AN OVERVIEW OF DATA PROTECTION IN AUSTRALIA

BY GORDON HUGHES*

A. *INTRODUCTION*

The ever increasing capacity of computers to store information about individuals inevitably gives rise to concerns about the security of the data and the privacy of the data subject. In many overseas jurisdictions, this has led to the emergence of so-called data protection schemes, pursuant to which statutory controls have been imposed upon those responsible for handling computerized information. In Australia, however, neither the federal nor the State governments have yet introduced such a scheme, notwithstanding the fact that the potential privacy threats posed by the computerization of personal information have been clearly identified.

The Privacy Amendment Act 1990 (Cth) and the Data-matching (Assistance and Tax) Act 1990 (Cth), along with current legislative proposals in Western Australia, provide evidence that the need for a formal data protection scheme has been recognized in some jurisdictions, at least. It is evident, however, that the collective initiatives to date have been of an unsatisfactory, *ad hoc* nature and have failed to provide a comprehensive and effective statutory basis for the protection of privacy of individuals in these circumstances.

This article will outline the threats posed to privacy by the computerization of personal information, analyse the deficiencies of the common law in regulating information handlers and examine the impact of various *ad hoc* legislative initiatives at both federal and State level. It will then propose a solution which would ensure that data subjects are adequately protected in Australia.

B. *PROBLEMS POSED BY COMPUTERS*

The range of subject-matter which can be stored on a computer is limitless. Storage may involve the public sector or the private sector or both. It may involve commercial or personal data, some of which may be public knowledge and some of which may be private. Unauthorized use of such information may have financial, political or personal consequences.

Unique problems have always existed in relation to the storage of personal information, particularly where the information subject wishes to maintain confidentiality, because the ramifications of misuse can be difficult to define. Whereas the impact of unauthorized use of commercially sensitive data can to some extent be objectively determined, the effect of misuse of personal data must generally be assessed in subjective terms.

* LL.M.(Melb.), Ph.D. (Mon.), Solicitor, Lander & Rogers, Melbourne.

The storage of personal information on computers introduces a new dimension to this vulnerability. It has been observed that, as a result, individuals find themselves 'naked and uncertain in a psychological prison fashioned by a complex technology',[1] and for this reason alone there is a need for specific regulation of computerized data storages.

It is arguable that there should be no difference in protective measures for information handled electronically, as opposed to information handled manually.[2] This proposition was recognized by the Younger Committee in the United Kingdom in 1972.[3] A consistent observation was made in the report of the Lindop Committee in the United Kingdom in 1978.[4] The Lindop Committee suggested that in the future, there would be 'greater ease of use by those with no technical knowledge of computing, which could make the distinction between computer-based, or computer assisted, systems and manual systems increasingly blurred'.[5]

On the other hand it is equally true, as stated by the Australian Law Reform Commission in 1983,[6] that 'personal information flows more freely in the computer age' and that, therefore, 'the potential for harm from incorrect or misleading information is greatly increased'.[7] The capacity for storage and collation of personal information is dramatically expanded, along with the capacity for abuse.[8] Unlike manual storage systems, computerized storage systems are susceptible to the theft of disks and tapes containing huge quantities of information and, where a telecommunications link is involved, susceptible to remote access of one processor and to interception of information passing between two processors. The risk of abuse through 'unscrupulousness, irresponsibility or inefficiency'[9] is potentially far greater than is the case under a manual system.

It is not difficult to appreciate the implications of insecure computerized data in the public sector. As revealed during the Australia Card debate in 1986, public concern over the possible creation by computers of personal profiles and the implementation of some form of computerized surveillance is unavoidable.

The implications of mismanagement of computerized databanks in the public sector have been acknowledged by the Commonwealth government. In a debate in the House of Representatives on the Privacy Bill 1986, the then Attorney-General, Mr Lionel Bowen, observed:

1 Cowen, Z., *The Private Man (Boyer Lectures*, 1969) 31.
2 Lindop, N., 'Legislating for Data Privacy', in Campbell, C. (ed.), *Data Processing and the Law* (1984) 155, 158.
3 United Kingdom, *Report of the Committee on Privacy* (1972) Cmnd 5012 (*Younger Committee Report*), paras 587 and 589.
4 United Kingdom, *Report of the Committee on Data Protection* (1978) Cmnd 7341 (*Lindop Committee Report*).
5 *Ibid.* para. 3.12.
6 Commonwealth, Australian Law Reform Commission, *Privacy* (1983) 22 A.L.R.C. (*A.L.R.C. Privacy Report*).
7 *Ibid.* para. 37.
8 See Burnside, J. W. K., 'The Legal Implications of Computers' (1981) 55 *Australian Law Journal* 79, 89.
9 *Younger Committee Report*, *op. cit.* n. 3, para. 590.

