# Privacy in Australia

Graham Greenleaf, Professor of Law, University of New South Wales


6 March 2008

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Formative episodes, 1987-1992</td>
<td>2</td>
</tr>
<tr>
<td>Key personal data systems and their impact</td>
<td>5</td>
</tr>
<tr>
<td>Major privacy measures and institutions</td>
<td>7</td>
</tr>
<tr>
<td><strong>I Key developments in privacy protection</strong></td>
<td>8</td>
</tr>
<tr>
<td>The Australian legal context – Privacy rights and the Courts</td>
<td>8</td>
</tr>
<tr>
<td>The Australian legal context – Legislative powers to protect privacy</td>
<td>9</td>
</tr>
<tr>
<td>The very slow rise of information privacy legislation</td>
<td>10</td>
</tr>
<tr>
<td>Privacy principles – Many laws, similar content</td>
<td>11</td>
</tr>
<tr>
<td>Limited effectiveness of the federal public sector law</td>
<td>14</td>
</tr>
<tr>
<td>Are the State and Territory public sector laws any better?</td>
<td>16</td>
</tr>
<tr>
<td>The rocky road to private sector legislation</td>
<td>18</td>
</tr>
<tr>
<td>Is the private sector legislation effective?</td>
<td>19</td>
</tr>
<tr>
<td><strong>II Role of public opinion</strong></td>
<td>20</td>
</tr>
<tr>
<td>Public and organisational attitudes to privacy protection</td>
<td>20</td>
</tr>
<tr>
<td>Elite involvement in privacy issues</td>
<td>21</td>
</tr>
<tr>
<td>Public opinion’s influence on privacy developments</td>
<td>22</td>
</tr>
<tr>
<td><strong>III Local culture and traditions vs international influences</strong></td>
<td>23</td>
</tr>
<tr>
<td>National culture and traditions</td>
<td>23</td>
</tr>
<tr>
<td>International privacy developments and their influence</td>
<td>23</td>
</tr>
<tr>
<td><strong>IV Winners and losers</strong></td>
<td>24</td>
</tr>
<tr>
<td>Information flows and constraints</td>
<td>25</td>
</tr>
<tr>
<td><strong>V Prospects for the future</strong></td>
<td>25</td>
</tr>
<tr>
<td>The political ascendancy of surveillance post-2001</td>
<td>26</td>
</tr>
<tr>
<td>‘The Access Card’ ID system – another near miss</td>
<td>27</td>
</tr>
<tr>
<td>Back to ‘muddling through’?</td>
<td>28</td>
</tr>
</tbody>
</table>
Introduction

The defining events in the history of privacy protection in Australia have had a great deal to do with politics, little to do with an orderly process of law reform, and nothing to do with the Courts.

Formative episodes, 1987-1992

The Australia Card In June 1987 a federal Labor Government was triumphantly returned to office after an unprecedented dissolution of both houses of Parliament. That dissolution had been trigged by Opposition rejection of a Bill to introduce a national identity card, the Australia Card. Since the idea of an ID card to combat tax and welfare fraud was first floated in mid-1985, public support had stayed around 68%. But three months later it was down to 39% and falling, and the intensity of the mounting opposition to the Card astonished everyone. Though it had rarely been a newsworthy item before or during the election, by September the media were preoccupied with the Card. Sydney talk-back radio journalist John Tingle claimed that for some weeks it was impossible to get callers to talk about anything else. The Australian newspaper editorialized (15/9/1987), when letters to the editor were running twenty to one against the Card:

“"There has never been a debate like it in the letters page; there has never been such a cry of opposition from the nation over one topic...It has dominated the mailbag to the point where today, for the first time, we present two pages on the topic.”

With dissidents appearing in its own ranks (particularly in State Parliaments), Labor faced a totally unexpected political crisis. It received a dramatic face-saving exit when opponents found an apparent loophole in the Bill’s drafting. This meant that the Opposition-controlled upper house could indefinitely delay the effective introduction of the Card even though the government’s election victory guaranteed passage of the Bill. There was considerable dispute over whether the drafting flaw was fatal (Starke 1987, Greenleaf, 1987a), but the Government quickly dropped the Bill rather than endure the politics.

What had caused the massive change in three months? With the election over (so government supporters were more willing to be anti-ID), and the reality of the Card imminent, potential opponents of the Card joined forces in a number of extra-Parliamentary opposition groups. The media-oriented Australian Privacy Foundation was formed as a coalition of public figures spanning the political spectrum, including rock singers, yacht designers, doctors and academics. By September, many grassroots local groups held significant anti-Card rallies, at a rate of more than one per day, with consequent continuous media attention. An important factor was a deep-seated distrust of the Health Insurance Commission (HIC), which was to operate the Card's computer system (Greenleaf and Nolan 1986, Greenleaf 1987a). The more people knew about the Australia Card, the less they liked it. It would in fact have been an extremely extensive information surveillance system with multiple uses from inception, no logical limits (or
intended limits) to its expansion, and de facto extension as a principal identifier in the private sector (Greenleaf 1987b, Greenleaf and Nolan 1987, Clarke 1988).

Twenty years later, Australia still does not have a national ID card. It has become a ritual observance in Australian politics for supporters of any identification scheme to deny that it ‘is anything like the Australia Card’, because the opprobrium attached to that name is still so strong. Yet in 2007 the Australian government was once again proposing to introduce a ID system, the ‘Health and Welfare Access Card’, which opponents argued would be worse than the Australia Card, but the government insisted was not a national ID card. This ritual is so entrenched that the legislation to enable the proposed card contained a clause proclaiming that it was not intended to be a national identification system. We will now take the journey from the Australia Card of 1987 to the Access Card of 2007.

Public sector surveillance emerges 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, Australia’s first enforceable privacy legislation. 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 new system, often called the ‘parallel data matching’ scheme, was strongly but unsuccessfully opposed by privacy advocates. They took the view that if promises of privacy protection could so easily be broken once a surveillance system was established, then the TFN system was likely to become ‘the Australia Card by installments’ (Greenleaf, 1990). This extension achieved some of the data matching aims of the original Australia Card proposals. 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 (OPC Annual Report 2004-05, Tables 3.1 and 3.4). There have been some limited further legislative extensions of the TFN system, but fifteen years later the TFN and the parallel data matching system has not been expanded further into one general purpose ID number and system. In this case ‘function creep’ was significant but not endless. However, as detailed below, other data matching schemes now pour data into the five key agencies, where it adds to the data used for ‘parallel data matching’.
**Positive reporting’s negative dividend** The defeat of the Australia Card, and its TFN and data-matching sequels, were key determinants of the shape of public sector surveillance for the next decade or more. The private sector equivalent was the defeat in 1991 of attempts to introduce ‘positive reporting’ by Australia’s near monopoly credit bureau, the Credit Reference Association of Australia (CRAA). In 1989 CRAA provided over 95% of consumer credit reports. CRAA and other Australian credit bureaux only provided ‘negative reports’, meaning that their credit provider members only reported when a consumer defaulted on a credit arrangement, by late payment or otherwise, plus details of applications for credit, but not whether credit was granted. In 1989 CRAA proposed to change to a system of ‘positive reporting’ whereby all major credit providers in Australia would provide CRAA with a monthly computer tape listing the ‘payment performance’ of each of their credit customers, whether or not there had been any default on the account. They claimed that this would allow credit providers to assess whether an applicant was over-committed. This resulted in considerable adverse media comment. Capitalising on this, the Australian Privacy Foundation (the NGO formed to fight the Australia Card) convened a ‘Credit Reporting Summit’ in early 1990, at the conclusion of which the federal justice and consumer affairs Ministers jointly announced that the Government would introduce legislation to prohibit ‘positive reporting’ and, furthermore, to comprehensively regulate credit reporting (Greenleaf, 1992).

