THE PRIVACY ACT: REFLECTIONS ON FEDERAL LAW AND ITS RELEVANCE TO STATE ADMINISTRATION

*Kevin O'Connor**

Presented to the Victorian chapter of the AIAL, Melbourne, 28 July 1992 and first published in AIAL Newsletter No 11 1992.

I am pleased to have the opportunity today to address the Victorian chapter of the Australian Institute of Administrative Law on the Federal Privacy Act and its possible relevance for adoption by State governments.

The *Privacy Act 1988* came into operation on 1 January 1989 and at that time had two spheres of operation. Those spheres related to, one, all personal information handling activities of almost all Commonwealth government departments and agencies; and, two, the use of a particular category of information - the tax file number and information linked to that number - within the whole Australian community. Since that time, the Privacy Commissioner has been given responsibility for ensuring the effective operation of Commonwealth law limiting the use and disclosure of old conviction information (the relevant provisions being contained in Part VIIC of the *Crimes Act 1914*) and, more significantly, responsibility for implementing a complex array of new requirements in relation to the handling of credit reporting and other credit history information affecting consumers, contained in Part IIIA of the Privacy Act.

Part IIIA of the Privacy Act became fully operational on 25 February 1992. Two aspects of the Privacy Commissioner's brief in relation to Commonwealth administration have since been the subject of detailed statutory provisions: data-matching using the tax file number by the Department of Social Security (the *Data-Matching Program (Assessment and Tax) Act 1990*) and the operation of the Pharmaceutical Benefits and Medicare Schemes (s135AA of the *National Health Act 1953* and related amendments).

I have recorded the work of my office in my annual reports to the Attorney-General, which are tabled in Parliament. The first annual report covers the first six months of operation of the office to 30 June 1989. The second and third annual reports cover the years 89/90 and 90/91 respectively. At the moment, I am preparing my fourth annual report, dealing with the period 91/92. I mention these reports as they probably provide the most comprehensive view of the work of the office and would, I feel, be instructive to any governments contemplating adoption of Privacy Act standards in their own jurisdictions.

Influences leading to Privacy Act

The Privacy Act was the product of two policy influences at work in Federal administration during the 1980s. The first influence was the work of the Australian Law Reform Commission (ALRC) and, in particular, its then Chairman, Justice Michael Kirby. In 1983, the ALRC handed down its report entitled *Privacy*, comprising two large volumes, being the product of almost seven years of work, following a reference given to it in the early days of the Fraser Government by

* *Kevin O'Connor is the Commonwealth Privacy Commissioner.*

(then) Attorney-General Ellicott. During the period of that reference, Justice Kirby was involved in the work of the Organisation for Economic Co-operation and Development (OECD) in seeking to develop international guidelines on the protection of the privacy of personal data. The OECD work culminated in 1980, with the adoption by the OECD of guidelines on the protection of the privacy of personal information and the regulation of transborder data flows.

The ALRC report of 1983 dealt with the two major strands of privacy concern: one, electronic and physical intrusions into privacy, usually by means of surveillance devices; and, two, the privacy issues raised by modern practices and developments in relation to the collection, use and dissemination of personal data. The ALRC's recommendations in relation to the second matter involved the suggestion that there be enacted a Federal Privacy Act which laid down a series of information privacy principles regulating the collection, storage, use and dissemination of personal information. The ALRC information privacy principles were influenced by, to some extent, the language of the OECD guidelines. But, in many respects, the ALRC's information privacy principles were more specific than the OECD guidelines. The administrative model recommended for implementation of the information privacy principles was to give responsibility to an office of Privacy Commissioner attached to the Human Rights Commission. The Privacy Commissioner would essentially have an Ombudsman-like role, with a power to examine issues of concern, make proposals as to policy and give advice to the areas affected by the legislation. But there would be no formal sanctions in respect of any alleged contraventions of the information privacy principles. The ALRC model envisaged that the information privacy principles would apply to the public sector and generally within the Territories.

