both the private sector and the federal public sector), and the similar reference to the NSW Law Reform Commission (NSWLRC) to review the public sector privacy law in New South Wales (the most populous State). Greater national uniformity is one of the objectives of these reviews. The ALRC delivered its Report 108 For Your Information: Australian Privacy Law and Practice (ALRC, 2008) in mid-2008. The NSWLRC has yet to do so except in relation to a statutory privacy action (NSWLRC, 2009).

The federal Government for the past year been preparing its response to the ALRC’s recommendations, and on 14 October 2009 published its response to most of the ALRC’s recommendations, confirming its proposals for legislation (AusGov, 2009). It will deal in a second response with those recommendations concerning exemptions from the legislation, a statutory privacy action, and data breach notification, children’s privacy and telecommunications privacy. The government proposes to release an ‘exposure draft’ Bill in early 2010, with the intention of introducing legislation into Parliament later that year. Because the government has decided to reject or modify many of the ALRC’s recommendations, it is only now that we can say with any confidence at all what the near-future shape of Australia’s privacy legislation might look like.

Given these factors, a major aim of this brief report must be to explain how the government's proposed reforms relate to the issues under examination by this 'New Challenges' Project, rather than to examine many aspects of Australian privacy law on which the Commission already holds detailed reports by Bygrave and Greenleaf.

However, although mention is often made of 'adequacy' as used in the Directive, no attempt is made in this report to make any assessment of what these proposed changes might mean for the adequacy of Australia's privacy regime, given that any changes are as yet far from certain.

2. Political and economic context

Australia is a federation of eight states and territories, all of which have a common law tradition. The political context of privacy protection in Australia is one of unbroken ‘normality’: Australia’s peaceful achievement of independent nationhood, her continuous
democratic history since Federation in 1901, her almost entirely peaceful internal political development, and the relatively low level of external threats (due in part to Australia’s lack of land borders). Perceptions of both internal and external threats to security continue to have adverse effects on privacy protection, but Australian democracy and privacy have never had to ‘recover’ from authoritarian rule as has happened in other countries.

As a result of the severe limits in Australia’s constitution, common law rights and international obligations in relation to protection of privacy (as outlined in the following sections), Australian law’s protection of privacy has principally involved legislation, or attempts to legislate. In a federation with nine jurisdictions, the question of which Parliaments have the constitutional power to legislate to invade or protect privacy is important. The Australian federal Constitution gives the States the residual powers to legislate where there is no specific head of Federal power, and there is none in relation to privacy. The Federal government has wide constitutional powers to legislate in relation to many areas especially telecommunication, corporations, and foreign affairs. It has relied on these heads of power to legislate generally in relation to privacy in the credit industry (1991) and the private sector generally (2000). Some States have also legislated in relation to surveillance, health information and other privacy issues affecting private sector bodies located in their jurisdiction, but can do so where these laws are capable of operating concurrently with the federal legislation. These potential clashes in legislative competence have not yet become an issue in Australia.

In recent decades governments have rarely controlled the upper houses of Australian Parliaments, due to the electoral successes of minor parties. This political fact has been very significant. It has given civil society organisations opportunities to defeat or modify government proposals, and helps explain their active role. The federal Privacy Act, its extension to the private sector, the NSW legislation and the federal data matching legislation have all undergone major modifications as a result. In NSW the government’s attempt to abolish the Privacy Commissioner was defeated by the upper house in response to a NGO campaign. The role of political conflict, and of NGOs, in shaping Australia's privacy protection is encapsulated in the defeat of the 'Australia Card' national ID card scheme in 1986-7, and the remarkably similar defeat of the 'Access Card' national ID scheme in 2006-07 (Greenleaf, 2007, 2007a, 2008).

3. Surveillance context

Some key aspects of Australian surveillance practices, and the legislative context on which the practices depend, are outlined here, and others later in this report. They are discussed in more detail in Greenleaf (2008) and references cited therein.

Closed-circuit television (CCTV) saturates the infrastructure of Australian cities, in city streets and train stations, on buses, trains and taxis, sporting venues and in crime hot spots. The ostensible reasons are personal safety, crime prevention, and recently anti-terrorism. One reason for this proliferation is that there is no legislation governing visual surveillance in public places. Australia is said to spend more money per capita on workplace surveillance equipment than most other industrialised nations. There is State-level legislation governing some workplace surveillance (by video, tracking devices, or computer), but it places few limitations on overt surveillance (for example, Workplace Surveillance Act 2005, NSW).
Telecommunications interception (‘wiretapping’) is under stricter legal control in Australia. It is illegal to intercept the content of calls except where authorised by a judicial warrant (Telecommunications (Interception) Act 1979). Legal intercepts are at much higher rates than comparable countries. An increasingly sophisticated system of financial transaction surveillance has been developed over nearly 20 years. Almost anyone dealing with $10,000 or more in cash is required to submit financial transaction reports to AUSTRAC (a federal agency), resulting in over 10 million reports per year (Financial Transactions Reports Act 1988). This surveillance network has been expanded very significantly by the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).

The statutory ‘parallel data matching’ system, explained later under data matching laws, is augmented by a huge amount of government data matching that takes place outside the controls of the data matching legislation. All of these compulsory extractions of data are ‘authorised by law’ exceptions to the non-disclosure requirements of the Privacy Act 1988. Mass surveillance of taxpayers and benefit recipients is a vast and complex enterprise by federal agencies. Its sources include uncounted private sector organisations and State government authorities (PCO Annual Report 2004-05, Table 3.7). Furthermore, this extra matching feeds data into the files of the five agencies involved in the parallel matching system, and therefore into its matching processes.

Since Australia does not yet have a national or state ID card or ID number, identification systems in Australia are usually built on the basis of production of alternative, or multiple, identification documents. The key federal numbering systems, the tax file number (TFN) and the Medicare number and card, are little used outside their intended domains. The Medicare card is often asked to be produced as part of a ‘100 point system’ proof of identity, but there is no ‘TFN card’ to produce. The main ID systems in current operation are: drivers’ licences (which are administered at State level); passports (held only by a minority of Australians); birth certificate copies (for particularly important events) and after that a profusion of different benefit cards, student cards, employer-provided IDs and so on. There is no requirement to carry ID in Australia, except that drivers must carry their licence when driving. Credit cards will usually be accepted without any other ID being produced, but it is common for a driver’s licence to be requested when cashing cheques, and for the licence number to be noted on the cheque. Post-2001, ID is requested more frequently, for example in order to post a parcel. Some states now issue ‘non-driver’ photo ID cards to serve the same identification function as a driver’s licence.

Private sector data surveillance of Australians is still characterised by personal data held primarily within industry sectors. Such data are aggregated very efficiently within particular sectors, but with limited ‘crossover’ either between private sectors or from the public sector. In credit reporting, Veda Advantage’s service (formerly the industry-owned CRAA) claims to hold personal data on more than 14 million consumers, out of a total adult population of 21 million in 2007 (Veda Advantage’s Consumer Credit Enquiries). It has had over 90% of all consumer credit reporting business since at least the late 1970s. Credit bureaux can only store a legislatively-defined range of ‘negative’ information (excluding information about rental history, insurance defaults, reasons for job changes etc). Default information other than ‘clearouts’ and bankruptcies only stays on file for five years. In insurance reporting, Veda Advantage also runs Australia’s largest insurance claims database, separate from its credit files. It claims it is contributed to by almost all of Australia’s insurance companies and
contains more than 18 million insurance claims of individuals and companies dating back ten years, complemented by public registry sources. Access is limited to the insurance industry.

The health services sector, which more than any other straddles the public and private sectors, does not have any single national or regional method of surveillance of medical histories as yet. Employers, insurers and others seeking details of a person’s medical history are therefore forced to obtain the patient’s consent to obtain reports from their most recent treating doctor, and do not have any comprehensive source. As explained later, this is now undergoing major change.

Private sector access to personal information in registers held by public agencies varies widely across States and Territories because of varying legislation (or lack of it). At the ‘accessible’ end of the spectrum, there are open online registers of bankrupts and company directors, land ownership, and encumbrances over motor vehicles. Vehicle registration records are normally only accessible for good cause (e.g. locating parties to accidents). Local councils have open registers of property development proposals, but usually only for inspection in person. Australia adopts the practice of other common law countries of allowing public online access to fully identified court decisions, and allows republication by third parties. At the ‘inaccessible’ end of the spectrum, access to records of convictions or criminal charges is generally prohibited. Some companies such as Acxiom are attempting to aggregate publicly available personal information.

The domestic direct marketing industry operates carefully compared with some countries. Direct marketers are generally required to offer an opt-out in marketing communications (Privacy Act 1988). Do-Not-Call list legislation commenced operation in mid-2007, and penalties imposed have already been significant, such as a $100,000 fine against Telstra. There has never been significant domestic email spamming. Nevertheless, the federal SPAM Act 2003 imposes severe penalties on any activities resembling spamming. Its main effect is probably to prevent anyone using Australia as a base for international spamming operations. The first prosecution under the Act resulted in financial penalties of $4.5M for the company concerned, Clarity1, and $1M for its principal.

4. Social attitudes to privacy

Privacy is usually an elite concern in Australia as a public issue, but is capable of quickly seizing public attention and widespread media coverage. This ensures that policymakers do not ignore privacy issues, but instead devote resources to managing them.

By the mid-1970s there was considerable media attention to privacy issues throughout Australia, arising from fear of computers (Australian businesses being relatively ‘early adopters’), from notorious abuses of ‘Special Branch’ police political surveillance, and from widespread fears of the actions of credit bureaux. Although the Australian Law Reform Commission privacy investigations from 1976 helped keep the issue alive, privacy was less prominent as a public issue throughout the early 1980s. The ‘Australia Card’ defeat in 1987 gave privacy credibility as a national issue, and it has remained a significant public issue since then, but there has been no equivalent extra-ordinary issue to galvanise opinion. The result has been (in the view of privacy advocates) that Australians have suffered the fate of the boiling frog: that each incremental increase in surveillance has gone largely unnoticed.
Public concern in Australia for privacy and data protection interests is generally high, at least in the abstract, according to survey data, with widespread public support in Australia for legal safeguards of these interests, but poor community knowledge of existing safeguards or institutions. Australian organisations in both the public and private sectors seem generally to regard public concern about privacy issues as legitimate and as a significant factor to take into account when dealing with information about their customers and clients. They seem to be generally supportive of existing privacy laws.

Elite participants interested in privacy issues are well served in Australia, in the sense that it is possible for individuals to have an impact on policy development, and there are NGO structures to facilitate their doing so. Although it is a big country geographically, Australia has a relatively small civil society and most significant meetings are held in Canberra or Sydney. Attendance is often possible for the policy elites residing in those cities. Ministers, Opposition spokesmen, Privacy Commissioners and other policymakers are relatively accessible. Consumer groups, including specialist telecommunications, credit and medical consumer groups, as well as the broad-based Australian Consumers Association, take a continuing interest in privacy issues, as do some general civil liberties organizations. Since 1987 the Australian Privacy Foundation (APF, 2007), formed to oppose the Australia Card, together with its members in other roles, have been the most consistent and effective privacy advocates in Australia, though still rarely gaining the policy changes they seek.

Business groups are almost always better resourced than NGOs, and key groups have much more ready access to Ministers than do NGOs. However, business groups have often not been as adept in using the press on key privacy issues as have NGOs, and they do not uniformly achieve their objectives. A privacy issue is never a hopeless cause in Australia, nor is victory assumed.

5. International obligations in relation to privacy

International Covenant on Civil and Political Rights 1966

The only treaty imposing obligations on Australia to protect privacy is the International Covenant on Civil and Political Rights 1966 (ICCPR 1996), Article 17 of which requires privacy protection. While this has no direct effect in Australian domestic law, Australia is one of the few countries in the Asia-Pacific to have also acceded to the Covenant’s First Optional Protocol allowing for individual complaints (‘communications’) to the UN Human Rights Committee (UNHRC). Nicholas Toonen, a gay rights activist from Tasmania, objected to his State’s Criminal Code which made all sexual contact between consenting male adults in private a crime. Instead of trying to protect his sexual privacy through Australia’s Courts, he took his case to the Human Rights Committee of the United Nations, under Article 17 (Toonen v Australia (1994). The UNHRC held that adult consensual sex was within the meaning of ‘privacy’. The Tasmanian legislation meant it was not properly protected, and Australia was in breach of the ICCPR. Although countries cannot be compelled to implement UNHRC findings, the Federal Labor government subsequently legislated, relying on its constitutional power over foreign affairs, to make the Tasmanian legislation ineffective. The protection of privacy in Australia through international law, while very limited, is possible.
Despite Australians’ minimal obligations under international privacy agreements, Australia has had a significant role in the development of those standards, and its domestic legislation has in fact been influenced by those international developments. Three agreements have had key influences in each of the last three decades.

**OECD Guidelines on Privacy and Transborder Data Flows, 1981**

The OECD privacy Guidelines (1981) were adopted by Australia in 1984. There is no method of enforcing the Guidelines, either by OECD members or by individuals, and no external assessment of whether they have ever been implemented (though their terms require implementing legislation). Australia implemented them for its federal public sector in 1988, but took until 2001 to implement them in the private sector, and has put no pressure on State public sectors to implement them. The OECD Guidelines clearly influenced the information privacy principles (IPPs) in the Australian Law Reform Commission's Report Privacy (1983), and via that route the public sector IPPs in the Privacy Act 1988 which mirrored them fairly faithfully. Since then there has been a ‘ripple down’ influence through all Australian privacy laws, which all probably satisfy the OECD Guidelines’ reasonably weak requirements. Australia subsequently became a strong promoter of the OECD Guidelines as the ‘only credible international standard’ (Ford, 2002) in the negotiations over the APEC Privacy Framework.