The resulting legislation overturned previous practices. Over the previous twenty years, in the absence of effective prohibitions in State legislation, CRAA had allowed real estate agents to check prospective tenants, government departments to check some occupational licence applicants (and applicants for telephone and other government services), insurers to check the credit history of suspect insurance claimants, and mercantile agents to search for debtors’ addresses. Employment checking was not allowed. The new Act prohibited access to credit reporting files for any of these purposes. It added a set of information privacy principles tailored for credit reporting, plus a considerable number of criminal offences. CRAA had successfully extended the scope of its surveillance system for twenty years, but in attempting to further expand into ‘positive reporting’, it provoked far more extensive legislative control. The legislation therefore not only limited the future expansion of credit reporting in the private sector, it effectively ‘rolled back the clock’ by banning past extensions of credit surveillance which had become accepted practice in the private sector. It was described by CRAA as ‘the most restrictive credit reference laws in the Western world’. (Greenleaf, 1992) It is rare for privacy legislation anywhere to attempt such a retrospective repeal of the extension of data surveillance. This legislation in effect destroyed CRAA’s momentum toward becoming a comprehensive personal data register for the private sector. However, one downside was that from 1992 the practices such as tenancy checking that were forced out of the well-organised CRAA system in effect went unregulated until legislation caught up with the rest of the private sector in 2001.

Fifteen years later, personal information is still held by Australia’s private sector in separate databases relevant to each industry sector, rather than in centralised multi-use repositories. CRAA’s successors (Baycorp Advantage, now called Veda Advantage) revives the call for positive reporting every few years (Baycorp 2002) but without success as yet. Australia’s 2001 privacy legislation for the whole private sector, preserves
the ‘containment’ of personal information within industry sectors (sometimes called ‘silos’). This would not have happened if the key battle had not been won when CRAA overreached itself.

**Key personal data systems and their impact**

Here are some pieces in the Australian jigsaw puzzle of surveillance, and the legislative context on which the practices depend.  

*Closed-circuit television* (CCTV) saturates the infrastructure of Sydney and Melbourne, in city streets and train stations, on buses, trains and taxis, sporting venues and in crime hot spots (Chulov and Hodge, 2005). The ostensible reasons are personal safety and crime prevention, but the anti-terrorist dimension became clear with the installation of 315 extra cameras with face recognition technology in public transport facilities for the purposes of the September 2007 APEC meeting in Sydney (Besser and Clennell, 2007). One reason for this proliferation is that there is no legislation governing visual surveillance in public places. Australia spends more money per capita on workplace surveillance equipment than most other industrialised nations (Bromberg 2004, cited in Cripps 2004). 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 quadrupled from 1998 to 2003, to more than 2,500 per year (*T(I)A Annual Report* (2002-3) and earlier years).

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*).

The statutory ‘parallel data matching’ system, already explained, 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, Baycorp 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.

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 (eg 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 new companies are attempting to aggregate publicly available personal information, particularly Acxiom which claims that its InfoBase product is the largest
collection of Australian consumer and business data available in one source (Acxiom website, 2005). It is provided to clients principally for customer relationship management and direct marketing. For example, they sell lists of ‘pre-movers’, people who are about to move and therefore whose loyalty to existing businesses may be weakened, as well as ‘New Movers’, ‘Renovators’, ‘Affluent Homeowners’ and so on.

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. 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, and $1M for its principal (Clarity1 Case, 2006).

**Major privacy measures and institutions**

The Courts have not yet developed any general common law protection of privacy. Privacy Commissioners have been so mild and technical in their enforcement of privacy legislation that they rarely win public attention. Compared with the essentially political events outlined at the outset of this Chapter, the enforcement of privacy laws by Courts or privacy Commissioners have lacked defining moments which shape public or elite consciousness about privacy.

By 2007, 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) and Tasmania (plus a Bill in passage in Western Australia). This leaves only South Australia and Queensland without such a law but only non-enforceable government administrative rules. 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 contains a set of information privacy principles based substantially on the OECD privacy principles (OECD, 1980). 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. Nevertheless for the purposes of this chapter 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.

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.

I Key developments in privacy protection

The Australian legal context – Privacy rights and the Courts

The determining factors in Australia’s privacy history have been political conflict, the media and their effective use, and legislation (both its passage and its defeat). Unlike elsewhere Courts have played a minor role. Why is this so? Australia’s very boring history, constitutional structure, and legal history provides much of the explanation of why privacy is protected in Australian law principally by a patchwork of specific legislation, not by any broad remedies developed by the Courts.

The political context is that 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. But as we will see, such a boringly happy history provides no guarantees against the emergence of a surveillance state in the 21st century, and could prove to be a disadvantage.

Australia is a federation of eight states and territories, all of which have a common law tradition. It 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.

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, and awarded her A$234,000 damages (Jane Doe v ABC case, 2007). The case is now on appeal. Many
lawyers had believed that an old High Court case (Victoria Park Case, 1937) established that there was no such common law right of privacy, but in 2002 the High Court said this was still unresolved (Lenah Game Meats Case, 2002). The appeal cases in Jane Doe v AB may resolve this question.

Nicholas Toonen, 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. How did he get there? 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). So the first complaint made against Australia under the ICCPR was on a privacy issue under Article 17 (Toonen’s Case, 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. Toonen’s case shows that the protection of privacy in Australia through international law, while very limited, is possible.

The Australian legal context – Legislative powers to protect privacy

As a result of these limits in Australia’s constitution, common law rights and international obligations, 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 very slow rise of information privacy legislation

Privacy as a public issue in Australia is usually traced to a series of radio lectures by Professor Cowen published later as *The Private Man* (Cowen, 1969). Throughout the 1970s and 1980s many bills to protect privacy in various ways were introduced into Australian parliaments (see Jackson, 2001), but except in New South Wales (and some unimportant credit reporting laws elsewhere) they all failed to be enacted.

The Privacy Committee of New South Wales (Australia’s largest State) appeared to be innovative when established in 1975, the third permanent privacy protection body in the world, following Sweden and the Lander of Hesse, Germany. It was enacted after recommendations in a law reform report (Morison Report, 1973). From 1975 - 1999 the *Privacy Committee Act 1975* empowered the Privacy Committee to act as a ‘privacy ombudsman’, which could investigate any alleged invasions of privacy in the public or private sectors. It had strong powers, which it never used, to conduct such investigations and then to attempt to conciliate, and to make recommendations. The Act did not contain any definition of privacy, nor any information privacy principles, nor any enforceable rights or penalties. The Committee consisted of 12 statutory appointees largely independent of government, but dependent upon it for staffing etc. Over its nearly 25 years of existence the Committee conciliated numerous complaints, and influenced NSW legislation (particularly concerning workplace surveillance) and government proposals to be less privacy-invasive (see NSWPC Annual Reports, 1975-99). It had a high public profile in the late 1970s and played a significant role in raising elite and public awareness of privacy issues, but left a limited legacy. It failed to publish any useful details of its complaint resolutions, so the instructional value of its long history was lost. For some years it had a perverse policy of opposing enforceable privacy legislation. The Committee’s ‘Voluntary Agreement’ with the credit industry in 1976 gave individuals a non-statutory right to access and correct their credit bureaux files, and was the basis of credit reporting practices until the federal legislation of 1991. It played a courageous role in opposing the Australia Card in 1986-87. But the NSW Privacy Committee was a dead end, emulated briefly in Queensland and by an irrelevant non-statutory committee in another State.

