POLITICS TRIUMPHS IN AUSTRALIA'S NEW DATA PROTECTION LAW

After a decade of indecision, bureaucratic stalling and political controversy, Australia has at last joined much of the rest of the industrialised world in enacting national data protection legislation. Graham Greenleaf examines the new law.

In November the Commonwealth Parliament passed the Privacy Act 1988. The Act only applies to the Commonwealth (Federal) public sector, and not to State government agencies nor to the private sector. It can therefore only be considered a "first instalment" toward Australia's compliance with the OECD Guidelines or eligibility to ratify the Council of Europe Convention. However, it does cover both computerised and manual records.

A vindication of the political process

The Act is a very significant improvement on both the Draft Privacy Bill recommended by the Australian Law Reform Commission in its 1983 Privacy Report, and on the Privacy Bill 1986. The 1986 Bill was introduced into Parliament by the Government as part of a package with the defeated national Identity Card (ID) proposal, the so-called "Australia Card." It contained many subtle qualifications, and some serious omissions, designed to ensure that it would be ineffective, by a Commonwealth bureaucracy and a Labour Government indifferent to privacy.

However, the rejection of the ID Card left the Government desperate to enact some measure of information surveillance through an enhanced Tax File Number, to attempt to reduce tax and social security fraud. Faced with a hostile upper house (the Senate), the Government was forced to accept substantial amendments to the Privacy Bill as the political price for the passage of its Tax File Number legislation. On this occasion the political process has, on balance, resulted in informed amendments which favour individual liberties against the extension of bureaucratic control.

Structure of the Act

The core of the Act consists of eleven information Privacy Principles which are enforceable against Commonwealth government agencies. Individuals may enforce the Principles by injunctions, and may obtain compensatory damages for any loss or damage caused by a breach of the Principles. The Act creates a Privacy Commissioner, who will have power to investigate complaints of breaches of the Principles and to seek injunctions against agencies to enforce them, as well as other functions. There are few exemptions from the Principles stated in the Act. Instead, any agency may seek an exemption from some part of the operation of the Principles on the grounds of public interest, by application to the Privacy Commissioner, who will then make a Public Interest Determination after hearing from interested parties.

The Act does not include a registration system involving either prior approval (the strong Scandinavian model) or prior notification (the weak British model). Instead, Principle 5 requires each agency to maintain a record stating the nature, purpose, access and disclosure conditions etc. for each type of record, and to make it available for public inspection. Agencies must also make a copy of the record available annually to the Privacy Commissioner, who will publish an annual Personal Information Digest of such details.

The Act also contains numerous specific and parallel controls on the use of the Tax File Number, including its use in the private sector. In the European usage, this is sectoral legislation interwoven into the general Act, and it will not be discussed here. It is significant, however, that it gives wide delegated legislative powers to the Commissioner to prepare enforceable Guidelines on the use of the Tax File Number, applicable to both public and private sector users.

The Information Privacy Principles

The eleven Information Privacy Principles (s14) are similar in many respects to the principles contained in the New South Wales Privacy Committee Guidelines (1978), the OECD Guidelines (1980), the Council of Europe Convention (1980) and the United Kingdom Data Protection Act (1984). The Principles are paraphrased below.

Principle 1 — Agencies must not collect personal information unless:
(i) it is collected for a lawful purpose directly related to function or activity of the agency; and
(ii) the means of collection are lawful and fair.

Principle 2 — Agencies must ensure that people from whom they solicit personal information are generally aware of: (i) the purpose of collection; (ii) any legal authority for the collection; and (iii) any third parties to which the collecting agency discloses such information as a usual practice.

Principle 3 — Where an agency solicits personal information (whether from the subject of the information or otherwise), it must take reasonable steps to ensure that the information is (i) relevant to the purpose of collection, up-to-date and complete; and (ii) its collection does not unreasonably intrude upon the person's affairs.

Principle 4 — An agency must protect personal information against misuse by reasonable security safeguards, including doing everything within its power to ensure that authorised recipients of the information do not misuse it.

Principle 5 — Any person has a right to know whether an agency holds any personal information (whether on him or her or not), and if so (a) its nature; (b) the main purposes for which it is used; (c) the classes of persons about whom it is kept;

(d) the period for which each type of record is kept; (e) the persons who are entitled to have access to it, and under what conditions; and (f) how to obtain access to it. Each agency must maintain an inspectable register of this information, and must inform the Privacy Commissioner annually of its contents.