The other major influence on the development of the Privacy Act was, of course, the proposals which emanated from the high-profile economic summit of 1986. At the summit, Mr Eric Risstrom of the Australian Taxpayers' Association had floated the idea that there be a universal identity number and card system developed by the Government to assist in the administration of various government functions. That idea was later picked up by the Government and formed the basis of the development of the Australia Card policy. As you will recall, considerable controversy surrounded that proposal. One of the elements of the Australia Card package was that there be a Privacy Bill introduced, to apply safeguards in relation to the handling of personal information in Commonwealth administration. Responsibility for ensuring that the Australia Card system operated within the boundaries set by the law and that information generally in Commonwealth administration was adequately protected by privacy safeguards was given by the Australia Card Bill to a Data Protection Agency, working in conjunction with a Data Protection Advisory Committee.

The proposal for an Australia Card was eventually dropped in 1987 and agreement reached between the Government and the Coalition to proceed with an upgraded tax file number system to assist in the administration of the tax system. That agreement was subject to the condition that the Privacy Bill be proceeded with. A number of revisions were made to the contents of the previous Bill (the one introduced as part of the Australia Card package). Responsibility for oversight of the legislation which applied information privacy principles to Commonwealth administration was given to a retitled office of Privacy Commissioner, attached to the Human Rights and Equal Opportunity Commission.

The information privacy principles were made legally binding, with contravention entitling the Privacy Commissioner to issue a formal determination against a Commonwealth agency, which might include an order for damages. The 1988 Bill, subsequently enacted, did not give the Privacy Commissioner any formal jurisdiction over the general community, other than in the area of the tax file number system. Instead, the Privacy Commissioner was given a function to encourage corporations to adhere to the OECD guidelines and their information-handling practices. The preamble to the Privacy Act referred to international instruments as providing part of the basis for the Federal Parliament's intervention in this area - namely clause 8 of the International Covenant on Civil and Political Rights, which refers to the protection or privacy as a human right and, more significantly, the OECD guidelines of 1980, which have been adopted by Australia.

The Privacy Act as a code of administrative procedure

For administrative lawyers, the legislation is particularly interesting. What it does - and in this regard I suspect it is unique within the framework of Australian administrative law - is lay down a legally-binding code of procedure to apply to the everyday personal-information-handling activities of Commonwealth administration. I recall that the only unacted-upon element of the administrative law package put forward to Commonwealth administration by the Kerr Committee in the early 1970s was that which related to the enactment of a code of administrative procedure to apply in relation to Federal Government administrative decision making. It could be argued that, to some extent, the Privacy Act fills that gap. But the Privacy Act provisions do not depend for their application on there being an endpoint decision to which the process is directed, as would presumably be the case for an administrative procedure code to apply.

Information Privacy Principles

The Information Privacy Principles are set out in section 14 of the Privacy Act. As you will see, they lay down standards in relation to: the practices to be followed by agencies in collecting information either directly from the individuals concerned, or from third parties; the storage and security of that information; the notice to be given to the public of the existence of data systems; access and correction (where the principles reinforce the requirements of the *Freedom of Information Act 1982*); and the use of information and the disclosure of that information. The principles do not directly address issues to do with the retention and destruction of data, as these are left to the oversight of the Archives Office, under the *Archives Act 1983*.

Systematic activity

My office's work has focussed on systemic issues in the area of Commonwealth administration. This focus reflects the emphasis on these issues in my statement of functions (see ss27, 28 of the Privacy Act as to the Commonwealth sector) and is in line with the role envisaged for the office by the ALRC in its 1983 report (see especially items 4, 13, 62 and 88 of the Summary of Recommendations - Report No 22 (1983), vol 1).