> With the greater range of services being provided by the Government, the greater is the accumulation of personal information about individuals. More than anything else, the capacity of modern computers to search and process information offers the greatest potential for invasion of personal privacy by misuse.[10]

In the private sector, the increasing ability of computers to handle personal information allows 'record keepers involved in traditional relationships with clients, customers, patients, research subjects and others to increase the volume of information held',[11] thereby increasing the risk of that information flowing 'in directions never envisaged by the existing legal and official framework governing those relationships'.[12]

The impact of computers on private sector record-keeping activities has, perhaps, been most significant in the context of personal finance. This concern was evidenced by the adverse reaction in March 1989 to a proposal by the Credit Reference Association of Australia that it intended to store personal loan and credit records of all Australians in a centralized, privately operated computerized record system.[13] Ultimately, it was necessary to abandon the proposal and, subsequently, Commonwealth legislation was introduced in the form of the Privacy Amendment Act 1990 (Cth) to regulate any such database in the future.[14]

It follows that computerized information storages should be regarded as more than a simple alternative form of record-keeping. They should be regarded as an independent technological phenomenon with capacities and implications previously unanticipated and unappreciated. Viewed in this context, it is inevitable that traditional regulatory measures which have evolved in relation to manual storage systems will be an irrelevant, or at least unsuitable, basis for regulating automatic databanks.

It is not suggested that the computerization of information only has negative implications. Nevertheless, with each of the social and economic benefits generated by computerization, there are inevitably corresponding risks of greatly facilitated abuse arising from the security problems inherent in the transmission, linkage and general accessibility of computerized information.[15]

It is, therefore, imperative that the benefits and the risks of computerization be adequately balanced. Achieving this balance is a difficult exercise but without some safeguards and restraints, the benefits the computer can bring to our society will be accompanied by a loss of individual privacy that many may find unacceptable.[16]

[10] Commonwealth, *Parliamentary Debates*, House of Representatives, 23 October 1986, 2656. The Commonwealth privacy legislation is analysed in more detail below.

[11] *A.L.R.C. Privacy Report*, *op. cit.* n. 6, para. 84.

[12] *Ibid. Cf.* United Kingdom, *Computers and Privacy* (1975) Cmnd 6353, para. 6. This White Paper, together with the supplementary report *Computers: Safeguards for Privacy*, United Kingdom (1975) Cmnd 6354 analyzed the nature and extent of information held in government computers, the adequacy of existing regulations and the need to introduce legislation regulating the storage of personal data on computers in the public and private sectors.

[13] It was estimated in 1988 that the Association held 6,000,000 records of 'personal information relating to people's financial transactions': Commonwealth, Senate Standing Committee on Legal and Constitutional Affairs, *Feasibility of a National ID Scheme; the Tax File Number* (1988), para. 5.9 (*Senate TFN Report*).

[14] The Privacy Amendment Act 1990 (Cth) is discussed in more detail below.

[15] See *A.L.R.C. Privacy Report*, *op. cit.* n. 6, para. 118.

[16] Niblett, G. B. F., 'Computers and Privacy' in Robertson, A. H. (ed.), *Privacy and Human Rights* (1973) 174.

The Australian Law Reform Commission, in its Report on Privacy, identified four major dangers arising from technological change. First, there was the ability of computers to store, collate and transmit huge volumes of information in a manner which would have been inconceivable where a manual record-keeping system was involved. Second, there was an increased risk of unauthorized disclosure by persons with authorized access, facilitated by the increased ease of identifying and extracting specific data. Third, there was the ability to store large amounts of information without the need for destruction, resulting in the retention of out-of-date and perhaps inaccurate records. Finally, there was an increased temptation for unauthorized access by outsiders, again facilitated by the increased ability to identify and extract specific data. Those observations, published in 1983, remain valid today.