Principle 6 — A person has a right of access to personal information held by an agency, subject to exceptions provided in the Freedom of Information Act 1982 or any other law.

Principle 7 — Agencies must make corrections, deletions and additions to personal information to ensure that it is (i) accurate; (ii) relevant, up-to-date, complete and not misleading (given the purpose of collection and related purposes), subject to exceptions provided in the "Freedom of Information Act 1982" or any other law. Agencies are also required to add a reasonable statement by a person to that person's record, on request.

Principle 8 — Agencies must take reasonable steps to ensure that personal information is accurate, up-to-date and complete (given the purpose of collection and related purposes) before using it.

Principle 9 — Agencies may only use personal information for purposes to which it is relevant.

Principle 10 — Agencies may not use personal information for purposes other than for which it was collected, except (a) with the consent of the person; (b) to prevent a serious and imminent threat to a person's life or health; (c) as required or authorised by law; (d) where reasonably necessary for the enforcement of criminal or revenue law; or (e) for a directly related purpose. In the case of exception (d), but not otherwise, the use must be logged.

Principle 11 — Agencies may not disclose to anyone else personal information, with the same exceptions as apply to Principle 10 (a) - (d), plus an additional exception where the subject of the information is reasonably likely to be aware of the practice of disclosure (or reasonably likely to have been made aware under Principle 2). The recipient of information under one of these exceptions may use it only for the purpose for which it was disclosed.

The use and disclosure Principles (10 & 11) do not apply to information which has already been collected.

Enforcement of the Principles

Agencies are prohibited from breaching the Principles (s16), thereby opening the way for individuals to seek to enforce their observance. Any person may seek an injunction from the Federal Court to restrain an agency

(or any other person) from contravening the Act, or to require a person to take actions so that the Act will not be contravened (s98). It is therefore not only actual data subjects, or only persons who have suffered or are likely to suffer harm because of the breach, who can enforce the Principles.

Individuals may also complain to the Privacy Commissioner of an "interference with privacy" (s36). "Interference with privacy" is defined so that it includes only a breach of the Principles or a breach of the Guidelines concerning Tax File Numbers (s13). If the Commissioner finds the complaint substantiated he or she may seek to conciliate (s27), or may make a declaration that the agency should desist from further breaches, perform actions to remedy any loss or damage suffered by the complainant (s52) or pay pay compensatory damages to the complainant (s 52). Complainants may also be awarded payment of expenses incurred in pursuing a complaint, irrespective of the declaration made (s52(3)). Such declarations are binding on the agency concerned (ss55-56). Complainants can recover compensatory damages and costs as a debt (s57), and can enforce other determinations in the Federal Court (s59). Both a complainant and an agency may appeal against a decision of the Commissioner to the Administrative Appeals Tribunal (s58), and thence to the Federal Court.

"Representative complaints" may be made on behalf of more than one person (s36(2)), but in that case damages may not be awarded (s52).

The Commissioner may also investigate possible breaches of the Principles or Guidelines on his or her own initiative (s40(2)). If the agency concerned fails after 60 days to comply with any recommendations the Commissioner makes, the Commissioner may have a report tabled in Parliament in a further 15 days (s30). He or she may also seek an injunction from the Federal Court to remedy any breaches found (s98), without any need to delay. The ever-present possibility of an injunction could be expected to make agencies take s30 recommendations somewhat more seriously than they might otherwise be disposed to.

The range of measures available to enforce the Principles are therefore comprehensive, ranging from persuasion to injunctions and, most importantly, damages. They are also a judicious blend of what Norways's Knut Selmer characterised at the 1988 Data Protection Commissioner's Conference as "the American approach of enforcement by individual initiative, and the European approach of enforcement by a government authority."

The Privacy Commissioner

The Privacy Commissioner is to be appointed by the Government for a seven year term (s19), and is to be part of the existing Human Rights and Equal Opportunities Commission.

Almost all of the Commissioner's functions (s27) are related to, and therefore limited by, references to "interfaces with privacy", the meaning of which is limited to breach of the Principles and breach of the Tax File Number Guidelines (s13). The Act does not give the Commissioner any significant role concerning "invasions of privacy" outside these two specific categories. Any limitations in the scope of the Principles will therefore

have a direct effect on the Commissioner's functions. In contrast, the New South Wales Privacy Committee can investigate any type of "interference with privacy," but has very limited enforcement powers.