Enforceable rights of correction of records of personal information held by federal agencies were included in the federal Freedom of Information Act 1982, in advance of general privacy legislation. They then became a standard feature of FOI Acts in every Australian jurisdiction, even those that still have no general information privacy laws. Privacy Commissioners have usually left access and correction complaints to be resolved by the FOI system.

The Australian Law Reform Commission (ALRC), chaired by Justice Michael Kirby, received in 1976 a reference on the protection of privacy, as a result of an incoming government’s election platform. In 1978 Kirby was also appointed as the Chair of the
expert group asked to make recommendations on privacy to the OECD, which resulted in the 1980 OECD privacy Guidelines (OECD, 1980). The ALRC’s report on Privacy (ALRC, 1983) took seven years to produce but in the end only recommended non-binding OECD-influenced Information Privacy Principles for the federal public sector. By 1983 this approach had already been overtaken by enforceable privacy laws in many European countries, and was to a large extent a wasted opportunity. Politics had to perfect the ALRC’s incomplete solution.

Australia symbolically agreed on New Year’s Day 1984 to ‘adhere’ to the OECD Privacy Guidelines (OECD 1981), but the Federal Government made no moves to introduce privacy legislation. In 1985 the Hawke/Keating Labor government introduced its Australia Card proposal, and the Privacy Bill 1986, which like the ALRC’s proposed bill did not include any enforceable provisions, was introduced to Parliament as part of the ‘package’. As we have seen, the defeat of the Australia Card proposal in 1987 resulted in a political compromise. The opposition parties, supported by consumer and advocacy organizations, agreed to passage of legislation for a strengthened TFN surveillance system, which the Government promised would only be used to stop tax evasion. They did so on the basis that it was ‘balanced’ by the simultaneous passage of the Privacy Act 1988, based in part on the ALRC’s recommendations, but which would now include enforceable information privacy rights stated in eleven Information Privacy Principles and a federal Privacy Commissioner to enforce them. Australia’s first enforceable privacy legislation thus resulted from hard-fought mass campaigns against surveillance, followed by elite negotiations over a compromise.

**Privacy principles – Many laws, similar content**

So Australia obtained its first information privacy law, the federal Privacy Act 1988, with eleven Information Privacy Principles at its core, and applying only to the federal public sector and that of the Australian Capital Territory. It took another decade before NSW enacted the first similar State legislation covering its public sector (1998), followed by Victoria (2000), the Northern Territory (2002), and Tasmania (2006), and in a Bill introduced in Western Australia (2007).

What rights do these Acts create, and are they enforced? The content of the Information Privacy Principles (IPPs) is not very surprising, particularly as most can be traced to the OECD Guidelines, with some later influences from the EU Directive. There is as yet such a scarcity of authoritative interpretation by Courts, Tribunals or Privacy Commissioners that the interpretation of many of the key provisions of all Acts is speculative. The description below is relevant to the IPPs in all seven jurisdictions with information privacy laws except where major variations by jurisdiction are noted.

**Key Terms** All of the Acts apply to ‘personal information’, which means information or an opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion itself, or with other information that can be expected to be used in combination with it. Most uses of information about a person which affect privacy will be caught by such definitions. However, they will not catch uses of data which are sufficient to allow an organisation to interact with an individual in
a personalised manner even though they do not know the person’s identity, such as telephone numbers and Internet Protocol addresses (which may be correlated with consumer behaviour) (Greenleaf 1996).

When a University lecturer disclosed personal information about a student to another University without following the correct procedures, it was not in breach of the legislation because the information about the student was only ever held in the mind of the lecturer, and had not been written down (*FM v Macquarie case*, 2005). All Australian legislation requires that personal information must have entered into a ‘record’ of an organisation before the law applies. Information only ever held in the minds of employees of a business, or a public servant, falls outside the Acts. However, once the information has entered a record, visual or verbal disclosures may constitute breaches.

All the Acts exclude information contained in a ‘generally available publication’ (or some similar expression) such as a newspaper, book or public register. This does not, however, exempt the databases or other records from which the ‘generally available publication’ is derived, and the question then becomes whether it is an allowable use of the information in the database to include it in a generally available publication. For example, an agency may hold a database of adopted children, but this does not mean it could publish a book listing such children.

**Collection limitations** Information may only be collected for purposes related to the objective functions of organizations, but within this relatively weak limit there is no requirement that the purpose be socially justified in some way. There is no provision for Privacy Commissioners or anyone else to require privacy impact assessments (PIAs) before systems involving particularly sensitive collection and use are built. Collection must be of the minimum information necessary for the purpose of collection, and by fair and lawful means. An additional limit is the Anonymity Principle found in all State and Territory laws (except that of NSW), which requires that individuals be given the option of anonymity in a transaction wherever it is lawful and reasonable to do so. This potentially radical principle remains untested, but could be used, for example, to attack the development of tollways or road tunnels which do not provide any option for payment by cash or some other method preserving anonymity.

Notices must be given to the individual on collection from him or her (and in some Acts even where the information is collected from a third party), specifying purpose, likely disclosures, and means of access and correction. These notices have done more than anything else to make Australians aware that they do have some privacy rights, because they see ‘Privacy Notice’ on so many forms, even though the content is often prolix, in fine print, and unread.

**‘Finality’ limits on use or disclosure** All Acts allow only four means of using or disclosing personal information beyond the primary purpose for which it was collected. The first is consent. Australian laws generally allow implied consent in addition to express consent, with the likely result that in some cases a failure to opt out will be taken to be consent. Second is typically that the use is related to the purpose of collection and is such that the individual would ‘reasonably expect’ the use. Third is where it is necessary to avoid harm to the individual or another, or (generally) for various purposes of
prevention or detection of crime or other wrongdoing. Finally, Australian legislation generally has an exemption where ‘the use or disclosure is required or authorised by or under law’ including common law principles. This final exemption means that any data controller can, if it wishes, comply with any legislatively authorised request for information. The extent of legal data flows between organisations is impossible to calculate. This exemption has been rightly criticised by Europeans for being unacceptably broad (A29 Working Party, 2001). In the private sector law there is an exception, similar to the one found in EU law, which allows direct marketing by an organisation to its customers, provided it gives them a means to opt out of further communications.

The corollary of notices on collection in creating public awareness is refusals to disclose information ‘Because Of The Privacy Act’. ‘BOTPA’ is a mantra that is now recited by desk and telephone clerks whenever you visit or ring an agency or company and request details from (or actions in relation to) your own files, and even more so if you ever ask for any information about another person. In the former case you must go through a sometimes elaborate and formal process of answering a number of questions to establish your identity. In the latter, people are becoming familiar with the irritation of being unable to obtain information about spouses, children or parents (ostensibly BOTPA) where it is perfectly reasonable for them to do so,. Some noted BOTPAs were claimed in justification of the lack of anti-theft cameras in aircraft luggage holds; in the refusal to disclose details of $300 million of unlawful payments in Iraq; in refusals to release details of the roles of military personnel in Australia’s worst military disaster in a decade; and in an attempt to make a journalistic briefing about abuse of a Departmental client confidential, where the effect was to cover up the malperformance of the Department and its contractors (APF, 2007a).