**EC privacy Directive 1995**

Throughout the 1990s, the EU privacy Directive (1995) was a constant feature of elite debates and newspaper reportage in Australia because of the success with which privacy advocates played the ‘adequacy card’. The content of the Directive had some influence on the federal Privacy Commissioner’s NPPs in relation to ‘sensitive’ information and inclusion of a data export provision. However, the European Union is not yet satisfied that Australia's private sector privacy legislation is ‘adequate’ in European terms. Europe’s data protection Commissioners were very critical of the Australian legislation (Article 29 Working Party, 2001), with its findings disputed by Australia’s federal government (as exemplified by Ford, 2002). Due to the passage of nearly fifteen years with few significant findings of 'adequacy' (or lack of it) by the European Commission, the argument of the need for an adequacy finding is no longer of much interest to Australian policy-makers or the media, though the EU Directive retains influence as an international standard.

**APEC Privacy Framework**

In the present decade, the international focus of Australian policy has turned to APEC (Asia Pacific Economic Cooperation) and the development of the most recent international privacy instrument, the APEC Privacy Framework (2004, completed 2005). Australia had a significant influence on the development of the Framework, the first draft of which was by an Australian committee chair (Greenleaf, 2003a). The principles in the APEC Privacy Framework are weaker than in Australia’s existing laws and are at best an approximation of the OECD Guidelines. The APEC framework has had no influence on Australia's privacy laws except that the Government is now proposing a new data exports principle which superficially bears some resemblance to APEC’s 'Accountability Principle' but is in fact very different. The APEC Framework does not expressly reject the legitimacy of data export restrictions and therefore set itself against EU notions of ‘adequacy’, contrary to the fears of some commentators (Greenleaf, 2006). The final framework said virtually nothing on the
subject and there is now relatively little chance that APEC will develop into an anti-EU bloc. The history of the APEC Privacy Framework is reviewed in Greenleaf (2009)

Australia has therefore had twenty years’ involvement in developing international privacy standards as an influential non-EU participant. Its chosen role has been to advocate privacy protection as a legitimate and unavoidable issue, but one that can be managed in the interests of business and government, rather than advocacy of privacy as a human right.

6. Constitutional protections and Human Rights Charters

Australia lacks any significant constitutional protection of privacy at Federal or State level. There is no entrenched ‘Bill of Rights’ in the constitution of any Australia jurisdiction, so there is nothing there on which Courts can build privacy rights. The closest thing to a constitutional right of privacy is that common law courts, when interpreting legislation, will do so in ways which avoid interference with ‘fundamental rights’ unless the statutory language clearly directs them to. On the other hand there are no ‘first amendment’ problems: there are no constitutional freedom of speech rights which can prevent legislative restrictions on disclosures of personal information. Other than some very limited protections of political speech. If governments want to prevent access to Court records, limit who can access credit bureaus, or forbid disclosures of any personal information, there is no constitutional bar to their doing so.

However, there is a trend towards the adoption of Human Rights Acts or Charters at State level, which can be invoked in relation to privacy rights.

Thus, Victoria's Human Rights and Responsibilities Act 2006 includes privacy in the human rights it aims to protect. It imposes obligations on all public authorities to act in a way compatible with human rights, requires statements of compatibility for all legislation introduced into Parliament, and confers jurisdiction on the Supreme Court to declare that a particular statutory provision cannot be interpreted consistently with human rights (a Declaration of Inconsistent Interpretation), requiring the Government to table a response in Parliament within six months (see Bygrave and Greenleaf, 2006: 2.1). The Australian Capital Territory passed similar legislation in 2004 (see Bygrave and Greenleaf, 2005: 3.4.4).

7. General law actions for interference with privacy

There are some protections of privacy rights at common law and in equity; and some statutory actions are proposed.

Common law and equity protections

Until 2001, it was a widely held view that the High Court's 1937 judgment in Victoria Park Racing and Recreation Grounds Company Ltd v Taylor & Others (1937) 58 CLR 479 had conclusively determined that there does not exist a tort for breach of privacy under Australian common law. The validity of this view is now questionable in light of the High Court decision in Australian Broadcasting Commission v Lenah Game Meats Pty Ltd (2002) 208 CLR 199. Shortly afterwards Skoien J of the Queensland District Court held in Grosse v Purvis [2003] QDC 151 that it was time to recognise the existence in Australian common law of a right of an individual person to privacy, breach of which could give rise to a civil action
for damages, and awarded very significant damages in a case that was essentially about stalking. The case subsequently settled before an appeal was heard (see Bygrave and Greenleaf, 2005: 3.5.1 for discussion of both cases).

In *Jane Doe v ABC* (2007) a Victorian District Court awarded high damages on the basis of the existence of tort of invasion of privacy. Following a sentencing hearing of YZ for rape within marriage of Jane Doe, ABC radio broadcast details including the name of YZ, that the offence was rape, the suburb in which the rapes took place, and in one broadcast the real name of Jane Doe. Many listeners subsequently attempted to contact her and her family. Evidence was given of the substantial and long-lasting psychological damage that this caused to her. Two ABC journalists subsequently pleaded guilty to breaches of legislation prohibiting identification of rape victims. Ms Doe then sued both the journalists and their employer (the broadcaster), and one of her grounds was a breach of a common law right of privacy. A District Court found in her favour on this and other grounds including breach of an equitable obligation of confidence, and awarded her A$234,000 damages. The case was on appeal but settled before trial.

The question of whether there is a common law action for invasion of privacy is therefore still not settled in Australia. However, the House of Lords in the UK has unanimously held that a tort of invasion of privacy as such is not part of English law (*Wainwright v Home Office* [2003] 3 WLR 1137), and this decision is likely to exercise greater influence on Australian courts than the contrary decision of the New Zealand Court of Appeal in *Hosking & Hosking v Simon Runting & Anor* [2004] NZCA 34.

**Proposed statutory actions for interferences with privacy**

The Law Reform Commission (NSWLRC) in the State of New South Wales in its Report 120 Invasion of privacy (2009) recommended that there should be a civil action (a tort) which can result in remedies 'if the conduct of another person invaded the privacy that the individual was reasonably entitled to expect in all of the circumstances having regard to any relevant public interest'.

Some aspects of the NSWLRC recommendations are considerably stronger than those put forward by the ALRC in its 2008 report: the ALRC tort requires a 'serious' invasion of privacy, but the NSWLRC does not; the ALRC requires the plaintiff to show conduct 'highly offensive to a reasonable person of ordinary sensibilities', whereas the NSWLRC only says this is a factor to be taken into account, and drops the word 'highly'; the ALRC only allows recovery for 'intentional or reckless acts', whereas the NSWLRC also allows recovery for negligent acts. Other weaknesses in the ALRC proposals are also ameliorated in those of the NSWLRC: failure to give an explicit role to Privacy Commissioners in at least conciliating complaints, and a right of appearance in any court cases; defence of qualified privilege is probably too strong. Otherwise, the two law reform bodies make similar recommendations.

The federal Government has delayed responding to the ALRC's recommendation until its second tranche of replies, and there is no timetable for the NSW government to respond to the NSWLRC recommendation: it will probably wait to see what the federal Government does.

The implementation of either would mean that Australia ceased to be one of the few developed countries which provided neither a constitutional nor a civil action for invasion of privacy.

DK/May10
II. Main information privacy legislation

1. Nine jurisdictions and eight main data protection laws

By 2009, Australia has seven major information privacy laws: the federal law covering the private sector; and the laws covering the public sectors of the Commonwealth, NSW, Victoria, the Northern Territory, the Australian Capital Territory (ACT), Tasmania and Queensland. There was a Bill in passage in Western Australia but there has been a change of government and its fate is uncertain. This leaves only South Australia which has only a non-enforceable government administrative rules. So there are seven main public sector laws and one law covering the private sector in all jurisdictions: eight main laws in total.

In a federation like Australia, State and Territory governments control more important personal information than the Federal government, including births, deaths and marriages registers, drivers licences, education records, some building approvals, prison records, and criminal records. It is therefore important that data protection laws be effective at all levels of government. Where State and Territory privacy laws exist, they include local governments in their scope.

In addition there are some sectoral laws with customised sets of information privacy principles for credit, health and telecommunications data. These numerous laws vary a great deal in their exceptions and exemptions and in the effectiveness of their enforcement.

Each of these laws - private sector, public sectors and sectoral - contains a set of information privacy principles based substantially on the OECD privacy principles (OECD, 1980) but with additions and (in general) strengthening. They are variously entitled ‘Information Privacy Principles’, ‘National Privacy Principles’ and ‘Information Protection Principles’. They contain many variations which provide grist for lawyers and disappointment for complainants (see Bygrave and Greenleaf, 2005: 4.2.1 for discussion of the extent of inconsistency and its implications). Nevertheless for the purposes of this Report their content is substantially the same and they will be referred to generically as ‘information privacy principles’ or ‘IPPs’. None of these laws contain general definitions of ‘privacy’: breaches of these laws are defined to require breaches of their IPPs.

2. The proposed new 'Unified Privacy Principles' (UPPs) and this Report

A major objective of the current reforms is to achieve uniformity in these numerous sets of IPPs, for which purpose the ALRC proposed a set of 'Unified Privacy Principles' (UPPs). The government shares this objective and proposes to (i) amend the Privacy Act 1988 (Cth) by replacing both the NPPs covering the private sector and the IPPs covering the federal public sector with a set of UPPs based on those proposed by the ALRC; and (ii) seek to convince the State and Territory government to amend their legislation in similar fashion (AusGov, 2009, 18-1; 3-2).

The ALRC provided a set of consolidated draft UPPs in its Report (ALRC, 2009), and they are annexed to this report for purposes of reference. However, as will be explained, the Government is proposing to amend some of the ALRC’s UPPs before legislating, and it has not yet drafted its proposed replacements, only explained in general terms what the changes
will be (AusGov, 2009: Part D). Furthermore, it says it will not necessarily follow the ALRC's drafting (AusGov, 2009: p12):

'The ALRC’s report provided a proposed model for its recommended UPPs. However, the Government is responding to the policy intent of individual recommendations, and is not responding directly to the form or drafting of the model UPPs. The Government will determine the most appropriate way to give effect to the policy intent when it drafts the necessary amendments to the Privacy Act.'

Since it is beyond the scope of this report to cover all the variations in the State and Territory laws, and the federal government has clearly stated its intention in relation to the scope and content of the new UPPs (which are not very different in most respects from the previous NPPs and IPPs), this Report will concentrate on elements in the proposed new UPPs, and in the existing Australian federal laws, which are significant or which are relevant to the 'new challenges' the subject of this project.

3. **The State and Territory public sector laws**

The State and Territory data protection laws are analysed in some details in Bygrave and Greenleaf, 2005: 4.5 and 2006: 2.12 - 2.14, particularly the laws of New South Wales (2005: 4.5.4) Victoria (2005: 4.5.2), Tasmania (4.5.6) and the Northern Territory (4.5.7). Queensland's *Information Privacy Act 2009* is new, and is analysed in an Appendix to this report.

4. **Definitions and Core Concepts**

*Personal information*

The *Privacy Act 1988* applies to the processing of “personal information”. This is defined as:

> “information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion” (s. 6(1)).

The term ‘individual’ covers only living individuals, and not deceased persons or groups (see below, at 5).

This definition appears flexible enough to give similar coverage as the definition of “personal data” in Art. 2 of the data protection Directive.

The definition of 'personal information' will remain substantially unchanged by the current reforms, except that biometric information will be added to the definition of 'sensitive information' (AusGov, 2009, 6-4).

*Consent*

Current Australian legislation generally requires simply “consent”, not specified forms of consent. According to s. 6(1) of the *Privacy Act 1988* (Cth), consent “means express consent or implied consent”. On the face of the Act, then, consent may be implied in any situation –
also with respect to processing of sensitive data. This is in contrast to the Directive which stipulates that, in relation to processing of sensitive data, consent must be “explicit” (Art. 8(2)(a)) while in relation to other personal data, consent must be “unambiguous” (Art. 7(a)). The Directive also makes clear that, for its purposes, consent must always be “freely given, specific and informed” (Art. 2(h)). Under the Privacy Act, it is likely that consent can be implied from a failure to opt-out in some situations.\(^1\) Bygrave and Greenleaf (2005: 4.2.2) sets out where consent is required in the Privacy Act 1988, and the meaning of implied consent, concluding that 'All in all, the consent requirements under the Privacy Act do not fall so far below the equivalent requirements of the Directive as to militate against a finding of adequacy for the purposes of Article 25.'

The Government does not propose to change the current law, only that the Privacy Commissioner should issue further guidance on the meaning of consent (AusGov, 2009: 19-1).

**Other terms and concepts**

There is no specific definition of a “controller” or “data user”, such as can be found in the European data protection directives and in the national laws of the EU Member States giving effect to those directives. However, as elsewhere, most of the important data protection requirements - and in Australia, in particular, the information privacy principles - bear on the organisation responsible for the processing of personal data (although the Act is less specific in this regard than European data protection laws).