A corollary of this concern about data security is a concern about the accuracy of the information stored,[17] given the absence of manual involvement in the collation of some information, the risk of inaccuracies in the case of manual input, the threat of contextual errors inherent in 'matching' operations and, in general terms, the increased reliance on computers to make decisions affecting individuals. It is clear, therefore, that the privacy issues under discussion cannot be resolved without reference to the right of an individual to know the precise nature of information relating to him or her. Accordingly, a consideration of the adequacy of data protection laws inevitably involves a review of existing freedom of information legislation.

Against this background, it is clear there is a need for an effective data protection scheme — a legislative regulation of information stored in computers. The need has been recognized and implemented in a number of overseas jurisdictions, but it has been addressed only in an *ad hoc* fashion in Australia. Without an effective data protection scheme, computerized information banks in both the public and private sectors will proliferate at the expense of the privacy of individuals.

C. *SOME OVERSEAS INITIATIVES*

It is important to observe the extent to which overseas jurisdictions have legislated for the protection of privacy and, more specifically, for data protection and freedom of information. These initiatives have been most pronounced in the United Kingdom and Western Europe, whilst the experience in Canada and the United States is worth noting.

(a) *United Kingdom*

In the United Kingdom, the Data Protection Act 1984 was enacted with the principal intention of effecting ratification of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the Council of Europe Convention) and in turn facilitating British

[17] For an early but informative analysis of the dangers of inaccurate data storage, see Karst, K. L., '"The Files": Legal Controls over the Accuracy and Accessibility of Stored Personal Data' (1966) 31 *Law and Contemporary Problems* 342.

competition within the European Market.[18] The Act, which was implemented progressively in four steps between 1984 and 1987,[19] provides protection to individuals against the inaccuracy or misuse of information stored about them on computers.[20] The Act contains eight data protection principles, based on the Council of Europe Convention, which are enforceable by the Data Protection Registrar. It further provides civil remedies in the event that loss is suffered as a result of inaccurate data or unauthorized disclosure of data. The Act has broad application in the public and private sectors, applying to data users, computer bureaux and data subjects.

The Data Protection Act is restricted to 'personal' data in a form which can be processed by equipment operating automatically. It does not, therefore, apply to information processed and stored manually. There is a series of exemptions including, in appropriate circumstances, word processing applications, payrolls and accounts, mailing lists, research and statistical data, certain government data and exclusively domestic data. Data users and computer bureaux are subject to registration and it is an offence of strict liability to process data when unregistered.[21]

A total of 15 new criminal offences are created to assist in the enforcement of the Act.

Whilst there is no specific freedom of information legislation in the United Kingdom, the Data Protection Act provides an individual with the right to be supplied with a copy of personal data being held about himself or herself and, in appropriate circumstances, a data subject may apply for the rectification or erasure of inaccurate records.[22]

(b) *Western Europe*

A majority of the Western Europe countries have enacted data protection and freedom of information legislation,[23] administered in each case by a data protection agency.[24] The emergence of these laws is largely due to pressures of

[18] See, *e.g.*, Savage, N., and Edwards, C., 'Transborder Data Flows: the European Convention and United Kingdom Legislation' (1986) 35 *International and Comparative Law Quarterly* 710, 714.

[19] The final stage of the Act came into force on 11 Novermber, 1987; the Council of Europe Convention was ratified by the United Kingdom on 1 December, 1987. The Council of Europe Convention came into force on 1 October, 1985 and has now been ratified by nine countries: Austria, France, West Germany, Luxembourg, Norway, Spain, Sweden, United Kingdom and the Netherlands.

[20] For a general analysis of the legislation, see, *e.g.*, Niblett, B., *Data Protection Act 1984* (1984), Sterling, J. A. L., *The Data Protection Act 1984* (2nd ed. 1985), and Gulleford, K., *Data Protection in Practice* (1986).

[21] It has been suggested that the success or failure of the Act is principally dependent upon compliance by data users with registration requirements and the willingness of the Registrar to enforce compliance: Savage, N., and Edwards, C., 'The Legislative Council of Data Processing — the British Approach' (1985) 6 *Computer Law Journal* 143, 156.