Access and correction rights, already available in the public sectors through FOI laws, only became common in the private sector after 2001. They are of course central to any IPPs. Their operation in Australian FOI and privacy laws is similar to other countries (Waters and Greenleaf, 2005).

With theft of personal data now becoming a far more serious problem, the security principle is a particularly valuable right against data controllers who may negligently allow personal data to be stolen, particularly as substantial claims for compensation may be available, such as the A$25,000 settlement discussed below (Waters and Greenleaf, 2004). Some Acts add a deletion 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’ (from the private sector law).

Data exports and Australian consumers In August 2005 a television documentary revealed that information on Australians was being sold on the Indian black market after being outsourced by the local agent of an Australian telecommunications company to a call centre provider in India. Its staff had been collecting excessive personal details such as passport numbers) without authority of their client, then selling them and other details (‘Four Corners’, 2005). The Privacy Commissioner promptly launched an ‘own motion’
investigation of both Australian companies. What can she do when personal data of Australians is exported and misused in countries with no privacy laws?

Australia prohibits transfers of personal information to any recipient in a foreign country unless one of six conditions apply. The six conditions are so broad that only a very disorganised business could fail to comply with them. They include obtaining express or implied consent to the transfer, or taking reasonable steps to ensure that the data is held, used and disclosed consistently with the IPPs. However if the apparently compliant Indian outsourcer turns out to be a rogue or to have inadequate security (even over its own staff), then the Australian consumer has no remedy against the Australian data controller under the Australian legislation. Little wonder that there are as yet no reported breaches of IPP 9. This is the only personal data export restriction law in force outside Europe, but it is weak protection.

**Limited effectiveness of the federal public sector law**

The federal *Privacy Act 1988* has been in operation for nearly twenty years, so there should be more evidence on which to assess its effectiveness than for more recent State and Territory Acts.

The Privacy Commissioner’s role has significant limitations. The Commissioner is an independent statutory office, but is appointed by the executive government, not Parliament, for a renewable five year term. He (or she in two of the four appointments to date) is dependent on the executive for a budget, and has no security of tenure in any position after the completion of his or her term as Commissioner, so it is a conditional independence. The Act has limited scope because it does not recognise any general notion of ‘breach of privacy’, but only deals with breaches of the IPPs discussed above. Outside the investigation of individual complaints, the Commissioner’s powers are limited. He has powers to audit federal agencies’ compliance with the IPPs, but this has stopped due to funding constraints. He cannot require ‘Privacy impact assessments’ (PIAs) for new information systems. However, he has a potentially significant ‘watchdog’ function of making statements on the privacy implications of proposed legislation or technologies including where their implications go beyond the IPPs. The Commissioner’s office does make public submissions, usually to Parliamentary committees or in response to agency requests for submissions, and participates in many inter-Departmental committees. In doing so, his views do not usually have special status or weight compared with those in other submissions. He does not have any power to sit in judgment on government proposals or actions, unless they become the subject of a complaint under the Act.

The essence of this Act is that enforcement of the IPPs is largely complaint-driven, as is the case with all Australian data protection legislation. The Act requires individual complaints of IPP breaches before enforcement action can take place. Enforcement of the Act is largely reactive: there are few if any means by which pro-active action is taken by the Commissioner to ensure it is observed.

Of over 1000 complaints investigated per year, about 17% relate to the public sector (OPC, 2004). Wide powers to investigate individual complaints, are rarely, if ever, used.
Complainants are first required to attempt to resolve the complaint with the data controller. Most complaints are handled by mediation. The Commissioner has powers to make ‘determinations’ awarding compensatory damages or requiring apologies or remedial acts, if mediation fails, but has only done so four times against public sector bodies in 19 years. Almost all complaints are settled by mediation or otherwise disposed of. This does not indicate that most complainants are satisfied with the Commissioner’s mediations, because he dismisses complaints where he is satisfied that a business or agency has dealt satisfactorily with a complaint, irrespective of what the complainant thinks.

The system is biased against complainants in other ways. There is no right of appeal to a Court against the Commissioner’s determination. However, if a determination is unfavourable to a data controller, it can in effect appeal to the Court because a complainant must go to Court to enforce the determination. The data controller can simply refuse to pay or comply and then have the whole matter heard again by the Court (Greenleaf, 2001). The only appeal right complainants have is against the amount of any compensation ordered against a public sector body by a determination. The Commissioner has never ordered compensatory damages except by consent of the data controller.

Mr Rummery was a whistleblower whose personal information had been improperly disclosed by his employer to corruption investigators. The Commissioner considered that, while the agency was entitled to disclose relevant personal information about him to the investigator, this did not give them ‘open season’ and they had gone too far. But he then refused to award any compensation for the distress that had resulted. In the only case where a complainant has appealed against the Commissioner’s refusal to award compensation, Rummery was awarded A$8,000 compensation (Rummery Case, 2004). Complainants with his tenacity are rare.

Of the approximately 200 public sector complaints in 2003-04, investigations found a possible breach of the IPPs in 38% (75). Over half the complaints were about agencies disclosing personal information, and the rest were about data security, failure to check accuracy, and collection practices. One indicator of successful operation of a complaints-based system is that it can demonstrate that individual complainants get the remedies that the legislation provides in theory. What happened in the 38% of cases investigated where breaches were found? Unfortunately, the OPC did not publish any systematic information about remedies granted, although recently this has improved a little, so we can only generalise from the few complaint summaries that are published. Since 2003, the Commissioner has published an annual average of 15 brief anonymised summaries of significant complaints which have been resolved without a determination, as well as the few determinations. Of the 19 complaint summaries published in 2004, only three related to agencies. Two of these were simply illustrative examples of where the Commissioner declined to investigate. In the one remaining case the agency's employee did disclose to the complainant's ex-partner that the complainant was to receive money from a court settlement, allowing the ex-partner to obtain a court order restraining the complainant from accessing that money. Because the complainant wished to pursue other action against the agency in the courts, the Commissioner ceased investigation.
is a typical year: there is no substantial evidence that the Commissioner enforces the Act against Commonwealth agencies in any way that produces remedies for complainants. This non-reporting makes the office less accountable, and squanders the potential deterrent effect of the Act. Other Asia-Pacific Privacy Commissioners are also opaque in their enforcement practices (Greenleaf 2003), though perhaps not to this extent.

There are some innovative enforcement aspects of the Act, but they have been little used. First, the Commissioner can conduct ‘own motion investigations’, which do not require an individual complainant, but any recommendations made are not enforceable by determinations. Although 42 such matters brought to her attention by media reports or other sources were investigated in 2004-05, few details of these investigations or their outcomes were published. Their potential as an avenue for public critique of system failures is lost. Second, individuals can seek a court injunction against breaches of the data protection principles, or threatened breaches (s98), but otherwise cannot enforce their rights in the Courts. 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, in part because of the risk of substantial legal costs being awarded against an unsuccessful litigant. The Commissioner can also seek injunctions from a court but has never done so. Third, NGOs, lawyers and other are allowed to make representative complaints on behalf of a class of complainants, and these can result in enforceable determinations (including damages) in favour of all members of the class. In the only published instance of this occurring, a consumer NGO represented the class of complainants against a private company (TICA determinations, 2005a, discussed later).

**Are the State and Territory public sector laws any better?**

The experience of New South Wales, the largest State, shows that many factors can make privacy protection precarious, from exemptions to politics to costs orders.