5. **Substantive scope of the Privacy Act**

Subject to a range of exemptions and variations, discussed below, at 6, the Privacy Act 1988 applies generally to all “organisations” (or, in the public sector, “agencies”) that “[perform] an act, or engage in a practice”, that “relates” to “personal information”.

As already noted, the latter term only covers information on (living) individuals: data protection will continue to apply only to living individuals and will not apply to the deceased (AusGov, 2009: 8-1/3) nor to indigenous or other groups collectively (AusGov, 2009: 7-1/2).

6. **Exemptions and variations**

   **Exemptions**

A significant number of agencies and organisations are exempted from having to comply with the Privacy Act. These include intelligence agencies, the Australian Crime Commission, parliamentary departments, some government business enterprises and registered political parties (see ss. 6–7 Privacy Act 1988 in conjunction with Part 1 of Schedule 2 to the Freedom of Information Act 1982 (Cth)).

The ALRC has proposed the abolition of many of the exemptions from the private sector provisions, including the 'small business' exemption, which had previously been a principal source of criticism of the Act by local commentators and by the Article 29 Working Party of the EU. The government has not yet announced its response to these recommendations.

\(^1\) Dixon, *supra* n. 36, para [5-320].
Variations (Public Interest Determinations)

The Commissioner may issue a written Public Interest Determination (PID) under Part VI of the Act permitting an agency or private sector organisation to breach one or more IPPs where the public interest in the agency so acting substantially outweighs the public interest in the agency adhering to the IPP(s) (ss. 72–73). Division 2 of Part VI empowers the Commissioner to make Temporary PIDs with respect to urgent matters. A large amount of discretion is vested in the Commissioner in this area. At the same time, the process of making a PID is fairly transparent and allows for input from all potentially affected bodies and persons (s. 74 et seq). Less input and transparency pertains, however, in the process leading to the making of a Temporary PID. Any PID may be disallowed by the Commonwealth Parliament (ss. 80(i), 80C). So far just under a dozen PIDs have been made, along with four Temporary PIDs. No PID has yet been disallowed. The bulk of the Determinations concern narrowly circumscribed and relatively non-contentious matters (Bygrave and Greenleaf, 2005: 4.1.5).

The Government now proposes to empower the Privacy Commissioner to refuse to accept a PID application if it is ‘frivolous, vexatious or misconceived’ (AusGov, 2009: ). Given that there are no known examples of agencies or companies abusing the process, the rationale for such a change is not obvious.

A much more dangerous and ill-considered ALRC proposal was rejected by the Government. The ALRC had proposed that the UPPs should be able to be modified by regulations, making them more or less stringent. The Government has decided that Parliament must have an 'express role' (ie pass legislation), rather than only the negative power of disallowing regulations (AusGov, 2009: 5-1).

"Purely personal processing": Applicability of the Act to individuals and social networking sites

The ALRC did not recommend any change to the exemption relating to individuals who process personal data in a non-business capacity (s. 7B(1)). This exemption is reinforced in s. 16E which provides that the NPPs do not apply to processing by an individual carried out solely for the purposes of, or in connection with, his/her “personal, family or household affairs”. Reading both provisions together, the exemption seems to correspond with Art. 3(2) second indent of the data protection Directive (as construed by the ECJ in Lindqvist).

It is unlikely, but not impossible, that the Government will propose legislative changes where the ALRC has not proposed any at all. It is therefore likely that Australian data protection legislation will continue to exempt the actions of individuals in processing personal information of others through social networking sites or other means of internet communications.

A remedy for individual misuse of the personal information of others is most likely to be provided by legislation for a civil action for an interference with privacy, as discussed above, as recommended by both the ALRC and the NSWLRC. However, such legislation by itself is unlikely to deal with the question of immediate 'take down' procedures, while litigation proceeds.
7. **Territorial scope of the Privacy Act**

The current situation

The Privacy Act aims to stop companies avoiding its provisions by moving personal information overseas. In summary s5B gives almost all of the Act extra-territorial operation, provided one of two types of nexus is satisfied:

(a) An organisational link with Australia - The organisation must be an Australian citizen or resident, or a partnership, trust or company formed here, or an unincorporated association managed and controlled here; or

(b) An operational link with Australia - The organisation carries on business here, or the personal information was collected or held here by that organisation either before or at the time of action about which a complaint is made.

The Privacy Commissioner's powers to investigate and make determinations are extended to cover this extra-territorial operation. If an act or practice is required by an applicable law of a foreign country it will not constitute a breach of the Australian Act (s13D). This avoids clashes between observance of Australian privacy law and the law of the foreign country. Also, except for NPP 9 (data exports), s5B only applies in relation to information about an Australian citizen or resident.

This exact extent of this extra-territorial operation concerning Australians may be more extensive than it looks at first:

(a) What will constitute 'carrying on business' in Australia? Will web sites that have a substantial number of Australian customers, or who send email to a list of customers including Australians be 'carrying on business' here? In areas of law such as passing off and trade marks a relatively small connection with Australia has been sufficient to constitute 'carrying on business'.

(b) When will information be 'collected ... in Australia'? For example, if a person in Australia fills out a form on a web page of a US business (the server for which is in the US), when the form is being filled out it is on the user's computer in Australia, prior to the data being transferred to the US server. Where is the information 'collected'? This is less clear that the EU Directive, which includes in its scope data collection which 'makes use of equipment' in an EU country (A 4(1)(c)), but the possibility of considerable extra-territorial scope remains.

In contrast, it may be less extensive than it needs to be if (as discussed later) s5D does not extend to anyone who is not an Australian, and therefore EU citizens are unprotected against their data being exported to Australian businesses in privacy-unfriendly foreign countries.

**Proposed extension of extra-territorial provisions**

The current review does not propose any changes to the territorial scope of the legislation insofar as private sector organisations are concerned.
The ALRC recommends below that the Privacy Act be amended to clarify that it applies to the acts and practices of agencies that operate outside Australia, and that a similar provision should be included in state and territory legislation (ALRC 2008: 31.79). The Government has not yet responded to this recommendation.

The exception in s13D will apply to require Australian agencies holding personal information overseas, as well as Australian companies, to comply with foreign laws of the jurisdiction in which they are located, in preference to the extra-territorial operation of the Privacy Act. The ALRC (2009: 31.85) does not propose that this be changed:

The ALRC does not recommend that s 13D of the Privacy Act be amended to limit the circumstances in which personal information transferred outside Australia will become subject to foreign law. In the ALRC’s view, the policy justification for s 13D is sound—acts and practices that take place in a foreign country, and are required by the laws of that country, generally should not be considered a breach of the Act. It would not be workable to prevent the transfer by agencies and organisations of personal information to countries such as the US. Also, it would be unfair to render an agency or organisation transferring personal information under s 13D responsible for an act or practice of the recipient which is required by a foreign law, when neither they, nor the recipient, can control or prevent the acts or practices required under such a foreign law.

31.86 The OPC’s guidance on the recommended ‘Cross-border Data Flows’ principle should set out the steps to be taken when personal information transferred outside Australia may become subject to a foreign law, including laws such as the US Patriot Act. The guidance also should provide advice to agencies when contracting government services to organisations outside Australia.

8. Sectoral and other laws affecting data protection

There are three specific organisational/industry sectors which have their own detailed data protection legislation in Australian law. One sector – health – spans both public and private sector organisations, and is the subject of both federal data protection law (IPPs and NPPs in the Privacy Act 1988) and special data protection laws in three State and Territory jurisdictions (ACT, Victoria and New South Wales). The two other sectors – credit reporting and telecommunications – principally affect the private sector. In addition, there exists detailed data protection legislation dealing specifically with matching of personal data by and between federal government agencies. The OPC’s private sector review report noted that the health, finance and telecommunications sectors are the three “most complained about” sectors with which it deals. The details of these laws are in Bygrave and Greenleaf (2005: 4.4).

The Government's announced proposals (AusGov 2009) deal with the health sector and credit reporting, but the telecommunications sector has been deferred to the government's future second response. In this report the health and credit reporting sectors are dealt with below under Areas of Special Concern.

---

2 OPC, supra n. 32, p. 51.
9. Data Protection Principles

General considerations

Most of the proposed UPPs are discussed under this part, but some such as the separate UPPs for Sensitive Information, Identifiers and Direct Marketing, are discussed separately under 'Areas of Special Concern'.

The structure of the UPPs is still more influenced by the OECD Guidelines than by the structure of the Directive, making direct comparisons sometimes complex.

Purpose-limitation principle – collection, use and disclosure limitations

Collection limitations – current principles

The Directive’s requirement that data collected be “not excessive” is addressed to a large extent by the current requirement of IPP 1 that collection be limited to what is “necessary for or directly related to that purpose” and by the requirement of NPP 1.1 that “[a]n organisation must not collect personal information unless the information is necessary for one or more of its functions or activities” (Bygrave and Greenleaf, 2005: 4.2.5).

Proposed new UPP 2 Collection

The proposed new Collection UPP 2 will include this 'minimum collection' element and will also strengthen the existing law (AusGov, 2009: 21:1/5) as follows:

- information must be collected only from the individual concerned, where reasonable and practicable;
- it provides protections to unsolicited information, once a decision is made to keep it;
- there must be no collection unless necessary for the current functions of the collector.

Proposed new UPP 1 Anonymity and Pseudonymity

The existing Anonymity Principle in the NPPs, which requires that individuals be given the option to interact anonymously with organisations wherever it is lawful and practicable, will be strengthened further by the addition of an option of pseudonymity, and by extension of application to public sector agencies (AusGov, 2009: 20:1/2). This will strengthen an already strong 'minimum collection' aspect of the Australian legislation.

Use and disclosure limitations – current principles

The basic principles are the same in both the European and Australian approaches: personal information should be collected only where necessary for legitimate purposes and should only be used or disclosed for such purposes, with limited exceptions.

The current National Privacy Principle 2 requires that the secondary use or disclose be “related” to the purpose of collection (or “directly related” in the case of sensitive information), but also requires that “the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose”. This additional “reasonable
expectations” test seems to impose a standard at least as high as the Directive. There is room for disagreement about the precise meanings of “incompatible”, “related” and “directly related”, but it is fairly certain that the Directive does not set a clearly higher standard here than the Australian provisions.’ (Bygrave and Greenleaf, 2005: 4.2.3)

Proposed new UPP 5 'Use and Disclosure'

The proposed new 'Use and Disclosure' UPP 5 is based on NPP 2, and includes the same tests as above for allowed secondary uses (AusGov, 2009: 25-2). The government also proposes to include the four specific disclosure exceptions in the current NPP 2. The ALRC apparently forgot to recommend their inclusion in its formal recommendation, though it included them in its UPPs, so the Government has added them). Three of the exceptions (consent; investigation of misconduct; and law enforcement) are not controversial.

The fourth exception, ‘where the use or disclosure is required or authorised by or under law' has been controversial in relation to its potential effects on the adequacy of Australian law (discussed in detail in Bygrave and Greenleaf, 2005: 4.2.3 ‘Authority of law' exception). A new definition of 'law' for this purpose sets out a broad definition of law (including delegated legislation, common law, equity and court orders) but excluding obligations arising under contracts (AusGov, 2009: 16-1). This will leave the UPP much the same as the current NPP 2, but remove any basis for fanciful interpretations that anything not forbidden is 'authorised by law'. However, it still leaves an exception to use and disclosure considerably broader than what is allowed by the Directive. The problem remains that any Act or regulation can authorise or require an exception to the Disclosure Principle, without even expressly stating that it is doing so.

The Government also proposes to add a new fifth Use and Disclosure exception ‘for the purpose of locating missing persons’. This exception will permit, not require, such disclosures, and empower the Privacy Commissioner to develop binding rules (by a legislative instrument which is therefore disallowable by Parliament) as to how such disclosures will be carried out. This is a sensitive area, as some people do not wish to be located, but the proposal is sensitive to this problem.

Data quality obligations (proposed new UPP 7)

At present, both the IPPs and NPPs deal with data quality and proportionality in a way which is adequate, except for the lack of a deletion principle in the IPPs (Bygrave and Greenleaf, 2005: 4.2.5). The Government does not propose any changes in the new Data Quality UPP 7 (AusGov, 2009: 27-1), and is dealing with the deletion question as part of the new UPP 8 concerning security.

Data security obligations (proposed new UPP 8)

The security provisions in IPP 4 and in NPP 4.1, though stated briefly, cover the essential aspects of security required by the Directive in Articles 16 and 17 (Bygrave and Greenleaf, 2005: 4.27). The proposed UPP 8 concerning Security does not change this.

---

3 Cf. Bygrave, supra n. 155, p. 340 (arguing that, under Art. 6(1)(b) of the Directive, “any secondary purposes will not pass the test of compatibility/non-incompatibility unless the data subject is objectively able to read those purposes into the primary purposes, or the secondary purposes are otherwise objectively within the ambit of the data subject’s reasonable expectations”).
Data breach notification proposal

The ALRC made recommendations concerning data breach notification, but the Government has deferred consideration of this until the second tranche of legislation.

The Privacy Commissioner has also published voluntary data breach guidelines.

'Openness' concerning practices (proposed new UPP 4)

Transparency is addressed in two ways in both the IPPs and NPPs: (i) by an “openness” principle, and (ii) by requirements of notice on collection of personal data (discussed later under individual rights).