Policy Development

This month, I am issuing data-matching guidelines for adoption on a voluntary basis by Commonwealth agencies. Earlier in the year, I issued covert surveillance guidelines for adoption on a similar basis. Both resulted from long and detailed consultation processes with agencies. In some areas, my guidelines have legally-binding status. These include those on tax file numbers and on the data-matching program at the Department of Social Security (DSS) involving the tax file number. I have also been given power to issue binding

guidelines affecting the operation of the pharmaceutical benefits and Medicare systems. I have declined to act on that brief to date due to technical difficulties with the enabling legislation. I reported formally to that effect to Parliament during May.

Formal investigations and reports

The development of guidelines has generally occurred outside the framework of any particular public controversy. But incidents which have given rise to public concern have on occasions provided the basis for my office making proposals for systemic improvements to agencies.

Examples are -

- The report issued in August 1990 relating to allegations first made in the *Age* newspaper in September 1989 of a 'trade' in passenger data as between various officials in Commonwealth administration and also with private detectives. While I found no evidence to support the main allegations, I did detect weaknesses in administrative procedures which could lead to improper disclosures occurring or improper access being obtained to the data. Various recommendations, accepted by those agencies, were made to the Department of Foreign Affairs, the Australian Customs Service and the Department of Immigration to better control the flow of microfiche copies of passenger movement data.

- During this year, I have issued reports on mail-out errors at DSS and the Australian Taxation Office, with a report pending in relation to the Department of Employment, Education and Training (DEET).

- Most recently, I issued a report on the release by the Australian Federal Police (AFP) of an arrest list of AIDEX demonstrators to DSS. Again I have recommended that there be a tightening of procedures, this time in the AFP and at DSS. That report is being examined by a working party.

Audit

Audit is the final way in which systemic observance of the Information Privacy Principles is sought to be achieved. I have several staff devoted full-time to visiting Commonwealth agencies and auditing their practices. Audits have been undertaken in relation to aspects of the operations of the Cash Transaction Reports Agency (CTRA), DSS, DEET and the Australian Customs Service. An account of this work will be included in the next annual report.

The audit program seeks to respond to the difficulty that individuals do not know or may not understand what happens to their data in the hands of administration. The audit program seeks to ensure that privacy principles are observed behind the fours walls of administration.

Individual complaints and inquiries

Complaints often only give a limited insight into the satisfactoriness or otherwise with which administration complies with privacy standards. Often complaints are one-off, concerned with isolated incidents or are relatively trivial. Some, of course, are more significant and have agency-wide importance.

It is not advisable for me to discuss publicly the details of complaints and inquiries made to my office, but the following statistics may give you an insight into the operation of my office in this area:

General inquiries

There were 16 600 general inquiries in the year 91/92, divided as follows: 2 266 involved 'complaints' about alleged breaches of privacy by a variety of bodies in the country, of which only a very small

number turned into formal statutory complaints; general information requests - 9 954, with the majority of these in the credit reporting area; 3 634 requests for publications; and 1 181 classified as 'other'. Over 100 000 pamphlets and over 9 000 copies of the credit reporting code of conduct were issued.

Formal statutory complaints

In the year 91/92, there were 201 formal complaints, 140 being in relation to alleged breaches of the Information Privacy Principles by Commonwealth agencies.

Some complaints prove to be unfounded. Of those regarded as reasonably raising a concern, almost invariably Commonwealth agencies are prepared to resolve them by negotiation. Usually, the agency agrees to modify its conduct or remedy the particular harm with which the complainant is concerned.

So far, in three and a half years, I have not made a final formal determination of a complaint. One has been the subject of a preliminary determination which has yet to be finalised. Several others which have not been capable of resolution in the usual way are not proceeding to determination.

Sectoral approach

Perhaps drawing on the example of other Western democracies and the constraints imposed by the Australian Constitution, the Australian approach to privacy has been 'sectoral', with the initial area regulated being Commonwealth government administration. There is some incidental protection of information privacy interests at State level by way of freedom of information legislation and confidentiality provisions. The Federal spent convictions legislation and the credit reporting legislation have had an impact on the State and private sectors.