NSW was the first State to legislate for enforceable privacy rights in a State public sector (*Privacy and Personal Information Protection Act 1998*). The Act contains reasonably strong IPPs and sufficient remedies including compensation up to A$40,000. The problem with the Act is that it is riddled with exemptions and exceptions for particular agencies and practices, and contains provisions which allow Ministers or the Commissioner to create further exceptions with very little control on whether they are consistent with the purposes of the legislation (Greenleaf, 1999). The NSW Privacy Commissioner was highly critical of this in a submission on a review of the Act (Johnston, 2005, 2005a):

‘The ease with which the privacy protection afforded by Parliament in the PPIP Act may be overridden by the government of the day through subordinate legislation and other statutory instruments has ensured that the level of privacy protection is a moveable feast, but only moving in one direction – away from the highest standards of privacy protection.’

The holes in the Act are so complex that the Privacy NSW website contains details of the “matrix of exemptions” in the Act. Its effect is as much to legitimate surveillance and mollify public fears as to protect privacy.
Australian Privacy Commissioners have rarely come into direct conflict with governments. The first NSW Commissioner, Chris Puplick, was the exception, becoming involved in public dispute with a government Minister. He resigned in 2003 after strong criticism by the NSW Premier. The Government then unsuccessfully attempted to abolish the office of Privacy Commissioner (Greenleaf and Waters, 2003). It then reduced the staff of Privacy NSW by one third and refused to appoint a new Commissioner for nearly five years, effectively removing the office from public debate until 2008. The fragile independence of Australian privacy Commissioners was never more apparent.

Despite this the Act continued to work to some extent because complainants have an alternative route to dispute resolution. They may seek internal review of their complaint by the agency concerned, and then appeal to the Administrative Decisions Tribunal if necessary. An average of three privacy cases per month continue to be decided by the Tribunal since 2003. However, in recent cases the Tribunal’s appeals division has started to require complainants to pay the costs of the agency in appeals where the complainant loses, even when the appeal has been brought by an agency. This may have a ‘chilling effect’ on complainants because of the uncontrollable risks of costs (Waters and Paramaguru, 2007).

In 2000 Victoria enacted Australia’s strongest public sector privacy legislation, the Information Privacy Act 2000 (Greenleaf 2000b). The first Privacy Commissioner, Paul Chadwick, was a former journalist with a reputation for independence. The Act’s principles are based on those in the private sector Act. It provides for an extensive range of remedies including compensatory damages, with mediation by the Commissioner followed by the right of complainants to seek enforceable remedies from the Victorian Civil and Administrative Tribunal (VCAT). Although the complaints functions have only been operative since 2004 substantial compensation does result. For example a A$25,000 settlement resulted when a government agency disclosed a woman’s new address to her estranged partner despite the agency’s file noting that she was ‘at risk’. Her premises were broken into and vandalised the same day, and she was forced to relocate.

Other than in these two States, data protection in Australia’s public sector is slow to develop, incomplete, and inconsistent. There has never been a push for national uniformity, although all State and Territory jurisdictions do provide access and correction rights to personal information held in government documents, as part of their Freedom of Information legislation. The Northern Territory has enforceable IPPs based on the private sector Act, and a Commissioner (Information Act 2002). The Australian Capital Territory (ACT) applies the federal legislation to its public sector. Tasmania’s ant-diluvian legislation includes IPPs but no means of enforcement beyond investigation and mediation by the Ombudsman (Personal Information Protection Act 2004). Western Australian has introduced a Bill which is similar to the Victorian Act but allows the State’s Ombudsman to be appointed as Privacy Commissioner (Information Privacy Bill 2007). South Australia and Queensland have non-legislative, non-enforceable and insignificant administrative instructions similar to IPPs applying to their public sectors.

Comparison of the enforcement of the federal, NSW and Victorian legislation suggests that effective privacy law enforcement in Australia might be better delivered by a quasi-
judicial tribunal such as in NSW and Victoria, rather than by a Privacy Commissioner, although introduction of a right of appeal against the Commissioner’s decisions might substantially change the federal system.

Australia’s privacy laws have not forced significant information systems to be shut down or redesigned, at least to public knowledge. Yet they do give either Privacy Commissioners or administrative tribunals enforcement powers in individual complaints, including powers to award damages, that are unusual in many other countries. In a common law country where privacy protection is not founded on broad principles but on technical legislation, individual cases are potentially very significant. Their cumulative effect as a deterrent to privacy invasion could be very substantial. However, this potential has largely been squandered in Australia. There are too many impediments to complainants pursuing their rights in some jurisdictions. Privacy Commissioners have also failed to publish sufficient information to create a realisation of the potential of Australia’s privacy laws.

The rocky road to private sector legislation

Why did it take 17 years from when Australia acceded to the OECD Guidelines in 1984, until the federal Privacy Act 1988 was extended to apply to the whole of Australia’s private sector in 2001 (Privacy Amendment (Private Sector) Act 2000)?

By the early 1990s there was some piecemeal private sector coverage, as already discussed: the NSW Privacy Committee had ‘ombudsman’ powers to investigate complaints against businesses in NSW; use of tax file numbers by businesses was regulated; and credit reporting was strictly regulated. Pressure grew through the first half of the 1990s for further private sector protections, influenced in part by increasing electronic privacy issues, and in part by the imminent EU privacy Directive. In 1996 Liberal Prime Minister John Howard scrapped proposals by his Attorney-General for private sector privacy legislation (A-G Discussion paper, 1996), in favour of voluntary self-regulation, due to pressure from some sections of the business community and a general antipathy to regulation. He requested the States and Territories to follow suit, but Victoria continued to plan legislation. Privacy and consumer groups continued to campaign for legislation (Greenleaf, 1997).

The Privacy Commissioner proposed a single national self-regulatory privacy code (OPC, 1997). Consumer and privacy groups boycotted any discussions of voluntary self-regulation, but agreed to discuss the content of privacy principles. The Commissioner convened discussions between business and consumer representatives and then published the set of ‘National Privacy Principles’ (NPPs) she favoured (OFPC, 1998). They were criticised by privacy advocates (Greenleaf 1998) as representing neither a high standard nor a consensus, but business groups were not overtly critical. Three years later, these NPPs, essentially unchanged, became the core of the private sector legislation. They were not designed for that purpose, and were never debated in Parliament, illustrating how accidents of history can shape law.

Privacy and consumer advocates continued to boycott discussion of voluntary methods of enforcement of the NPPs, and business groups lost interest in turning them into Codes
of Practice. Meanwhile, perceptions that the European Union’s privacy Directive, in force since 1998, could lead to data export restrictions between Europe and Australia continued to mount. Whether self-regulation could satisfy these requirements was contentious. Privacy advocates found a ready appetite in media organizations for stories on these lines. The Victoria Labor government offered to drop its proposed private sector coverage if the federal Government acted instead (Greenleaf, 1999b).

In January 1999 the Federal Government abandoned its self-regulatory approach in favour of so-called ‘light-touch’ legislation including provision for co-regulation via industry codes of conduct. It admitted this was because key industry groups had changed their mind and now wanted legislation to achieve national consistency and certainty. The resulting legislation (Privacy Amendment (Private Sector) Bill 2000) was strengthened somewhat during the political process, but too little to satisfy the Bill’s critics who claimed it would not deliver meaningful privacy protection (Greenleaf 2000, 2000a). The self-regulation road of 1997-99 had been turned into a dead end. The causes were complex, but it probably would not have occurred without a decade-long campaign by privacy groups, or without the belief that there were trade imperatives because of the EU Directive.