Following the OECD Guidelines, both the current IPP 5 and NPP 5 require data controllers to set out in documents their practices concerning management of personal information, including details of how persons can access their own records. Any person (not only a data subject) has the right to obtain this information. This valuable right of “openness” does not seem to be exercised often, though it would allow the press, academics and others to more effectively investigate surveillance practices. It is a strong aspect of the Australian law without an exact parallel in the Directive, and should be balanced against weaknesses of the Australian law in any overall assessment of adequacy (Bygrave and Greenleaf, 2005: 4.2.6).

The Government proposes to include in the new Openness UPP 4 specific requirements that ‘a Privacy Policy should express an agency or organisation’s consideration of how it handles personal information at each stage of the information cycle, and how the Privacy Principles apply to its activities’, and has also added requirements to document internal policies and practices to enable compliance with the UPPs (AusGov, 2009: 24-1). The explicit emphasis on the information life-cycle and for Privacy Policies to be updated continually is a major innovation in the government’s response to the ALRC report. The government has also accepted the ALRC proposal to require that Privacy Policies should be conveniently available electronically (AusGov, 2009: 24-2).

A further addition of significance by the government is that Privacy Policies should also include details of proposed overseas transfers, discussed later under Data Exports.

The Government proposes to abolish the Personal Information Digest (AusGov, 2009), pointing out it is strengthening the requirements for Privacy Policies considerable, and that they must be provided online. In reply, it could be said this is not the same as having them deposited, and searchable, in the one place – however, costs of doing so probably make this prohibitive.

Deletion of data (proposed new UPP 8 Data security)

The Directive requires information to be kept in identifiable form “no longer than is necessary” (Art. 6(1)(e)). The IPPs do not have any such requirement in relation to the public sector. NPP 4.2 has a requirement to “take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed” under NPP 2.

The Government now proposes that retention obligations extended to public sector as part of the proposed new Data Security UPP 8 (AusGov, 2009:28-4)
10. Areas of special concern

Processing of Sensitive Data (proposed new UPP 2 Collection)

The existing public sector IPPs do not make any special provisions for sensitive data in relation to the federal public sector. The federal public sector law clearly parts from the Directive in this respect. In relation to the private sector, NPP 10 does make special provision for sensitive data (which covers much the same categories as in Art. 8 of the Directive – as construed by the ECJ in Lindqvist), but only in relation to restricting its collection by requiring consent to collection or other justifications similar to those specified in the Directive. Use and disclosure are subject to the normal rules, except that secondary uses of sensitive information must be directly related to the primary use, not just “related”. However, consent to secondary use is not required. This is the main difference from the Directive’s requirements. The Article 29 Working Party noted this as a deficiency relevant to the question of adequacy (Bygrave and Greenleaf, 2005: 4.2.4).

Part of the proposed new UPP 2 Collection concerning Sensitive Information will overcome this potential adequacy problem by applying the same rules and exceptions as currently apply to the private sector under NPP 2 to the public sector (AusGov, 2009: 22-1/3).

Automated decisions ('Sensitive Processing')

Neither the IPPs nor NPPs include any direct equivalent of Art. 12(a) of the Directive giving data subjects a right to knowledge of the “logic” behind automated decisions, particularly of the kind described in Art. 15(1). There are no special provisions concerning automated decisions in the Australian law at present, and none are proposed by the Government. This is unlikely to be an impediment to an adequacy assessment.

Interconnection of files ('Data matching')

In the wake of the Australia Card, a political compromise was reached, comprising an enhanced Tax File Number (TFN) system, and the Privacy Act 1988. The original TFN legislation prohibited disclosure and use of TFNs beyond tax-related purposes (an essential part of the ‘no Australia Card’ bargain). However, only two years later, the federal Labor Government (with opposition support) reneged by extending it by further legislation, so that TFNs could be used for cross-matching of taxation information with information concerning federal ‘income support’ benefits (social security, veteran's affairs, student assistance and first home-owners benefits) provided by four ‘assistance agencies’. To check identification, electoral roll and Medicare identity information is also used. The matching is three way: between assistance agencies; from tax to assistance agencies; and from assistance to tax agencies. New legislation (the Data-matching Program (Assistance and Tax) Act 1990) authorised the new data surveillance regime (as it otherwise would breach the Privacy Act or TFN Act), set out very detailed operational rules for the surveillance system, and provided some procedural protections against its abuse, plus Parliamentary reporting obligations and Privacy Commissioner oversight.

Such detailed and explicit ‘data surveillance law’ is still unusual. This system, often called the ‘parallel data matching’ scheme, was strongly but unsuccessfully opposed by privacy advocates. Although it involves data surveillance on a massive scale, and in a relatively open manner, this data matching results in few if any complaints to the Privacy Commissioner.
There have been some limited further legislative extensions of the TFN system, but fifteen years later the TFN and the parallel data matching system have not had major expansions. However, as discussed earlier, other data matching schemes now pour data into the five key agencies, where it adds to the data used for ‘parallel data matching’.

The legislative operation of the current 'data matching' system, implemented largely through the Data Matching Program (Assistance and Tax) Act 1990, is detailed in Bygrave and Greenleaf (2005: 4.4.4), where the conclusion reached was as follows:

Australian data protection legislation does not make general provision for special procedures for automated processing of personal data. The data-matching legislation is the most obvious instance where such provision needs to be made, and the legislation does address the issue of human intervention when adverse decisions concerning a person are made (viz., Guideline para. 5). The data-matching legislation is not identical with the approach in the Directive. In particular, it does not make clear provision for the rights contained in Arts. 12(a) and 15(1). Nonetheless, it contains vestiges of these rights and supplements them with a considerable range of other control mechanisms. In our view, the legislative scheme meets the adequacy criteria of the Article 29 Working Party.

This system is not proposed to be changed by the Government's current proposals, except that the Privacy Commissioner is to review the current TFN Guidelines.

**Direct marketing**

**Current situation**

NPP 2, dealing with the private sector, contains a right to opt out but it only applies in certain circumstances. If direct marketing is a primary purpose of collection of personal information (with the notice required as a result), or if direct marketing is a secondary purpose that is both related to the primary purpose and within the individual’s reasonable expectations, or the direct marketing is carried out with the individual’s consent (NPP 2.1(a) & (b)), then the information may be used for direct marketing without any subsequent right to opt-out being offered in each marketing communication. This also applies where personal information has been collected from third parties for marketing purposes. It is only when personal information (which is not sensitive) is being used for direct marketing without prior notice, consent or reasonable expectation, that NPP 2 requires that “in each direct marketing communication with the individual, the organisation draws to the individual’s attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications” (NPP 2.1(c)(iv)).

 Quite apart from these general provisions, Australia has two very effective pieces of legislation dealing with specific forms of direct marketing: the Do Not Call Register Act 2006 (see Bygrave and Greenleaf, 2006: 2.3) and the SPAM Act 2003 (see Bygrave and Greenleaf 2005: 3.7.5 and 2006: 2.3.2).

---

4 Cf. the regime under the Spam Act 2003 (dealt with in section 3.7.5 above) which establishes an “opt-in” rule with respect to “commercial electronic messages”.

DK/May10
Proposed new UPP6 Direct Marketing

The proposed new UPP concerning Direct Marketing (AusGov, 2009: 26-1) will now apply the same opt-out conditions to all direct marketing. The key conditions for direct marketing will be: (i) where it is to an existing customer, the customer must have a reasonable expectation of direct marketing use; and (ii) where it is to someone who is not an existing customer, the business must first obtain the customer’s consent unless it is impractical to do so. A broad definition of ‘existing customer’ will be added to suit different situations (charities etc). Consent will now always required to use sensitive information in direct marketing. (AusGov, 2009: 26-2/4)

Government agencies will have to comply with the direct marketing principles when acting commercially, but not in relation to the promotion of government services (AusGov, 2009: 26-1).

Two innovative aspects of the government proposals are that the obligation to respect opt-outs will be extended to the source of the data used for marketing. Customers will also be entitled to require marketers to answer ‘where did you get my address?’ (AusGov, 2009: 26-5/6).

Credit reporting

Current situation

The existing credit reporting system was described in 2005 (see Bygrave and Greenleaf, 2005: 4.4.2 for a detailed description) as clearly exhibiting all of the formal requirements of adequacy in relation to both its principles and the avenues of enforcement, but that ‘Substantive adequacy is, as always, a separate question. There is fairly strong evidence that the present credit-reporting system is not functioning optimally’. There has been no significant change to the regulatory scheme or the Commissioner's practices in the last four years. It was also noted in 2005 (Bygrave and Greenleaf, 2005: 4.4.2) that:

At periodic intervals since the 1989 legislation there have been attempts to permit "positive reporting" in Australia – i.e. the inclusion in credit reports of data which embrace a great deal more than simply details detracting directly from a person’s credit-worthiness, such as data on defaults on credit repayments. All attempts to establish positive reporting have hitherto failed.

Proposed new credit reporting system

The Government is now proposing to adopt most of the ALRC's recommendations to substantially change the credit reporting system so that credit grantors and credit reporting organisations will now be able to report a limited amount of 'positive' information, particularly details of accounts opened, current credit limits, and dates on which accounts were closed (AusGov, 2009: 56-1). It is possible this may be extend to include details of whether a person has been in arrears in payments (without a default otherwise being listed) over the last two years, and if so by how many payment cycles, but this depends on the adoption of 'responsible lending' practices (AusGov, 2009: 56-2/3).

Because the ALRC recommendations and the Government response comprise over 30 pages of proposed legislation (AusGov, 2009: 54-1 to 60-3), it is beyond the scope of this report to analyse them here. The details of the regulation of credit reporting are also somewhat outside the scope of the main aims of the 'New challenges' project.
Health information

Current situation

The current regime concerning health and medical records was described in 2005 as having 'become extremely complex' because it is regulated by both the federal Privacy Act 1988 in relation to the private sector and the federal public sector, but some state and territory jurisdictions (NSW, Victoria, ACT and NT) have developed privacy legislation for their public sectors, whereas others have administrative arrangements for this purpose (Bygrave and Greenleaf, 2005: 4.4.3). Recently, Queensland joined the jurisdictions with legislation for its public sector.

Proposed new electronic health information systems regime

The ALRC recommended that 'If a national Unique Healthcare Identifiers (UHIs) or a national Shared Electronic Health Records (SEHR) scheme goes forward, it should be established under specific enabling legislation', and it suggested content for such legislation. The Government has accepted in principle this recommendation (AusGov, 2009: 61-1).

The Australian Health Ministers’ Conference (AHMC) announced in its 5 March 2009 communiqué that, consistent with the Council of Australian Governments (COAG) agreement, all Australian residents will be allocated an Individual Healthcare Identifier (IHI). No details of the proposed legislation are yet available.

The Government has proposed details of how the handling of health information within the Privacy Act will be amended, but this is no longer very meaningful in the absence of details of the IHI and SEHR legislation. The detailed regulation of health care privacy is also not central to the aims of the 'New challenges' project, and so will not be discussed in further detail here.

Identity information

Current situation

The Directive requires EU Member States to “determine the conditions under which a national identification number or any other identifier of general application may be processed” (Art. 8(7)). This requirement is not one of the Directive’s provisions emphasised by the Article 29 Working Party as relevant for adequacy assessments.

The requirement is met to some extent in Australian law by NPP 7 (Identifiers), which limits the use of government identifiers by private sector bodies (only), and also by the controls on tax file number usage imposed by the Privacy Act and other legislation. NPP 7 says that private sector organisations must not adopt (or use or disclose) as their own identifier an identifier that has been assigned by an agency, except under circumstances allowed under NPP or which have been prescribed.

The unique identifiers principle in the Victorian data protection legislation (IPP 7) is quite different from NPP 7, and an improvement on the latter because it is more comprehensive. Information Privacy Principle 7 attempts to limit the creation and adoption of unique identifiers, and to limit the collection, use and disclosure of unique identifiers (see Bygrave and Greenleaf, 2005: 4.5.2)
Proposed new UPP 10 identifiers

The proposed new Identifiers UPP 10 will substantially re-implement NPP 7, with some strengthening.

The Government proposes that regulations (which are therefore disallowable) can allow adoption, use or disclosure of government identifiers, where the Minister is satisfied that this 'will be for the benefit of the individual concerned'. The Government want to ensure closer consultation with the Privacy Commissioner on use of this regulation-making power (AusGov, 2009: 30-1).

The Minister (not the Commissioner as the ALRC suggested) will be able to make determinations (disallowable) as to what is a government identifier. The definition of 'identifier' will not include the Australian Business Number (ABN), as it does not in the current law. The ALRC's recommendation that biometric information collected for identification should be classed as an ‘identifier’ was rejected. However, 'identifier' will cover identifiers assigned by State and Territory governments, which will considerably expand the scope of the principle (AusGov, 2009: 30-2/5).

The Government has also accepted in principle that adoption of multi-purpose government identifiers will require a PIA conducted by the Government in consultation with the Privacy Commissioner. Unfortunately, the Government says nothing about public availability of the PIA, nor about the independence and terms of reference of the party conducting the PIA (AusGov, 2009: 30-6).

It accepts the ALRC's view that it would be appropriate for the Privacy Commissioner to review the Tax File Number (TFN) Guidelines under s17 (AusGov, 2009: 30-7).