Need for greater uniformity

The need for greater uniformity of standards in relation to information privacy protection - as between the Commonwealth and the States in relation to the public sectors, and as between the public sector as a whole and the private sector - is becoming more urgent. In its report of 1983, the ALRC identified the promotion of uniform approaches to data protection throughout Australia as a major role for its envisaged Privacy Commissioner.

At present, a number of important trends are occurring in government administration which underscore the need for greater attention to be given to the need for uniformity. These include -

(1) Within the Commonwealth administration, greater use of multi-agency strategies

- directed to the needs and problems of individuals eg DSS-Commonwealth Employment Service - Health, Housing and Community Services joint approach to Jobsearch and Newstart
- to protect agencies against fraud - an issue currently being examined by a Parliamentary committee.

(2) As between Commonwealth and State administration, greater sharing of information such as in law enforcement (eg CTRA's arrangements to share its data with State police forces made under memorandum of understanding); health services; and the management of the electoral roll.

(3) Greater use by Commonwealth agencies of 'outsourcing' arrangements, with the result that Privacy Act protections are reduced.

(4) The privatisation or corporatisation of functions formerly performed in the public sector, eg telecommunications, accompanied by removal of Privacy Act protections.

If the Coalition is elected to government at the next election, its policies as outlined in *Fightback!* will, if implemented, tend to heighten the trends to which I have referred, especially in the third and fourth areas that I have mentioned - 'outsourcing' and 'privatisation' or 'corporatisation'. Consequently, it was with particular interest that I noted that recently in a major speech the Opposition Spokesman on Science and Technology, Mr Peter McGauran, referred to the consequences for privacy protection of outsourcing and similar strategies. In his speech, he noted that a Coalition Government would contract out up to an estimated $1 billion in public service computer technology requirements. He said:

> We would have to have proper regard to privacy requirements and legislation, [but] I think we can work our way through that. For all but sensitive private matters there should be contracting out.[1]

State developments

It may be useful if I recount the position in the States and Territories, in particular, recent developments.

New South Wales

The New South Wales Privacy Committee is one of the world's longest-operating privacy protection bodies. It has a wide brief and can look at both intrusions and information privacy issues.

The Privacy Committee Act 1975 established the NSW Privacy Committee. The Committee performs the role of a privacy ombudsman. The Committee may:

- Investigate/conciliate complaints
- Make reports and recommendations to the Minister.

A NSW Privacy and Data Protection Bill, incorporating some of the recommendations made by the Committee for the Independent Commission Against Corruption (ICAC), introduced as a Private Member's Bill (by Mr Tink), was tabled in December 1991. Due to a lapse in time, the Bill will need to be tabled again. It is anticipated that the Bill will not be discussed until September or later.

Queensland

Queensland had a Privacy Committee (*Privacy Committee Act 1984*), however this was abandoned in 1991. A discussion paper was circulated in 1990, proposing the formulation of privacy guidelines akin to the Information Privacy Principles and establishing a Privacy Commissioner. Reform in this area is in abeyance and it is uncertain as to when reform, if any, will come to fruition.

South Australia

A Privacy Committee was established in July 1989. Its main functions are to make recommendations to the Attorney-General affecting privacy, to improve access to government-held information, and to refer written complaints to the appropriate authorities.

A Privacy Bill advocating a 'tort of privacy' was introduced as a Private Member's Bill (by Mr Groom). The Bill was supported by the Government and its carriage was transferred to the Attorney-General. The Bill created widespread opposition from media, business and industry. The Bill was referred to a parliamentary committee in response to a widespread opposition and was subsequently reintroduced into Parliament. As amended, the Bill excluded media and business from the

tort and this was passed by the House of Assembly. However, when the Bill was introduced to the Legislative Council, the Australian Democrats moved a significant number of amendments to the Bill. These included the establishment of a Privacy Committee, with both government and community representatives, to handle complaints relating to both government agencies and the private sector. It involved roles for the Ombudsman and the Police Complaints Authority, and the establishment of a new set of privacy principles (based on the NSW Private Member's Bill). The Privacy Committee was to be given widespread powers to delegate its functions.