Subject to this very strict limitation, the more significant functions of the Commissioner are: to attempt to settle complaints by conciliation; to examine proposed Acts when requested to do so by a Minister; to monitor developments in computing, including data-matching and data-linkage; to audit records of agencies for compliance with the Principles; to examine data-matching or data-linkage proposals on request by a Minister; and to encourage corporations to adopt the OECD Guidelines voluntarily.

Outside enforcement of the Principles, discussed above, the Commissioner's ability to take independent action to warn the public of dangerous developments threatening privacy are very limited. His or her power to examine proposed legislation or proposed data-matching and data-linkage practices is limited to when requested by a Minister, and even then there is no right to report to the public or Parliament on what was found. The Commissioner must make an Annual Report to Parliament on the operation of the Act (s97), and may presumably there give details of the exercise of every one of his or her functions. There is no equivalent to the NSW Privacy Committee's right to make public statements on matters concerning privacy generally.

There will also be a Privacy Advisory Committee of 6 part-time members appointed by the Government, but with a majority coming from outside the public sector (s82), and chaired by the Commissioner. The Committee can give advice to the Commissioner, but has no independence from the Commissioner whatsoever, being unable to even meet without the Commissioner's consent, and unable to make its own report to Parliament.

Exemptions from the Principles

The Act contains few express exemptions from the operation of the Principles. The main exemptions are: those in the use and disclosure Principles (10 & 11), as listed above; the exceptions to the subject access and correction Principles (6 & 7) imported from the "Freedom of Information Act", the exemption of some agencies in respect of their commercial activities; and a blanket exemption emanating from them (Part 11).

Instead, one of the main functions of the Privacy Commissioner will be to make the detailed decisions as to whether to exempt specific agencies from parts of the Principles for certain activities, on the grounds of public interest. The Commissioner is empowered to make such an exemption where the public interest in an agency breaching a Principle "outweighs to a substantial degree" the public interest in adhering to the Principle (s72). Such a "Public Interest Determination" means that such acts are deemed not to be a breach. The onus is properly left with the agency seeking exemption. The Commissioner must publish any agency application for a Determination (s74), take account of any submissions received (s79), and hold a conference on the application if any person so requires (s76).

This is one of the most novel features of the Australian Act. In principle it seems to be a sensible compromise between the desire for very general Principles which in most cases can be applied strictly, and a recognition that Principles of such generality will inevitably need some exceptions, given the diversity of governmental activities that they regulate. The creation of a public arena where the details of the proper scope of data surveillance and data protection can be debated and developed continually on a clear basis of public interest criteria, but with procedural flexibility, seems to be a sound solution.

However, the implementation of the Public Interest Determination procedures is one of the weakest parts of the Act, because these procedures are still blatantly biased in favour of agencies seeking exemptions.

An agency may apply for a determination under s72 in relation to such acts and practices as it decides (s73), but the Commissioner can only either dismiss the application or give it unconditional approval (s78). The Commissioner cannot impose conditions on allowing a breach of the Principles, nor even allow such breaches on condition that the matter be re-examined after a period of time. Nor is there any provision for the Commissioner or anyone else to re-open the application. Since exemptions from the Principles are inherently undesirable, this is clearly unsatisfactory.

Further evidence of bias is found in the requirement that the Commissioner make a draft determination only on the evidence of the applicant agency (s75); that agencies can have legal representatives at conferences but individuals cannot (s77); and, most extraordinarily, that an agency can suppress the disclosure of evidence on which its application is based to those who wish to contest it merely by claiming that the information is exempt under the "Freedom of Information Act" (s74)!

The Commissioner's Determinations may be disallowed by Parliament (s80), which is entirely appropriate for what is, in effect, the making of delegated legislation. Ultimately, therefore, any exemptions from the Principles must run the gauntlet of Parliament.

An initial appraisal

The political process seems to have served the Australian public well, insofar as the Privacy Bill has been converted from a travesty of data protection into what is in many respects a very strong Act, although one limited in scope. Such novel and complex legislation cannot be expected to be perfect, and the Privacy Act will need amendment, particularly in relation to Public Interest Determinations.

The Act allows the Commissioner, individual citizens, the Courts, and even Parliament to each play a continuing role in the development of data protection law within its framework. There is ample scope for them to make the Act a powerful weapon to protect individual liberties.

Graham Greenleaf is a Lecturer in Law, at the University of New South Wales, Australia, and is a Member of the New South Wales Privacy Committee. He was the first Australian representative to attend the annual meeting of Data Protection Commissioners, held this year in Oslo in September.