The Use of Publicly Accessible Data ('Public Registers')

The discussion under 'The surveillance context' outlines the social and administrative practices limited (and in some cases expanding) the use of public registers in Australia. There are limited legislative provisions dealing specifically with public registers from a privacy perspective. The federal Privacy Act 1998 (Cth) does not do so, except negatively through the term “record” being defined to exclude “generally available publications” (s. 6(1)) (as to which see the lengthy discussion in Bygrave and Greenleaf, 2003: 4.1.3 concluding that 'the justification for regarding it as a significant impediment to a finding of adequacy is questionable').

In the New South Wales legislation, the definition of “personal information” excludes “information about an individual that is contained in a publicly available publication” (s. 4(3)(b)). As discussed above in section 4.1.3 in relation to “publicly available information” in the federal Privacy Act 1988, such a provision does have limits on its operation and can be justified. Decisions of the NSW Administrative Decisions Tribunal have given the provision a wide reading but not one which would reverse this conclusion. On the protective side of the ledger, the NSW Act does provide some protection for information which is contained in publicly available publications in the form of public registers (Bygrave and Greenleaf, 2005: 4.5.4, which also gives more details of the protections available).
The ALRC's and Government's proposals do not deal with public registers, with the one exception that the Government rejected the ALRC's proposal that federal legislative instruments establishing public registers should set out an restrictions on electronic publication of the information.

11. The Internet

Australian privacy regulation has yet include any specific measures dealing with the Internet.

The ALRC insisted that its recommendations should be 'technology neutral'. The ALRC's Report (2008) devotes the whole of Part B 'Developing Technology' to issues relating to technological developments, primarily those involving the Internet, but its recommendations do not contain any concrete measures at all (other than the rejected one mentioned above). All of the ALRC's five recommendations were to the effect that the Privacy Commissioner should publish guidance or research on various aspects of technologies or their use.

The Privacy Commissioner has issues very brief and general 'FAQs' on Social Networking Sites and Identity Theft, but nothing more. Its track record does not inspire confidence that it will do what the ALRC suggests.

As discussed below, the Government's proposals to empower the Privacy Commissioner to develop mandatory Codes of Conduct concerning particular technologies, binding on their users, is potentially more significant than anything in the ALRC Report or its recommendations. But whether the Commissioner would use such a power remains to be seen.

12. Cross-Border Data Transfers

Current situation

Transfers into Australia (Outsourcing practices)

There are no special provisions concerning personal data transferred into Australia, except that there is still an anomaly that only data concerning Australian citizens (therefore excluding much personal data transferred into Australia) is covered by s5A Privacy Act 1988 which gives extra-territorial operation to the NPPs under some circumstances. NPP 9 concerning data transfers does however have extra-territorial operation in all cases.

Transfers out of Australia (Data exports)

The existing NPP 9 concerning the private sector has been the subject of considerable criticism by the A 29 Working Party and others which have not been addressed by the Australian government (Bygrave and Greenleaf, 2005: 4.2.10), but as was then noted 'While there are obviously considerable problems in finding that NPP 9 meets the Directive’s requirements, it should also be borne in mind that, to our knowledge, NPP 9 is one of the very few such data export provisions yet in force in any country outside Europe.' Some jurisdictions (e.g., NSW, Victoria, Hong Kong) have enacted such provisions but not yet brought them into force.' The Victorian provision is now in force, as is that of South Korea,

5 Restrictions on transborder data flow are also in force in Argentina (Personal Data Protection Act 2000 s. 12) and Canada (Personal Information Protection and Electronic Documents Act 2000, Schedule 1, clause 4.1.3), though the provisions of the Canadian legislation do not deal expressly with such data flow.
and a provision is currently before New Zealand Parliament. The existing IPPs governing the Australian federal public sector do not include any data export restrictions.

The current NPP 9, like the Directive, is based on a ‘border security’ approach: unless a proposed export (‘transfer’) of personal data outside Australia meets certain criteria, the act of exporting is itself a breach of the Act. The conditions are not strong enough, in the views of many commentators (see the summary by Waters and Dresner, 2000, cited in Bygrave and Greenleaf, 2005: 4.2.10), and included that the exporter only need ‘reasonably believe’ that there was ‘substantially similar’ protections in the recipient's jurisdiction. However, the conditions must be met on an export-by-export basis. If an exporter does not meet the conditions it will be in breach if it transfers personal data outside Australia, simply by the act of transfer. This applies both to transfers to an agent of the exporter, usually for further processing for the exporter (‘outsourcing’), or where transfers are to a third party for its purposes. Proving a breach by exporting without meeting the conditions is possible, though there have as yet been no cases or complaints (at least not in those published by the Commissioner) to test how difficult.

**Proposed new cross-border data flow rules UPP 11**

The Government is proposing to replace the existing 'border control' approach with a modified version of the ALRC 'accountability' (AusGov, 2009: 31-1/8). The key difference can be stated simply: any personal data about Australians will be able to be exported to anyone, anywhere. There will be no conditions on the legality of the act of exporting: it does not matter that the destination country has no privacy laws at all, and no privacy agency. The transfer of the data will still have to comply with NPP 2, which in this context primarily means that the discloser has to be transferring the data for a purpose (but not to a place) which the subject of the information ‘would reasonably expect’.

The new data exports UPP will apply to agencies, not only to organisations (AusGov, 2009: 31-1).

The 'accountability' aspect of the new approach is that although personal information can be exported to anywhere, including places that does not have ‘substantially similar’ privacy protections to Australia, if the exporter does so then theoretically they 'remain accountable' for overseas misuses of the personal information (AusGov, 2009: 31-1), meaning that a breach of a UPP occurring overseas will be taken to be a breach by the exporter (AusGov, 2009: 31-3). Critics (see Greenleaf, 2009b for example) argue that such accountability will only be theoretical, because the onus of proof (on the civil balance of probabilities) of a specific breach of a privacy principles by a specific overseas party will still rests with the data subject; as will the requirement to prove that the party in breach received the information directly or indirectly (but foreseeably) from the Australian exporting party; as will the requirement to prove that there was a causal connection between that breach and damage to the data subject. Additionally, the country from which the damage emanated might not be the same as the country to which the data was exported. Where personal data has been exported to particularly undesirable destinations (for example, depending on your viewpoint, Nigeria, India, Russia, or the USA) it might be very expensive, or even dangerous, to seek remedial action locally.

To make the situation worse for data subjects, the Government proposal (AusGov, 2009: 31-2), following the ALRC, then converts the previous (arguably over-broad) list of conditions
in NPP 9 which currently allow data exports into a list of excuses from even the above form of accountability. Complying with any one of them will allow the exporter to completely avoid (even in theory) ‘remaining accountable’ for any mis-uses of your personal information by the overseas recipient (or anyone they passed it on to). The government proposes to tighten some of these conditions in minor ways, but it doesn’t matter: they no longer serve the same function. It may be that this absolution from accountability will even apply to outsourcing of data processing as well as disclosures to third parties, so as to weaken the existing protections of the law of vicarious liability for the acts of exporter's agents – the details are not yet provided. In the views of critics, when these excuses are added to the inherent limitations in the enforceability of 'accountability', this specific Australian form of 'accountability' is a sham, characterised by the absence of any real likelihood of accountability.

The Government is proposing that data subjects will need to be told at the point of collection when their information is about to go overseas, but only under certain circumstances ((AusGov, 2009: 23-2). It says that the Notification Principle UPP 3 will include the requirement that companies or agencies must take ‘reasonable steps’ to give individuals notice when collecting their personal information that it may be transferred overseas, and to which countries. This is intended to be an improved protection, but it has considerable limitations: there is no need of any mention to be made that the destination countries (or some of them) provide no privacy protection; if the collector has not yet made up its mind whether it will export the information, or to where, then it does not have to say anything; and the collector is allowed to change its mind after it collects the information.

It is anomalous that, for credit reporting information both the Government (AusGov, 2009: 54-7) and the ALRC take an inconsistent approach, recognising that border controls are necessary for effective protection. The ALRC proposed that disclosures of credit information to foreign credit providers should be prohibited except according to conditions set out in regulations 'including the availability of effective enforcement and complaint handling in the foreign jurisdiction' - in other words 'border controls'. The government goes further, proposing to erect an almost absolute border control over credit information: no data exports to anywhere but New Zealand; and no capacity for any regulations to change this. It rejects the ALRC's approach because ‘consideration would still need to be given as to how adequate protections could be put in place to ensure there was no inappropriate secondary use of the information outside the jurisdiction where the information was originally held’. Any benefits ‘would be outweighed by the inability of the Privacy Commissioner to enforce effectively the credit reporting provisions against foreign entities’. It is not clear why the same reasoning does not apply to other personal information just as sensitive as credit information.

The Government's proposals concerning data exports have already become a matter of public controversy within a week of their release, and the Department of Prime Minister and Cabinet has already agreed to hold further discussions on the question with Civil Society organisations.
13. Rights of Data Subjects

Informing of data subjects during collection

Current situation

In relation to notice, NPP 1.3 requires notice on collection from the data subject, and NPP 1.5 requires notice on collection from third parties, mirroring Articles 10 and 11 of the Directive. The A 29 Working Party criticised the existing NPP 1.3 because it “allows for organisations to inform individuals before or at the time of collection but also adds that, if this is not practicable, it may inform individuals as soon as practicable thereafter”. It may be a legitimate criticism of NPP 1.3 that notice can occur after collection, but it is hard to see it as an inadequacy in comparison with the Directive (Bygrave and Greenleaf, 2005: 4.2.6). With sensitive information, it is likely that notice after collection would vitiate consent, so notice is therefore required before consent. In summary, neither of these objections by the Working Party seem to be sufficiently substantial to affect the adequacy of the Australian provision.

The federal public sector IPP 2 shares the criticised aspect of the possibility of notice after collection, and has two additional weaknesses. The first is that notice is only required when data are “solicited” from the data subject, and not when they are provided unsolicited from the data subject. The second is that notice is not required when data are collected from third parties.

There is an anomaly with NPP 1.3(d) which requires an organisation to notify data subjects only of private sector bodies to which the collector discloses information will be rectified by the new UPP concerning Notice, which does not distinguish between public and private sector recipients.

Another apparent anomaly is that NPP 1.5 only applies where personal information is collected from “someone else” (i.e., not the data subject). On its face, the reference to another person rather than from “another source” (or in the Directive’s negative expression “not … from the data subject”) means that where personal data are collected from newspapers or books or databases, notice need not be given. However, the OPC has construed NPP 1.5 as also applying to collection from such sources (where reasonable). This notwithstanding, the OPC views the wording of NPP 1.5 as problematic and recommends that the Australian Government consider amending it to expressly require that notice be provided on collection from any source. It could be argued, though, that such an amendment will itself raise problems because NPP 1.5 requires on its face that reasonable steps should normally always be taken to give notice, which could result (for example) in every organisation that keeps a press cutting or photocopies a law report being required to send notices to everyone who they can reasonably contact who is identified in that story or report. The Directive does not seem

---

7 OPC, Privacy and Personal Information that is Publicly Available, Information Sheet 17-2003. The OPC claims that this information sheet, albeit advisory only, “has gained widespread acceptance”: OPC, supra n. 32, p. 262.
8 OPC, supra n. 32, p. 263 (recommendation 76).
9 The OPC, however, has taken the view that, in some circumstances, it may be reasonable not to take steps to provide notice to an individual: OPC, Taking Reasonable Steps to Make Individuals Aware That Personal Information About Them is Being Collected, Information Sheet 18 (June 2003). The validity of this view has not been tested in the courts and the OPC recommends that the Australian Government consider an amendment to
to share this problem to the same extent, because Article 11 only requires notice of data collected from other sources to be given “no later than the time when the data are first disclosed” (to a third party). The current form of NPP 1.5 could be seen, accordingly, as a reasonable balance between giving more pro-active notice than the Directive requires, but with a trade-off that it is not required for collection from documentary sources.

**Proposed new UPP 3 Notification**

The Government's proposed new Notification UPP 3 will apply whenever there is collection of personal information 'about an individual from the individual or from someone other than the individual' (AusGov 2009: 23-2). This proposal will remedies the deficiencies in relation to the public sector IPPs, but leaves unanswered the uncertainties about NPP 1.5 and the types of collection that it covers.

The content of the proposed notice is the same as at present. The Government agrees with the ALRC that there may be circumstances where it is reasonable not to give any notice.

The Government proposes to add the requirement that notice includes that personal information is ‘reasonably likely’ to be transferred overseas and to where it is likely to be transferred. This has been discussed above in relation to data exports, and its limitations noted as part of the proposed overall new data exports scheme, but it should be remembered that any requirement of notice above overseas transfers is a strengthening of the rights of the data subject.

**Confirmation of processing**

There are no requirements in the Australian legislation concerning confirmation that data has been processed (used, disclosed or otherwise).

**Access**

**Current situation**

The Article 29 Working Party summarises the adequacy requirements derived from the access and correction principles as “the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.”

Both the IPPs and the NPPs provide the basic rights of access and correction required under Article 12. The sole concern of the Article 29 Working Party relating to the Australian access and correction rights was that s. 41(4) of the Privacy Act 1988 only allowed the Privacy Commissioner to investigate a breach of these rights if the complainant was an Australian citizen or permanent resident. This has now been resolved by changes to s. 41 made by the Privacy Amendment Act 2004 (Bygrave and Greenleaf, 1995: 4.2.8).
In practice, access to and correction of public sector personal information has been handled via the FOI Act, not via the Privacy Act, because successive Privacy Commissioners insisted that complainants used the FOI Act.