The Government proceeded with the Bill until Parliament rose in May 1992. The Attorney-General now intends to reintroduce a 'clean' Bill in August 1992. The revised Bill is intended to take into account all views expressed so far, with a view to it becoming law by the end of the year.

Victoria

The Victorian Law Reform Commission (VLRC) has a privacy reference and advocates developing guidelines which would give effect to the OECD guidelines. However, Victoria already has a degree of legislation where avenues are available for people to make complaints in relation to breaches of confidence (eg freedom of information, public records and credit reporting). VLRC may look at the possibility of incorporating administration of the Freedom of Information Act with administration of privacy legislation by the Attorney-General's Department.

Northern Territory

Cabinet has agreed to establish administrative instructions in relation to information privacy and freedom of information. These proposals will go to Cabinet in September. The intention is for there to be a privacy committee, however, there is no precise formula for this as yet.

Western Australia

A committee was proposing to bring forward a Privacy Bill as part of a freedom of information package, however this issue is in abeyance at present.

Australian Capital Territory

The ACT Administration is subject to the Privacy Act and to my jurisdiction.

Tasmania

I am not aware of any action on this issue in Tasmania.

Privacy agencies meetings

In early 1990, with a view to encouraging greater sharing of experience and to assist States and Territories contemplating information privacy legislation, I initiated a national meeting of privacy agencies. Since its first meeting in February 1990, this group has met regularly at approximately 6-monthly intervals.

Participating have been representatives of privacy bodies from New South Wales, South Australia, the Commonwealth and, until its body was disbanded, Queensland.

Invitations to attend have been given to jurisdictions without privacy bodies and all except Tasmania have attended on one or more occasions.

Applicability of the Privacy Act scheme to the States

As no doubt you might expect me to say, I do see State adoption of information privacy principles as desirable. But, equally, I acknowledge that it may not be realistic to expect the States to duplicate entirely the Commonwealth privacy protection scheme. While I regard the

'systemic' area as the one where an office of this kind can have the most impact, it may be that to some extent a State regulator can take advantage of the work being done by my office without having to revisit the entire subject. The framework of the national privacy agencies meeting could also be used to avoid duplication.

The nature of the personal data often held in State (or Territory) administration provides a significant reason for States adopting an information privacy policy. State government functions are often 'closer to the people', with a tendency for greater personal detail to be collected in State administration as compared to many areas of Commonwealth administration, eg prisons, police, community services, hospitals, educational institutions.

In the institutional areas mentioned, the data is often gathered in a 'case work' setting. Fine-grained data of the 'case-work' kind has not been seen traditionally as being as amenable to computer storage as basic category data of the kind often collected in Commonwealth administrative schemes. 'Case-work' data is more likely to be held in manual files and stored in manual systems. Insofar as the argument for detailed privacy protections is driven by concerns about computerised storage and dissemination, this factor may be seen as counting against the need for State laws. But the trend seems to be towards more reliance on computer systems, even in this area. In South Australia, for example, the State government has a computerised Justice Information System which, as I understand it, links the various departments and courts concerned with welfare and justice and contains a significant amount of personal data.

During my time as Privacy Commissioner, I have had informal discussions with a number of State offices and some State Ministers on the possibility of applying the Commonwealth model to the States. My advice as to what might be feasible has gone along the following lines:

- Adopt information privacy principles, with any modifications/changes to meet any necessary differences between State and Federal environment.

- Vest responsibility for their implementation in an independent agency

  - short of creating a new agency, options might be Ombudsman or Equal Opportunity Commissioner.

- Encourage regulators to take advantage of Federal work in the systemic area and encourage States as a whole to look at common standards on issues such as education records, hospital records, prisoner records. Federal office could play a role in this.

- If existing office chosen as regulator, engraft IPP-complaints onto the complaints-mechanism already in use in that office.

- Question remains of application of information privacy standards to private sector generally.

Endnote

1 See *The Australian*, 20 July 1992, pp 17, 20.