What rights did the ‘private sector amendments’ create? In most respects the NPPs are similar to the public sector IPPs that preceded them, but they included innovations that stemmed from the business-advocate discussions convened by the Privacy Commissioner. These included the ‘anonymity principle’, the principle limiting re-use of identifiers, the deletion principle, and the limits on data exports, all previously discussed. These additional principles have subsequently been taken up in most post-2001 State and Territory public sector laws.

Is the private sector legislation effective?

About 80% of all complaints to the Commissioner are against the private sector (OPC, 2005: Annual Report 2004-05). The private sector provisions of the federal Act are enforced in much the same way as the public sector provisions, discussed earlier.

Tenants Unions made a representative complaint on behalf of their members against TICA, a database about tenants consulted by real estate agents (TICA determinations, 2005). They persuaded an initially reluctant Commissioner to make determinations that TICA had breached the NPPs in numerous ways, including by charging tenants merely to make a request to access their tenancy record; by charging excessive amount for access; by failing to ensure data quality standards; by having excessively general reporting categories; by failing to advise tenants when they were listed; and by failing to destroy or de-identify information no longer needed. TICA was required to make systemic changes to its practices, to the benefit of many thousands of tenants.

In the six years the private sector provisions have operated, this is the only enforceable order (determination) made against a private sector body. There are also occasional significant mediated disputes, notably when the Commissioner convinced Veda Advantage to delete 65,000 debts listed by a telecommunications company in liquidation, since it could no longer prove their validity. What happens to the rest of the thousand or
so complaints received annually against the private sector? About 60% are closed without investigation. In only about 5% of cases does the Commissioner reach even a provisional view that there might be a breach of NPP, but subsequently ceases investigation after concluding that the respondent has dealt adequately with it, possibly after conciliation. No details of the outcomes of these conciliations were provided except that the resolutions include ‘provision of access to records, correction of records, apologies, change to systems, [and] amounts of compensation ranging from less than $500 to $20,000’ (OPC Annual Report 2004-05). Of the 22 complaint summaries published by the Commissioner in 2004-05 (OPC complaints 2004-05), none involved any financial compensation, let alone such a significant sum as $20,000. They are mainly variations on how complaints are dismissed, and none involve significant systemic changes. This is a substantial failure of accountability.

The federal Privacy Commissioner states that most business organisations consider that “the overall level of compliance is good and the Office’s approach is working well”, but notes that in contrast, “the perceived lack of enforcement mechanisms in the Privacy Act especially in relation to determination enforcement is a matter of strong concern amongst the advocacy and consumer groups” (OPC Review, 2005). This is an unduly self-satisfied conclusion. The Commissioner’s own Review (2005, Appendix 14) summarises the results of a survey of satisfaction levels of 100 complainants and 41 respondents. On every criterion of satisfaction measured (timeliness, impartiality, process information, communication of reasons, satisfaction with service and satisfaction with outcomes) complainants were far less satisfied than respondents. In some cases, the disparities in satisfaction were large: only 43% of complainants were satisfied with outcomes, but 86% of respondents were satisfied. In addition, 41% of complainants considered the service poor, and 56% did not think they had been dealt with fairly. Unless the dissatisfaction of complainants is quite unjustified, these results suggest that the complaints process itself may be demonstrating to respondents that they have little to fear from the Privacy Commissioner. The Commissioner’s failure to publish sufficient details of complaint outcomes reinforces such a belief.

The emphasis in this and preceding sections on complaint outcomes, compensation and reported complaints is perhaps typical of the empirical and inductive common law approach. It reflects an approach to privacy protection based on the technical minutiae of positive law. However, that is the only approach possible in the absence of any theoretical underpinnings of principle, such as Germany’s ‘informational self determination’ doctrine, strongly upheld in that country’s courts, yet conspicuously lacking any equivalent in Australian law.

II Role of public opinion

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

Public and organisational attitudes to privacy protection
Public concern in Australia for privacy and data protection interests is generally high, at least in the abstract, according to survey data. There would also appear to be widespread public support in Australia for legal safeguards of these interests (Morgan, 2004 referring also to 1995 and 2001 surveys). However, community knowledge of existing safeguards appears to be poor. Although knowledge that federal privacy laws exist has risen to 60% of respondents, only 34% were aware that the federal Privacy Commissioner existed (Morgan 2004).

Australian organisations in both the public sector (Morgan 2001) and private sectors (Morgan 2001a) seem generally to regard public concern about privacy issues as legitimate and as an important factor to take into account when dealing with information about their customers and clients. They seem to be generally supportive of existing privacy laws, though there are some gaps in knowledge of how these laws work, particularly with respect to the business community.

**Elite involvement in privacy issues**

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, 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 in comparison with the policy-makers of Washington or Whitehall.

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. Some general civil liberties organizations also do also. Of these, Electronic Frontiers Australia (EFA) has been the most prominent (EFA, 2005), providing continuous detailed input into privacy debates and lobbying.

Since 1987 the Australian Privacy Foundation (APF, 2007), formed to oppose the Australia Card, together with its members wearing other hats, have been the most consistent and effective privacy advocates in Australia, though still rarely gaining the policy changes they seek. ‘Ex officials’ including two former deputy Privacy Commissioners have been key APF board members or Chairs since its inception. The APF’s key achievements since the defeat of the Australia Card include leading the opposition to ‘positive reporting’ which resulted in the credit reporting legislation (1990), leading the boycott against self-regulation discussions (1997), and its role in opposing the ‘Access Card’ (2007). The APF also influenced the content of the NPPs (1998), obtained Opposition support for successful improvements to the federal private sector legislation (2000), obtained upper house support to stop the NSW government abolishing its Privacy Commissioner in 2004, and derailed federal plans to convert the census into an identified longitudinal database in 2005 (APF, 2005). The Australian Privacy Charter launched in 1993 is a restatement of privacy principles in a stronger and simpler form than the Privacy Act’s IPPs. It was developed outside the APF but led and drafted by APF.
participants. It had a strong influence on the NPPs, and was subsequently adopted by the APF as its ‘policy constitution’.

The APF also launched the Australian Big Brother Awards (the ‘Orwells’) in 2003, influenced by Privacy International. Winners of the premier ‘Lifetime Menace Award’ for long records of profound disregard for privacy have included a Federal Attorney-General for sponsoring anti-privacy legislation, and the NSW Government for its failure to appoint a new Privacy Commissioner. This irreverent approach to public officials sits well in the Australian psyche, and has obtained good media coverage.

Organisations of professionals have not had a continuing input into the development of privacy laws, with the exception of the Australian Computer Society (ACS), the largest organisation of computing professionals. Since the early 1970s ACS has consistently supported the development and strengthening of information privacy laws. In part this can be explained by an overlap of key activists with the APF, but nevertheless the whole professional body has been willing to appear in the pro-privacy camp.

Business groups are almost always better resourced than NGOs, and key groups have much more ready access to Ministers than do NGOs. The Melbourne-based employer group, ACCI, was particularly influential in getting the federal Liberal government to first oppose private sector legislation and then, two years later, to adopt it in a ‘light handed’ version. 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.

A small group of key business representatives, and a core group of privacy advocates have remained relatively stable for at least fifteen years, while government representatives have changed far more regularly. This has often facilitated effective communication of positions, with compromises on either side, particularly in relation to legislative developments. For example, in the 2005 review of the Privacy Act, businesses and privacy advocates were able to agree that requiring opt-out notices in all direct marketing communications was a sensible change to existing law, though it did not represent the ideal position of either side (OPC review, 2005).