**Proposed new UPP 9 - Access**

As part of its proposed reforms to the FOI Act, the Government announced on 24 March 2009 a proposal to amend the Privacy Act to enact an enforceable right of access to, and correction of, an individual’s own personal information, rather than maintain this right through the FOI Act. The Government explains its approach as follows (AusGov, 2009: 29-1):

The Government proposes that guidance and legislative amendment make clear that the Privacy Act is the primary avenue for access to, and correction of, an individual’s own personal information. These changes are intended to make the Privacy Act the key Commonwealth law for the collection, handling, disclosure and accessing of personal information. As a result, the focus of the FOI Act is intended to be on access to documents held by government other than an individual’s own personal information.

However, in recognition that there will be circumstances where documents held by agencies contain a mixture of: (a) an individual’s personal information; (b) the personal information of third parties; and (c) non-personal information, in such a way as to make it difficult to release only the individual’s personal information, or that individuals may make access requests for files that contain such a mixture of information, the Government agrees that rights to access some personal information should be retained under the FOI Act. Agencies will need to establish administrative processes for dealing with the different access and correction requests that will arise under the Privacy and FOI Acts, having regard to the types of records and information they hold.

Furthermore, the Privacy Commissioner will actually be required to make enforceable decisions on access and correction matters in relation to government agencies:

‘… the Government proposes that, for complaints from individuals about an agency’s decision to refuse access, or correction of, personal information, the Privacy Commissioner will be required to review the agency’s decision and make a decision on the review (affirming, varying or substituting the agency’s decision). This review process for access and correction complaints will not apply more generally in respect of complaints about agencies’ acts or practices relating to other Privacy Principles.’

However, in relation to private sector organisations, the Commissioner will not be required to make decisions, because the Government has decided it will not allow the Commissioner to be required to use the s52 Determinations power, as discussed below in relation to the Commissioner's complaint investigation processes.

**Correction**

**Current situation**

A problem which applies to the correction right in the IPPs (but not the NPPs) is that the right of correction depends on a person first obtaining access to their record, under the provisions of the legislation. So where a person’s record is exempt from access because of some exemption (such as those found in Art. 13 of the Directive), the data subject has no right to insist on rectification if they find out by informal means, or reasonably suspect, that the non-
accessible record is incorrect. On the face of it, the rectification right in Art. 12(b) does not depend on the data subject being able to exercise the access right in Art. 12(a) (Bygrave and Greenleaf, 1995: 4.2.8).

**Proposed new UPP 9 - Correction**

If terms similar to those used in the ALRC's UPP 9 are adopted by the Government, the above problem will disappear.

The general mechanism for correction procedures is discussed above in relation to access.

**Notification of disclosure**

**Current situation**

The Australian legislation does not include 'after the event' requirements to notify data subjects that their data has been disclosed, though they should be able to obtain this information as part of the process of accessing their personal information.

**Proposed notification after correction**

The Government is now proposing that where a person's information has been corrected, the agency or organisation will 'notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances' (AusGov, 2009: 29-5).

**Right to object to processing**

There are no general provisions allowing an objection to processing once personal information has been collected legitimately in the Australian legislation.

**Right to object to direct marketing**

This has been covered above in the part relating to the Direct Marketing UPP 6.

14. **Individual Remedies**

Bygrave and Greenleaf (2005: 4.3.2 and 4.3.3) provide details of the provisions concerning injunctive relief, compensation and other remedies, concluding that it was unlikely they would fall short of the requirements of the Directive. The Government does not propose to change these individual remedies as such, but does propose to change how the complaint investigation process may result in remedies becoming available, including avenues of appeal. This is discussed in the next section.

15. **Supervision, Notification and Enforcement**

**Structure and independence of the Office of the Privacy Commissioner**

The ALRC report was finalised before the Government announced that it proposed to follow through on its 2007 election commitment to create a new Office of the Information Commissioner (OIC) headed by an Information Commissioner, in which the Privacy Commissioner would be one of three Commissioners, the other being a FOI Commissioner.
The Government's explanation in the context of its privacy reforms (AusGov, 2009: p14) is as follows:

'As part of its 2007 election policy, Government Information: restoring trust and integrity, the Government committed to bringing the function of privacy protection within a new Office of the Information Commissioner (OIC) which would be responsible for both privacy and freedom of information (FOI) laws.

In March 2009, the Government released exposure draft legislation to implement this commitment. Under the proposed reforms, the Privacy Commissioner will be one of three independent statutory office-holders in the new agency. The Privacy Commissioner and an FOI Commissioner will operate under the leadership of an Information Commissioner as the agency’s CEO.

While formal powers will be vested in the Information Commissioner, the Privacy Commissioner will continue to have a role in exercising relevant powers and functions.’

There is no reason to expect that the new arrangements will provide any less independence to the OIC as a whole than is presently provided to the Privacy Commissioner, although the exact relationship between the three Commissioners concerning the exercise of powers and responsibilities under the Privacy Act 1988 remain to be seen.

The current Australian federal data protection regime is considered to be sufficient to satisfy the requirements of Article 28(1) of the Directive for a supervisory authority and one which “shall act with complete independence” (Bygrave and Greenleaf, 2005: 4.3.5).

It is quite possible that the inclusion of the Privacy Commissioner in a corporate decision-making body with other Commissioner who have overlapping and policy-consistent interests and responsibilities will result in a structure better able to withstand any pressures from government and the corporate sector, and therefore be more independent in substance.

**Powers of the Office of the Privacy Commissioner**

Below, we first of all provide an overview of the Privacy Act’s current approach to enforcement, with an appraisal of the effectiveness and adequacy of the current regime. This is followed by brief discussions of current and proposed further powers given (or to be given) to the Privacy Commissioner.

**An overview of the Privacy Act’s current approach to enforcement**

The Act allows individuals to seek a court injunction against breaches of the data protection principles, or threatened breaches, but otherwise does not allow individuals to go directly to a court to seek remedies for breaches. The Commissioner can seek injunctions from a court but has never done so. The injunction power has only once been used, in a dispute between two commercial organisations. In practice, complainants go to the Privacy Commissioner, not a court.

Individuals may complain to the OPC about any breach of the IPPs or NPPs (or other specific sets of data protection principles concerning tax file numbers, credit reporting etc – discussed
further below). On average, 1250 complaints are investigated per year, over two-thirds of which are under the private sector provisions. The Commissioner has wide powers to carry out investigations, but they are rarely if ever used. Complainants are first required to attempt to resolve the complaint with the data controller. Most complaints are handled by a process of investigation and mediation. Few systematic details are published of complaint outcomes.

The Commissioner does have, however, extensive powers to make “determinations” awarding compensatory damages or requiring apologies or remedial acts, in the event that mediation fails. The determination power has only been used eight times in the 16 years of the Act’s operation (and four of those were in the same dispute). Views differ on whether this is an indicator of successful resolution of complaints.

Because of constitutional reasons concerning separation of administrative and judicial powers, determinations by the Commissioner cannot be enforced against data controllers without the matter first being re-heard ab initio by a Court (although the findings of the Commissioner are prima facie evidence in such a hearing). The Commissioner can also seek enforcement of a determination.

If a determination is unfavourable to the complainant, the complainant has no right of appeal to a Court. The complainant can, however, seek judicial review of the Commissioner’s decision, which will generally allow review of any issues of law but not a full reconsideration of the merits of the case. There are no reported cases of complainants having obtained judicial review, only a few misconceived applications dismissed by the Courts.

If a determination is unfavourable to a data controller, the data controller has a de facto right of appeal to a Court, because it can simply refuse to comply with the determination, forcing the complainant to seek a Court hearing for enforcement which will then constitute a de novo re-hearing. No determination has ever been enforced before a Court.

Both complainant and data controller can appeal to the Administrative Appeals Tribunal to seek review of the amount of any compensation awarded in a Determination. The Commissioner has only once awarded compensatory damages in a disputed determination, and in that case the complainant successfully appealed against the low amount awarded.

The Act allows the Commissioner to conduct “own motion investigations”, using the investigative powers of the Act if needed, but these cannot result in enforceable determinations. The Act allows representative complaints to be made by one complainant on behalf of a class of complainants, and these can result in enforceable determinations in favour of all members of the class. In the only published instance of this occurring, a consumer NGO represented the class of complainants, and it is possibly no coincidence that this resulted in the only determination to date against a private sector organisation.

Anonymised determinations are published by the Commissioner. Since 2003, the Commissioner has published increasing numbers of brief anonymised summaries of significant complaints which have been resolved without a determination, now averaging 15 complaints per year.

---

Effectiveness and adequacy of the current regime

Concerning both the formal and substantive effectiveness (or, more technically, 'adequacy') of the enforcement aspects of Australia's privacy regime in 2005, Bygrave and Greenleaf concluded:

The Privacy Act 1988 provides the necessary formal elements which should be adequate to deliver a good level of compliance, support and help to data subjects, and appropriate redress. The only significant point of concern is the lack of sufficient rights of appeal against decisions by the Commissioner.

However, on the question of the actual effectiveness of the system, the evidence of adequacy is far less convincing, and is equivocal. Nevertheless, given the relatively recent introduction of the private sector provisions, and the numerous recommendations by the OPC to improve the system, it is quite possible that the effectiveness will improve considerably over the next few years.

In relation to evidence of substantive or actual effectiveness, there have been no significant changes in the past four years. Evidence of effective enforcement of both the private sector and public sector regimes by the current Commissioner (as with her predecessors) remains lacking, and discontent by many well informed observers, particularly in the consumer, NGO and academic sectors remains high. The business sector does not complain.

In relation to formal powers, the Government's proposed reforms will strengthen the powers of the Privacy Commissioner to a significant extent, as detailed below (though they were not inadequate to begin with). It may be that these increased powers, coupled with a new OIC regime and a new Privacy Commissioner as part of that, will result in evidence of more vigorously enforced enforcement post-2011.

Audit powers

Currently, the OPC does not have the power to audit a private sector organisation’s compliance with the NPPs. In contrast, it does have powers to audit Commonwealth government agencies with respect to compliance with the IPPs (s. 27(1)(h) and s. 27(2)), and to audit compliance with respect to processing of tax file numbers and credit reporting (s. 28 and s. 28A). The Commissioner is also empowered to inspect records that telecommunications carriers, carriage service providers and number-database operators must maintain in particular cases when they disclose personal information (see Telecommunications Act 1977 (Cth) s. 309; more generally, see Part 13, Division 5 of the same Act) (Bygrave and Greenleaf, 2005: 4.3.6).

The Government now proposes that the Privacy Commissioner be able to conduct ‘Privacy Performance Assessments’ (ie audits) of companies. This is good in theory, but, given that the Privacy Commissioner has suspended all public sector audits since 2007 due to a claimed lack of resources, unless the Government provides extra funding (or the OIC takes a different attitude), this grant of extra powers may be empty.

Privacy impact assessments (PIAs)

There are no provisions concerning Privacy Impact Assessments in the Privacy Act 1988.
The Government now proposes that the Privacy Commissioner will be able to direct federal government agencies (but not companies) to provide to the Commissioner a PIA on a ‘new project or development’ that the Commissioner considers will have a ‘significant impact’ on the handling of personal information, and to report to the Minister (query whether also the public) if the agency fails to do so (AusGov, 2009: 47-4). This is a valuable proposal, except that there is no requirement that a PIA be by an independent party, or that results be made public, or even that the Commissioner make such a direction public (but nothing preventing these results either). Since the Commissioner is also to produce ‘PIA Guidelines’, the effectiveness of this reform may depend to a large extent what is in those Guidelines.

The Government is to review in five years whether to extend this PIA power to the private sector (AusGov, 2009: 47-5).

**Enforcement of own-motion investigations**

The Act allows the Commissioner to conduct “own motion investigations”, using the investigative powers of the Act if needed, but at present these cannot result in enforceable determinations.

The Government now proposes that the Commissioner will be able to issue compliance notices, including notices requiring specific remedial actions, after own-motion investigations, and enforce them in the Federal Court (AusGov, 2009: 50-1).

**Civil penalties for serious or repeated interferences**

Until now the Privacy Act has not relied on fines, either through criminal penalties or 'administrative penalties' (also called 'civil penalties), as part of the privacy enforcement regime, except in relation to credit reporting (where the criminal provisions have not been used).

The Government now proposes that the Privacy Commissioner will be able to seek a civil penalty against an agency or organisation where there has been 'a serious or repeated interference' (ie breach of the UPPs), in the Federal Court. It notes that this will 'complete the enforcement pyramid', borrowing the terminology of theorists of 'responsive regulation' (AusGov, 2009: 50-1).

**Further proposals – critical analysis**

The Privacy Commissioner does not lack significant powers under the current legislation to investigate, to make determinations, or to award compensation or require other remedial actions: 'the Commissioner has ample powers to resolve individual complaints by making determinations under s. 52' (Bygrave and Greenleaf, 2005: 4.3.6).

The 2005 private sector review report by the Privacy Commissioner notes critical submissions from consumer groups and individuals about the low use of s. 52 powers, and states that the OPC “will consider whether it might be appropriate in some circumstances to use its other powers earlier, such as the determination making power”.

---

12 OPC, *supra* n. 32, p. 134.
This has not happened. The current Commissioner has not made a single use of the s52 Determinations power during her five years in office.

**Commissioner's powers to refuse to investigate complaints**

Under these circumstances, it is somewhat odd that a considerable part of the ALRC's and the Government's reforms in this area involve broadening the Commissioner's powers to refuse to investigate complaints.

The government proposes to give greater powers to the Commissioner to refuse/discontinue complaint investigation, including a vague ‘not warranted having regard to all the circumstances’ discretion (AusGov, 2009: 49-1). The Government acknowledges there are critics who insist that the Commissioner already over-uses the dismissal power in order to avoid making Determinations, saying that judicial review is still available to any dismissed complainant, and that the Commissioner will have to report on use of the extended powers in his/her Annual Report. These factors are unlikely to deter abuse of this power, as the first is too costly, and the second has no remedy nor anyone in power who pays attention to these statistics.

The Government also proposes that the Commissioner will be able to refuse to investigate complaints which in the Commissioner's view could be more suitably handled by some other complaint resolution scheme(AusGov, 2009: 49-2). The Government assumes that such schemes have ‘adequate dispute resolution processes and suitable remedies’, but does not propose to require this. This has potential for abuse by becoming a method of short-changing complainants by requiring them to use some other dispute resolution scheme which does not have power to provide compensation or the other remedies available to the Commissioner. The Government also ‘suggests’ that the Commissioner might like to publish a list of such schemes, and encourage them to ‘report back’ on privacy complaints.

**Commissioner cannot be forced to make a Determination**

The current Commissioner has never made a s52 Determination after nearly five years in office. None of the sanctions available to the Commissioner have therefore ever been used, and so no regulatory 'signals' have ever been sent to the 'market' (of potential complainants and respondents) of the 'price' of breaches of the Privacy Act. It is reasonable to suggest that this constitutes a failure of responsive regulation.

As a result, NGOs, academics and others made submissions to the ALRC that complainants who were dissatisfied with the Commissioner's attempts at mediation of their dispute should be able to require the Commissioner to make a determination (which might of course be adverse to them), which would at least set out a detailed analysis of the strengths or weaknesses of their claim. The Commissioner has expressly stated that, as a matter of practice, she considers that complainants have no right to insist upon a determination.

The ALRC recommended that the parties be able to require the Commissioner to make a determination when conciliation fails. The Government has rejected this, because it considers this might interfere with the conciliation process, and instead proposes (AusGov, 2009: 49-5):
Where the Privacy Commissioner deems that conciliation has failed, in place of the requirement in paragraph (b), the Commissioner must then decide whether to decline the complaint in line with its amended powers under section 41, investigate the complaint or investigate it further, or resolve the complaint by determination. Where the Privacy Commissioner decides not to investigate or further investigate the complaint and any parties to the complaint are not satisfied with this decision, they will have the ability to make an application directly to the Federal Court alleging interference with their privacy.

For parties to be able to enforce the UPPs by going to the Federal Court is desirable in itself, but for an applicant to have no option but to go to the Federal Court is very undesirable. The applicant must then bear their own high costs of commencing a Federal Court action, and if they lost being required to pay the costs of the corporate defendant as well. Few consumers without legal aid will take the risk. The low cost remedy that is provided by a decision by the Privacy Commission, plus a right of appeal to a low cost administrative tribunal, is lost to these complainants. Furthermore, the Privacy Commissioner continues to evade the responsibility to make decisions that the Act appears to impose.

The Government does not explain why they do not give the complainant the option instead to go to the Administrative Appeals Tribunal (AAT), which (as discussed below) will be the normal avenue for those dissatisfied with a determination by the Commissioner. Perhaps it is because there is technically no 'decision' by the Commissioner which can be the subject of a merits review of a decision. If so, this seems like an elevation of form over substance.

**Expanded powers to make s52 Determinations**

When making a determination under s. 52, the Privacy Commissioner is not able to apply systemic remedies; i.e., remedies that attempt to prevent future problems related to general patterns of behaviour or processes (beyond those directly related to the specific complaint giving rise to the determination). In other words, the OPC is unable to prescribe generally how a respondent should act. In the TICA Determinations, the Privacy Commissioner also considered that he did not have the power to require a respondent to take particular remedial actions to remedy a breach, but only to take (some) action to remedy the breach, though this was not tested in Court.

However, the Government has now decided to clarify in the Act that determinations can specify what steps must be taken to remedy a breach. It has also decided that the Commissioner will be able to make determinations ‘on the papers’ without an oral hearing (AusGov, 2009: 49-13). The Government optimistically states ‘this could lead to greater use of the determination power’, in light of the failure of any Commissioners to date to make use of this power.

**A right of appeal against Determinations by the Commissioner**

The Directive requires that decisions of supervisory authorities “may be appealed against through the courts” (Art. 28(3)). The Article 29 Working Party does not single this out as a necessary part of an adequate enforcement mechanism, but it is clearly a valuable component given that it receives separate mention in the Directive. The possibilities for appealing to the courts from a s. 52 determination by the Commissioner are restricted and unjust as between the parties. This is probably the principal deficiency of the current complaints regime of the Privacy Act 1988 (Bygrave and Greenleaf, 2005).
The Government now proposes merits review of the Commissioner's s52 determinations by the Administrative Appeals Tribunal (AAT) (AusGov, 2009: 49-5), and AAT decisions can be appealed to the Federal Court. Provided that the Commissioner does make some appreciable number of s52 determinations, this right of appeal is of particular importance, as this is the only route of any significance (the injunction power being unused) by which questions of interpretation of the Privacy Act are able to come before either an Administrative Tribunal that makes decisions involving full legal reasoning, or the Courts so that precedents may be set concerning the meaning of sections of the Act. At present, over twenty years after the Privacy Act 1988 came into force, there is only one court decision concerning the Act of any significance (on the otherwise unused injunctions power), and one AAT decision (on damages). The Privacy Act is still largely terra incognita as far as its correct legal interpretation is concerned.

As mentioned above, the Government has rejected the ALRC's recommendation that parties to complaints should be able to require the Commissioner to make a determination, but if the Commissioner will not investigate a complaint further, the Government proposes that the complainant can take the matter directly to the Federal Court. This provision, coupled with the right of appeal to the AAT (and thence to the Federal Court), will provide a right for complainants to have a complaint heard by a Court, albeit indirectly after commencing a complaint before the Commissioner. This is arguably one of the deficiencies of the current Act in relation to the A29 Working Party's requirements (see Bygave and Greenleaf, 2005: 4.3.6 for arguments).

Representative complaints

An innovative feature of the Act – rarely found in legislation in Europe or elsewhere – is that express provision for class actions is made in s. 36(2), in conjunction with ss. 38–39. This allows the Privacy Commissioner to entertain “representative complaints” if certain conditions are met. Until 2005 only two such complaints had been made. The second complaint resulted in the only findings made by the Commissioner to date requiring systemic changes by a private sector organisation (the TICA determinations).

The Government proposes that individuals can opt-out of such representative complaints (AusGov, 2009: 49-9), but otherwise proposes no changes.

16. Sectoral (Self-) Regulation and Codes of Conduct

Codes of conduct under the Privacy Act Part IIIAA

Current situation

The process of code formation and approval is regulated by Part IIIAA of the Privacy Act 1988. Basically, the Privacy Commissioner is empowered to approve codes that meet criteria specified in the Act and related guidelines. Once approved, the code replaces the NPPs as the standard to be observed by organisations that decide to subscribe to it. A code may also nominate an adjudicator – either the Commissioner or another body – to handle complaints

14 See Tenants Union v TICA Default Tenancy Control Pty Ltd, Complaint Determinations 1–4 of 2004, summarised by G. Greenleaf in Privacy Law & Policy Reporter, 2004, vol. 11, pp. 14–15. See also Case C2776, opened 3.7.1995, closed 6.12.1996. The complaint was mounted by a group of women employees at a social club who complained that video surveillance cameras had been covertly installed to film their work change-room. The complaint was withdrawn after being resolved pursuant to the Sex Discrimination Act 1984 (Cth).
under it. An overview of approved codes must be kept by the Commissioner in a publicly available register (s. 18BG).

Self-regulation and co-regulation have not turned out to be significant components of Australian privacy regulation. In 2005 the position was summarised as follows (Bygrave and Greenleaf, 2005: 5.1, and see the mechanisms for Code operation in the details following):

Co-regulation has been a much emphasised feature of recent Australian regulatory policy. It was envisaged as playing a central role in the regime established by the Privacy Amendment (Private Sector) Act 2000 (Cth)\(^{15}\) – an aspect of the regime which received favourable comment from the Article 29 Working Party in Opinion 3/2001. However, despite strong government support for it, co-regulation has so far played a minor role in practice. Only three codes have been approved under the Privacy Act. A major cause of this low level of industry uptake appears to be that code development is too costly and complex for most businesses.\(^{16}\)

The update in 2006 (Bygrave and Greenleaf, 2006: 2.15) pointed out that one new code had come into existence (the Biometrics Code), but that one of the previous three codes (the General Insurance Information Privacy Code) had been revoked by the Privacy Commissioner at the request of the industry. The position is unchanged since then, and business generally seems to have lost interest in the code of conduct aspect of the Act.

**Proposed changes**

The Government is now proposing (AusGov, 2009: 48-1) to modify the Act so that Codes do not replace the UPPs (as they previously could), meaning that businesses have to comply with the UPPs while complying with a Code. However, they will add a ‘clarification’ that it is permissible for codes to increase the protections in the UPPs but not reduce them. These provisions will strengthen the Act.

**New 'mandatory code' process**

The Government also proposes (although the ALRC did not) that the Commissioner should be able to request a group of organisations to develop a draft Code, and if they fail to do so, to develop and impose one himself/herself. These will be called ‘mandatory codes’. Such codes could cover industry sectors, or a group of organisations 'who engage in a prescribed practice (such as using certain tools or technologies)'.

The Government notes that 'This would result in a three tiered model for code development: codes voluntarily developed by organisations; mandatory codes developed at the request of the Privacy Commissioner; and where such a request is not complied with, a mandatory code developed by the Privacy Commissioner.' This model is based on Part 6 of the Telecommunications Act 1997 (Cth). The government notes that although these codes may not derogate from the UPPs, they may 'go beyond' the application of the UPPs. A breach of a binding code would be an interference with privacy under section 13A of the Privacy Act and would be subject to the usual enforcement mechanisms available for an interference with privacy.

\(^{15}\) See particularly Second Reading Speech, *supra* n. 174, p. 15750.

\(^{16}\) See OPC, *supra* n. 32, p. 166 et seq.
The extent to which the Commissioner will be able to modify a mandatory codes developed at her/his request is unclear. Nor is it clear to what extent there will be public consultation required in relation to codes developed on request (though this can probably be assumed).

At present, the Commissioner’s discretionary powers with respect to code approval are considerable, augmented by the fact that approved codes are not subject to Parliamentary disallowance and the Commissioner is not required to publish reasons for approving a code. The omission of such a requirement has been rightly highlighted as a matter of concern.17 (Bygrave and Greenleaf, 2005: 5.2). Although the Government states that the new provisions will require 'consultation with relevant stakeholders similar to that currently required for Public Interest Determinations', there is no mention of any requirement that the Commissioner publish reasons for approving a mandatory code, nor any mention of Parliamentary disallowance (both of which are required for a PID). This will require clarification during the legislative process.

These provisions may have little effect on the currently moribund process of codes voluntarily developed by industry sectors. However, the possibility of the Commissioner imposing (or 'requesting') mandatory codes in relation to those who use a particular technology is more significant than any of the ALRC's recommendations concerning technology. If the Commissioner decided to develop such a code early in the life of adoption of a particular technology, then the public participation required in code development could result in something resembling a mandatory 'privacy impact assessment' process for a technology, with a binding code resulting.

Other co-regulatory schemes relevant to privacy

The Direct Marketing Code of Practice (November 2001) and the industry codes of practice in the telecommunications sector developed pursuant to Part 6 of the Telecommunications Act 1997 (Cth), are relevant to privacy, are discussed by Bygrave and Greenleaf (2005: 5.4).

Privacy seals and certifications

There are no significant privacy seal programs operating in Australia, the Act does not mention them, and nor do the Government or ALRC proposals.

III. Summary and conclusions

Future directions of data protection in Australia

The Australian Law Reform put forward a very detailed set of recommendation in relation to Australia's Privacy Act 1988, but over half of them were only that the Privacy Commissioner should give guidance on particular topics (a matter on which the government cannot give the Commissioner directions). The other recommendations are often useful improvements to the Act, but are generally of a technical nature and do not propose any major or perhaps even significant new approaches to dealing with issues of privacy regulation. Nor do they involve a serious attempt to evaluate which aspects of the Privacy Commissioner's performance have failed, which have succeeded, and what implications this has for the needs of regulatory reform.

The Government's selection from the ALRC’s recommendations of those it proposes to enact are in general a selection of the recommendations that most favour the position of data subjects, with some notable exceptions. The Government has added some proposals of its own such as mandatory codes in relation to technologies which could be significant for the 'New challenges' project, but by and large they are a conservative set of proposals.

**Position in relation to international standards**

Australia's existing data protection regime is complex, and the question of its adequacy in terms of the Directive is equally complex and is unresolved as yet.

It is uncertain exactly how the Government’s reform proposals will translate into legislation that succeeds in obtaining passage through Parliament, or how long that will take. It would therefore be premature to make any further assessment of the 'adequacy' of Australia's laws in the terms of the Directive until that process is complete.

Because of the proposals concerning data exports, and some aspects of the complaint resolution process, it is not even certain that the reforms, if enacted, would constitute a net improvement in Australia's position in terms of adequacy.