**Public opinion’s influence on privacy developments**

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 (the tax file numbers and ‘parallel matching’,
the extensions of financial surveillance, the spread of CCTV etc) and largely unopposed because the cumulative impact is not apparent.

III Local culture and traditions vs international influences

National culture and traditions

Australia’s self identification as ‘The Lucky Country’ (Horne, 1966) is apposite in relation to privacy. There has been no wartime occupation or an authoritarian regime from which to recover and no terrorist actions as yet within the country to prompt (or justify) major changes in mass surveillance. Australian privacy protection has therefore as yet only needed a story of incremental wins balanced against losses, not a cultural revolution. It is a complex balance sheet, with much scope for disagreement about what type of balance has been reached.

Our legal culture’s British inheritance has not served us well in creating foundations for privacy protection. From Britain Australia inherited no common law right of privacy, and no constitutional bill of rights as a basis for privacy protection, and nor does it have major treaty obligations. Whereas Britain has now imported the last two from the Continent, Australia languishes with neither and lacks any underlying principle such as ‘informational self-determination’ on which privacy protection can be anchored. If the immediate future is one of increasing encroachments on privacy and other civil liberties, where justifications are framed in terms of increasing risks from terrorism, Australia’s national culture and legal traditions have few tools with which to resist and shape such encroachments.

International privacy developments and their influence

Despite Australians’ minimal obligations under international privacy agreements (discussed earlier), 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.

The OECD privacy Guidelines (1981) were adopted by Australia in 1984. An Australian, Justice Michael Kirby, chaired the expert group that drafted them. 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 IPPs in the ALRC privacy Report (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.
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 are very critical of the Australian legislation (Article 29 Committee, 2001), resulting in claims of unfairness and willful misunderstanding by Australia’s federal government (as exemplified by Ford, 2002). The EU commenced its formal assessment of the ‘adequacy’ of Australia’s privacy laws in 2005 and (depending on the outcome) this may further increase hostility between Australia and Europe over data protection issues.

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). 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 (Greenleaf, 2005). The APEC Framework was only completed in mid-2005) in relation to data export restrictions. Although the Australian government has expressed antipathy to judgments of its privacy laws by any other country (see Ford 2002), APEC did not 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 little chance that APEC will develop into an anti-EU bloc (Greenleaf, 2005a).

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.

IV Winners and losers

The broad trajectory of the development of privacy protection in Australia is one of steadily increasing surveillance, but the picture is not uniformly negative. Often these losses to privacy are accompanied by small gains in individual privacy rights and ability to exercise them. Increased surveillance and increased legislative protection have often occurred in tandem, as legislative ‘packages’. It may well be that Australians are accepting more surveillance as part of the price of an information-based economy and to achieve an acceptable level of social control, but this is still accompanied by demands for mechanisms to control abuses. ‘One step forward, two steps back’ is the general trajectory.

Court decisions and complaints to Commissioners have played very little significant role in bringing about systemic changes to practices. Privacy Commissioners have delivered
some justice to individual complainants. But even there their record has been very limited and their general failure to use their complaints experience as a method of deterrence and public education makes it questionable whether the expenditure of public monies has been worthwhile.

Australian privacy legislation leaves many consumers and citizens as major losers in many of their most important life roles. Unprincipled exemptions from the federal *Privacy Act* are a major cause: as voters, political parties owe them no privacy; as employees, they are left to fragments of protection in industrial laws and varying State laws; as customers of the majority of businesses in the country (so called ‘small’ businesses) they have no privacy rights unless the business trades in personal information.

The negative privacy protections of inefficiency mean that Australians are still winners in not having a national ID card. ‘Like the Australia Card’ is still the kiss of death to any identification proposal in Australia, and is flatly asserted and denied by those on either side of an issue, usually with little grasp of what the Australia Card proposal involved.

**Information flows and constraints**

The main gains in privacy protection in Australia stem from the simple fact that legislation exists. Both government agencies and private sector bodies are generally law abiding even in the absence of any effective sanctions or credible threat of sanctions, at least if the compliance costs are not too high. The potential for embarrassing media publicity is probably more potent than the featherweight sanctions employed by Privacy Commissioners.

In the private sector, observance of the law still keeps personal information by and large segregated into databases which reflect different industry sectors, and all consumers are winners in that. There have also not been radical changes in relation to private sector access to data from public sector registers. Data aggregators seek to break down both these barriers, but for the moment have not succeeded. In 2007, industry efforts recommenced to remove the restraints found in the credit reporting and private sector legislation.

The flows of personal information from the private sector to the public sectors have expanded to a massive extent over the past fifteen years, thanks to the various data matching schemes, and to the financial surveillance requirements. However, within the public sector, and from the private sector to the public sector, recent developments threaten to tear down barriers to information use and merger. All Australians in their capacity as citizens are in danger of losing their privacy. That must be the focus of an assessment of future prospects.

**V Prospects for the future**

The future of privacy always looks dangerous because there are always proposals on the horizon, or new systems in place, which look as though they pose great dangers of abuse.
In hindsight we see that most proposals fail – with excessive privacy dangers sometimes a cause – and that many new systems are implemented more cautiously than we feared.

**The political ascendancy of surveillance post-2001**

By 2007 the future for privacy in Australia looked more bleak than it had at any time since the Australia Card seemed a *fait accompli* almost two decades earlier. The prospect of a never-ending ‘war on terror’ has made everyone’s privacy a hostage to agendas which have little to do with genuine attempts to defeat terrorism, but which find it a convenient cover. There are many post-2001 developments in Australia which fall within this category. The ease with which such legislation could be passed in Australia is partly explained by the fact that although terrorist attacks have not yet occurred within Australia, there have been significant terrorist attacks on Australians in Bali, Indonesia in 2002 and 2005. The Labor federal Opposition during those years, and the Labor governments of most States and Territories, were cowed by the perceived danger of being labeled ‘soft on terror’, and even promised to pass proposed legislation before they saw the details. Repeatedly the federal Liberal Party Government refused to release contentious legislation in bill form so as to enable informed public debate and used its majorities to rush it through both houses of Parliament.

The ease of passage of invasive legislation was caused by a drastic change in the political situation described in the opening of this paper, whereby the protection of privacy in Australia has always depended on limitations on political power in Australia. In particular, governments in Australia have rarely controlled the upper house of Parliament, and have therefore been forced to make political compromises to pass legislation. In July 2005 the Howard Liberal Party government obtained a slim majority in the federal Senate. They then relentlessly pursued a radical agenda of political change in industrial law, education, social security and, not least, national security and surveillance. The political balance that formerly protected privacy was lost.

Telecommunications interception legislation was amended in 2004 to eliminate the requirement of judicial warrants for access to stored communications such as email, SMS and voice mail. This followed earlier amendments allowing security agencies to plant surveillance devices in computers and take other actions which would otherwise breach computer crime legislation.

New passports legislation in 2005 allows the Department of Foreign Affairs and Trade to develop an electronic passport, featuring a facial biometric and possibly other biometrics. The justification offered was mainly the demands of the USA for such passports if countries wished to retain visa-free status for their nationals.