- o – O –o -

**General references:**

For full details and references, see the two expert reports by Bygrave and Greenleaf on the adequacy of Australia’s privacy protection, in 2005 and 2006 (Bygrave and Greenleaf, 2005, 2006). See also (in particular on proposed changes and additions) the ALRC Report 108: For Your Information: Australian Privacy Law and Practice (ALRC, 2008).

**Attachments:**

I. Queensland’s Information Privacy Act 2009  
II. ALRC's Model Unified Privacy Principles (UPPs)
Appendix I: Queensland’s Information Privacy Act 2009

The Information Privacy Act 2009 combines principles that hark back to the 1980s with an enforcement mechanism that is thoroughly up-to-date. It adds another layer of complexity to Australia’s patchwork of privacy laws.

The scope of the Act is broad, covering most parts of Queensland’s public sector including local government (s18), and Ministers but only in relation to the agencies they administer (s20). Complete exemptions are few (Schedule 2), the most significant being the Parliament, judicial aspects of adjudicative bodies, and government-owned corporations (as they are covered as private sector bodies by the Federal law).

The Act gives statutory effect to the two sets of administrative principles which Queensland agencies have been supposed to follow since 2001 (Information Standards 42 and, for the Health Department, 42A), although there has been no supervisory authority or reports on implementation.

The eleven Information Privacy Principles (IPPs) in the Schedule 3 of the Act are based squarely on the eleven similarly named principles applying to the Federal public sector in the Privacy Act 1988 (Cth). However, they have numerous differences in wording, some with ‘plain English’ motivations but others being differences of substance. These principles also have many differences from the Uniform Privacy Principles (UPPs) proposed by the Australian Law Reform Commission in its review of the private sector and federal agency provisions (see Greenleaf and Waters, Privacy Laws & Business Issue 97), and so will need to be replaced if the ALRC has its way.

To add a little more complexity, the IPPs do not apply to the health department. Instead, the ‘National Privacy Principles’ (NPPs) in the Privacy Act 1988 (Cth), which apply to private sector health providers in Queensland also apply to the Health Department (s31). The 1988-vintage IPPs do cover everything you would expect of OECD-influenced sets of principles. Missing are any post-1980s principles such as deletion/de-identification or data breach notification principles.

The Queensland IPPs inherit many deficiencies from their Federal cousins, including:

- Although collection is limited to data ‘directly related’ to an agency’s lawful purposes, the finality principle is weakened in relation to disclosures because the collecting agency can merely declare in a notice to a data subject that it is its ‘usual practice’ to disclose the data to some other entity (not necessarily an agency) (IPP 1), and that notice is then in itself sufficient justification for the disclosure to the entity (IPP 11), provided the entity is only collecting the data for a legitimate purpose. By this means, agencies can ‘bootstrap’ disclosures that they could not otherwise justify.

- Requirements to give notice, to ensure data quality at time of collection, and to avoid intrusiveness, only apply if data is collected from the person concerned (IPPs 1 and 3), and not when collection is from a third party or (perhaps) by observation.

- Uses and disclosures need to be logged when made for investigative purposes (IPP 10(2) and IPP 11(2)), but not for any other purposes.

Innovations in the Queensland IPPs include:

- A broad exemption for both uses and disclosures for research or the generation of statistics, in the public interest, where publications are de-identified and obtaining consent is not practicable (IPPs 10 and 11).

- ‘Disclose’ is defined to mean where entity B did not know certain personal information and was not in a position to find out, and entity A either gives entity B the information or makes it possible for it to find out, and A ceases to control B in relation to who will know the information in future (s23). This definition has various implications, such as (a) information is not ‘disclosed’ if the recipient already knows the information (a dangerous rule, unless the source of the information is included as part of the information); and (b) there can be disclosure of information even if the discloser is not in possession of the information but discloses, for example, an access code on a third party’s system.

- ‘Use’ of personal information is explicitly defined to include taking it into account in the making of a decision, and intra-entity transfers to a part of an entity with a different function (s23). Although ‘use’ and ‘disclose’ are key terms, such explicit definitions are unusual in Asia-Pacific data protection laws.

- An agency can disclose personal information to another entity for marketing purposes, but must ensure that entity complies with rules very similar to those governing direct marketing in the NPPs (IPP 11(4)).
In common with a trend in other Australian jurisdictions, the Act transfers access and correction rights and processes in relation to an individual’s own personal information from the freedom of information legislation to the privacy law (Chapter 3).

Separate from the IPPs, there is a data export limitation principle (s33) which purports to limits transfers to ‘an entity outside Australia’ (not ‘outside the State’, unlike the equivalent controls in the Victorian and NSW laws). The conditions for a personal data export are based on NPP 9 in the Federal Act, but modified to apply to agencies, and also tightened so as to require a higher standard than the Federal provisions (which are not as restrictive as EU Directive Article 25). Personal data cannot be so exported unless the individual agrees, unless the transfer is authorised or required under a law, or the agency reasonably believes that the transfer is necessary to prevent or lessen various types of ‘serious threats’, or unless the transfer meets at least two of four further conditions (any one of which was sufficient to meet the Federal provisions). The four conditions, in summary, are (i) reasonable belief in similar principles being enforceable at the export destination; (ii) necessary for performance of the agency’s functions; (iii) for the benefit of the individual, and consent would have been likely if possible to obtain; or (iv) the agency has taken reasonable steps to ensure that recipient will act consistently with the IPPs.

The signal problem with this provision is that since it is located outside the IPPs, none of the Act’s enforcement provisions apply to it. Both the requirements for a compliance notice (s158) and the privacy complaint provisions (s164) only apply to IPPs. The meaning of ‘IPPs’ is limited to what is in Schedule 3 (s25, s26 and Schedule 5 Dictionary). By the same token the commissioner cannot relax s33 any further by the waiver/modification procedure (s157), since it also only applies to an IPP. This is all either a result of negligence by the draftsperson (and the Parliament) or an indefensible policy choice of an unenforceable ‘principle’. The latter seems unlikely, but the Explanatory Notes to the Bill shed no light.

A Privacy Commissioner is to be appointed as a deputy to the Information Commissioner, who can delegate powers to him (s139), and can direct him (s142). Both are referred to herein as ‘the Commissioner’. The Information Commissioner’s office is now being established as part of a conjoint review of Queensland’s FOI law, following recommendations of the Solomon review of 2008. The Privacy Commissioner, although oddly described as a member of the Information Commissioner’s staff (s141), is to be appointed after advertisement and after consultation with a Parliamentary Committee (s145) and can be re-appointed for up to a total of ten years (s146). The newly-established Queensland Civil and Administrative Tribunal (QCAT) commencing in December 2009, is to be the adjudicative body in relation to complaints.

The Act enables persons to make a complaint about the handling of their personal information by an agency first to the agency for internal review (s166(2)), and then if the agency is unable to satisfy the complaint, to the Commissioner who must take all reasonable steps to mediate the complaint (s171). The terms of agreement of successful mediations can be certified by the Commissioner, and the terms then enforced by QCAT (s172, 173).

The Act is, on paper, too rigid in its timing requirements and gives the Commissioner too much latitude to discontinue complaint investigations because of ‘lack of cooperation’ by complainants or other reasons (s168). Complainants cannot bypass the Commissioner and go directly to the Tribunal after internal review (in contrast to NSW), or to the Courts (s39). Much will depend on the Act being sympathetically administered. If mediation is unsuccessful, then at the request of the complainant (only), unresolved complaints must be referred by the Commissioner to QCAT (s176). Following a hearing, QCAT will be able to make orders for a range of remedies for breaches of the privacy principles (s178), including requiring injunctions against continuing breaches, apologies, compensation of up to A$100,000, and reimbursement of expenses in pursuing the complaint. This approach is most similar to that in the Victorian legislation.

Breaches of the IPPs can also result in the Commissioner issuing compliance notices to an agency, where a breach is ‘serious or flagrant’, or has occurred on five separate occasions in two years (s158). Agencies must take all reasonable steps to comply or they can be subject to a civil penalty (s160). They can seek a review by QCAT (s161).

The Commissioner has other broad powers including conducting reviews of any systemic privacy issues, reporting results to Parliament, ‘conducting compliance audits’ of any entities under the Act, commenting on any privacy issues relating to the public sector, and issuing guidelines on the application of the Act and ‘privacy best practices generally’ (s137). Much will depend on the size of the Commissioner’s budget allocation to carry out these tasks, which is subject to government determination, but his/her priorities and exercise of powers are not otherwise subject to direction (s134).

The Commissioner also has a power of approving waivers or modifications of agencies’ obligations to comply with the IPPs (s157). Such exemptions are called ‘Public Interest Determinations’ in the Federal Act, and as in that Act the Commissioner here must be satisfied that such a waiver or modification is in the public interest. In the Queensland Act there are no provisions for public hearings or submissions before such an approval is made, but it is treated as subordinate legislation (s157(2)) and is thus subject to Parliamentary disallowance.
Appendix II: ALRC’s Model Unified Privacy Principles (UPPs)

UPP 1.  Anonymity and Pseudonymity
Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:

(a) not identifying themselves; or
(b) identifying themselves with a pseudonym.

UPP 2.  Collection

2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:

(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
(b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented;
(b) the collection is required or authorised by or under law;
(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;
(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:
   (i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and
   (ii) at or before the time of collecting the information, the organisation undertakes to the individual to whom the information concerns that the organisation will not disclose the information without the individual’s consent;
(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;
(f) the collection is necessary for research and all of the following conditions are met:
   (i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable;
   (ii) it is unreasonable or impracticable for the agency or organisation to seek the individual’s consent to the collection;
   (iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and
(iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or

(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.

2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.

UPP 3. Notification

3. At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:

(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;
(b) identity and contact details of the agency or organisation;
(c) rights of access to, and correction of, personal information provided by these principles;
(d) purposes for which the information is collected;
(e) main consequences of not providing the information;
(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;
(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency’s or organisation’s Privacy Policy; and
(h) fact, where applicable, that the collection is required or authorised by or under law.

UPP 4. Openness

4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:

(a) sort of personal information the agency or organisation holds;
(b) purposes for which personal information is held;
(c) avenues of complaint available to individuals in the event that they have a privacy complaint;
(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and
(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:

(a) electronically; and
(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.

UPP 5. Use and Disclosure

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
(ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose;

(b) the individual has consented to the use or disclosure;

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:
   (i) an individual’s life, health or safety; or
   (ii) public health or public safety;

(d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities;

(e) the use or disclosure is required or authorised by or under law;

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:
   (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
   (ii) the enforcement of laws relating to the confiscation of the proceeds of crime;
   (iii) the protection of the public revenue;
   (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or
   (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;

(g) the use or disclosure is necessary for research and all of the following conditions are met:
   (i) it is unreasonable or impracticable for the agency or organisation to seek the individual’s consent to the use or disclosure;
   (ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act;
   (iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and
   (iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable; or

(h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.

5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.

5.3 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation’s primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. Nothing in subclause 5.1 requires an agency or organisation to disclose personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.
Note 3: Agencies and organisations also are subject to the requirements of the ‘Cross-border Data Flows’ principle when transferring personal information about an individual to a recipient who is outside Australia.

UPP 6. Direct Marketing (only applicable to organisations)

6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:
   (a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and
   (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.

6.2 An organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:
   (a) either the:
      (i) individual has consented; or
      (ii) information is not sensitive information and it is impracticable for the organisation to seek the individual’s consent before that particular use or disclosure;
   (b) in each direct marketing communication, the organisation draws to the individual’s attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;
   (c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and
   (d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual’s personal information.

6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:
   (a) comply with this requirement within a reasonable period of time; and
   (b) not charge the individual for giving effect to the request.

UPP 7. Data Quality

An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

UPP 8. Data Security

8.1 An agency or organisation must take reasonable steps to:
   (a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure; and
   (b) destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.

8.2 The requirement to destroy or render non-identifiable personal information is not ‘required by law’ for the purposes of the Archives Act 1983 (Cth).

Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

UPP 9. Access and Correction

9.1 If an agency or organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:
Where the information is held by an agency:

(a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or

Where the information is held by an organisation:

(b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;

(c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;

(d) the request for access is frivolous or vexatious;

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings;

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;

(g) providing access would be unlawful;

(h) denying access is required or authorised by or under law;

(i) providing access would be likely to prejudice an investigation of possible unlawful activity;

(j) providing access would be likely to prejudice the:

(i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) protection of the public revenue;

(iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.

9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

9.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.

9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.
9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

(a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and

(b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and:

(a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and

(b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;

the agency or organisation must take reasonable steps to do so.

9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:

(a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the information; and

(b) notice of potential avenues for complaint.

UPP 10. Identifiers (only applicable to organisations)

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.2 Where an identifier has been ‘assigned’ within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or

(c) the identifier is genetic information and the use or disclosure would be permitted by the new Privacy (Health Information) Regulations.

10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

10.4 The term ‘identifier’, for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

(a) uniquely identifies or verifies the identity of an individual for the purpose of an agency’s operations; or

(b) is determined to be an identifier by the Privacy Commissioner.

However, an individual’s name or ABN, as defined in the A New Tax System (Australian Business Number) Act 1999 (Cth), is not an ‘identifier’.
Note: A determination referred to in the ‘Identifiers’ principle is a legislative instrument for the purposes of section 5 of the Legislative Instruments Act 2003 (Cth).

UPP 11. Cross-border Data Flows

11.1 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.