New anti-terrorism laws contain provisions which are not confined to terrorism offences but are part of longstanding government wishes to give agencies extra powers, including federal police powers to give notice to produce information for ‘other serious offences’, extensions of optical surveillance, changes to the *Financial Transaction Reports Act* (discussed below), and extended powers of Customs officers (*Anti-Terrorism Act (No 2) 2005*; see APF, 2005a).
Anti-money-laundering and counter-terrorism financing laws now require 63 categories of businesses to identify and monitor transactions and activities of their customers, extending to transactions as minor as phone or public transport smart cards. Critics argued that “At least under the current scheme, most reporting is by supposedly well trained bank employees, but in future thousands more people, from casual jewellery store clerks to junior real estate managers, will be legally required to pass on judgments about their customers, that could bring innocent individuals under official suspicion” (Anti Money-laundering and Counter-Terrorism Financing Act 2006; see APF 2005b). The APF identifies the AUSTRAC system as the central new surveillance system emerging in Australia which straddles the public and private sectors (APF 2005c):

“[The] existing FTRA/AUSTRAC regime … has offended against privacy principles since its inception, and has progressively developed into a wholly disproportionate surveillance system, part of which involves secret files which can have the potential to blight innocent people’s lives without any knowledge or recourse. The history of the FTRA … has been a classic example of ‘function creep’, with the original justification of fighting serious and organised crime having long since given way to routine use by agencies for other purposes, culminating last year in the granting of access to” [social security and child support agencies].

In addition to developments under the anti-terrorism cloak, there are many public sector developments which involve an unprecedented degree of surveillance for Australia, including in the areas of health and transport systems. However, the development of a national identification system under the guise of a ‘Health and Welfare Access Card’ posed the greatest long-term threat to privacy interests.

‘The Access Card’ ID system – another near miss

Liberal Party Prime Minister John Howard put the issue of an ID card back on Australia’s political agenda in the wake of the London bombings of July 2005, but it temporarily disappeared when it became clear that ID cards were not seen as related to this issue in the UK. It reappeared in April 2006 with the announcement that his government had rejected the idea of an ID card, but would introduce a ‘Health and Welfare Access Card’ instead, intended to replace up to 17 government benefit cards and to reduce fraud against the social security and medicare systems. It was proposed as a multi-function smart card, on part of which individuals would be able to store their own medical and other information. It was claimed that, while individuals would be free to use the card for any purpose they chose, no one outside the welfare and health benefits system would be able to demand its production.

Critics argued that the proposal was indistinguishable, other than for its greater technical sophistication, from the Australia Card proposals of twenty years earlier (Greenleaf 2007, 2007a, 2007b). The essential components of the proposal were a Register to contain photographs, signatures, location information and an ID number for each adult, and links to benefit agency systems; and a chip-based card which would contain the photo, signature, and ID number on both card and chip, plus a separate
number to act as a debit card linked to the financial system through ATMs. The proposed legislation would have allowed expansion of the content of both register and chip with little legislative control; access to the Register by Police and security agencies; and a system of ‘infringement notices’ when the card was improperly demanded. Supporters and critics disputed what was needed to reduce social security fraud, whether ‘function creep’ was inevitable (or even intended), and whether ‘pseudo-voluntary’ production of the card would see it develop into a near-universal ID system.

The Australian Privacy Foundation and civil liberties organisations opposed the proposals to little apparent effect until a Parliamentary upper house Committee with a government majority began what were expected to be routine hearings on the Bill after its passage through the lower house. The Committee agreed with critics that the Bill was unacceptable because it did not contain the whole legislation (it was proposed there would be a later second Bill). However, its report made clear that it was dissatisfied with many substantive aspects. The government withdrew the Bill within 24 hours. Three months later it released a ‘consultation draft’ of a completed replacement Bill (Greenleaf 2008).

The Howard government did not reintroduce the Bill into Parliament before Australia’s federal election in November 2007, partly because of the political risk involved in introducing ID card legislation once an election was imminent. This was the result that the extra-Parliamentary opposition had aimed to achieve. In the week before the election, the Labor Party Opposition finally announced its clear rejection of the Access Card. The Rudd Labor government was elected on November 24 and within a week it had formally announced the scheme was scrapped, had disbanded its administration, and told all contractors to stop work (Greenleaf, 2007b). Exactly twenty years after the defeat of the Australia Card, the political process had again rejected a national ID card scheme.

Despite the Howard government’s apparently dominant political position from 2005 to 2007 and the expenditure of millions of dollars on technical studies and consultants, it was unable to push this legislation through in the face of determined extra-parliamentary opposition and public skepticism. The scrapping of the Access Card is testimony to the enduring effect of politics in Australian privacy developments.

Back to ‘muddling through’?

It would be reassuring to be able to conclude that privacy in Australia will again ‘muddle through’ as a complex balance sheet of incremental gains and losses, a continuation of its past history. In Australia privacy is politics, because the constitutional and other institutional protections of privacy are so weak. The lack of a history of overturning authoritarian regimes may also make it more difficult for Australia to resist incremental encroachments on privacy. At the end of 2007 the political pendulum has again swung, and democracy has delivered a pro-privacy result. But it is too early to conclude that Australia has a government actively supporting privacy, and that is not expected.

It is more likely that Australia will be back to the usual situation of governments frustrated in pursuing their ambitions of surveillance (in order to achieve their other goals) because of oppositions opportunistically advocating privacy in order to create
political damage to their opponents. The new federal government does not have a majority in the upper house, and it is quite uncertain whether it will ever obtain one, so there are better prospects than in recent years for the extra-parliamentary supporters of privacy to impede surveillance by obtaining support from the opposition parties. However, there is no reason to expect that the recent losses to privacy outlined above will ever be rolled back: both sides of politics seem committed to expanding the surveillance capabilities of the state. Perhaps this government will be more reluctant to use ‘national security’ to continually erode privacy, but there is no guarantee of that, as it complied with most of the previous government’s wishes on that. The post-2001 trajectory of support for increased surveillance has had substantial support from both major parties, and at both levels of government. Privacy has few friends except opportunism.

To conclude on an optimistic note, by mid-2008 the Australian Law Reform Commission (ALRC) will complete the first major review of federal privacy law in twenty years, and the New South Wales Law Reform Commission will do likewise for that State’s legislation. The ALRC has indicated its intention to recommend major changes to the federal Privacy Act, strengthening its principles, unifying them between the public and private sectors, and removing many of the procedural defects such as the lack of rights of appeal (ALRC, 2007, Greenleaf 2007c). If these reforms are adopted by the Rudd government and its state counterparts, then information privacy protection will be strengthened, to complement the near certainty of accompanying extensions of surveillance. Whether they will be strengthened enough for a Web 2.0 society and a post-2001 state is a story for the future.
References – Australia


APF (2005a) - Australian Privacy Foundation Submission on the Anti-Terrorism Bill (No 2) 2005 to the Inquiry by the Senate Legal & Constitutional Committee, November 2005 at <http://www.privacy.org.au>

APF (2005b) – Australian Privacy Foundation letter to all Australian Privacy Commissioners, 19 Dec 2005 at <http://www.privacy.org.au>


Chulov and Hodge (2005) - Martin Chulov and Amanda Hodge 'All eyes are on you' *The Australian*, 26 July 2005


‘Four Corners’(2005) – *Four Corners* (Australian Broadcasting Corporation television programme), transcript of segment ‘Your money and your life’, 15/08/05


Greenleaf (2000a) – Greenleaf, G ‘Reps Committee protects the "privacy-free zone"' *Privacy Law & Policy Reporter* Vol 7 No 1, 2000, pg 16