[22] Subject access rights were introduced to the final implementation phase in November, 1987. For a discussion of the issues raised in this regard, see Kenny, J. J. P., 'Subject Access and the Data Protection Act 1984' (1988) 4 *Computer Law & Practice* 106.

[23] For a summary of national European legislation on databanks, see, *e.g.*, Frosini, V., 'The European Convention on Data Protection' (1987) 3 *Computer Law & Practice* 84, 85-6.

[24] It has been argued that as general awareness of the privacy problems posed by information technology increases, the role of 'specialised institutions of information control may become obsolete': Burkett, H., 'Institutions of Data Protection — an Attempt at a Functional Explanation of European National Data Protection Laws' (1982) 3 *Computer Law Journal* 167, 188.

trade and competition, obligations arising through membership of the Organization for Economic Co-operation and Development ('O.E.C.D.'), and the implications of ratification of the Council of Europe Convention.[25] For example, Austria, France and Luxembourg have enacted data protection legislation (including freedom of information provisions or separate, complementary freedom of information legislation) applicable to both the public and private sectors, based on a central registration system. The Netherlands has indicated a preference for more general data privacy legislation, based on self-regulated observance of 'material standards' as opposed to a licensing system.[26]

The Federal Republic of Germany has a unique administrative arrangement, whereby federal data protection laws are registered with regional governments and applied to the private sector. The scheme is restricted to files capable of being processed automatically. In a complicated adminstrative arrangement, three levels of data protection agencies operate within the Republic — one being responsible for administration of federal law in the private sector at regional level, and one being responsible for public sector administration at regional level according to regional law.[27]

Each of the Scandinavian countries has legislation relating to data protection and freedom of information in varying forms,[28] with Sweden being notable as the first country to introduce freedom of information laws and the first country to introduce national data protection legislation. The Swedish and Danish data protection legislation specifically extends to computerized records in the private sector.

(c) *Canada*

In Canada, the Privacy Act 1982[29] repealed and replaced the Human Rights Act 1978[30] and came into force on 1 July 1983 at the same time as the Access to Information Act 1983.[31] The Act is directed at personal information relating to individuals. It applies, with some exceptions, to personal information under the control of federal government institutions, whether recorded in computerized or manual form.[32] Privacy legislation[33] and freedom of information legislation[34] has also been enacted in six provinces.

25 The early development of European data protection laws is summarized in Hondius, F. W., *Emerging Data Protection in Europe* (1975).

26 See Altes, F. K., 'Computer Law Developments in the Netherlands' (1988) 2 (No. 9) *International Computer Law Adviser* 4, 6-7; De Pous, V., 'Recent Developments in Dutch Data Protection Law' (1990) 6 *Computer Law & Practice* 206.

27 Burkett *op. cit.* n. 24, 178.

28 For a commentary on the dual Danish data protection legislation (one Act regulating data storages in the public sector and one in the private sector), see Blume, P., 'New Danish Rules on Data Protection' (1988) 3 (No. 2) *International Computer Law Adviser* 16.

29 S. C., 1980-1-2-3, Ch. III, Schedule II.

30 S. C., 1976-7, Ch. 33.

31 S. C., 1980-1-2-3, Ch. III, Schedule I. For an early but comprehensive review of Canadian privacy laws (including provincial legislation), see Burns, P., 'The Law and Privacy: the Canadian Experience' (1976) 54 *Canadian Bar Review* 1.

32 It has been suggested that 'to date, Canada has not witnessed a particularly vociferous debate on the question of electronic privacy, at least regarding data held in the private sector': Potter, R. B.,

(d) *United States*

In the United States, the Privacy Act 1974[35] prohibits officers of federal government agencies from disclosing information about an individual without that person's written consent, except in the performance of their duties or in the event of other prescribed exceptions.[36] The Act requires agencies to disclose their data collection activities and to justify publicly their collection of data.

The Privacy Act operates on the basis of the creation of minimum standards for the collection of information, a breach of which entitles the individual to bring a civil action for limited damages. There is also a right, supported by the amended Freedom of Information Act 1974,[37] of access to, and amendment of, records in the possession of federal government agencies.[38]

There are several other federal legislative enactments in the United States which have a direct or indirect impact on the security of computerized information. These include the Fair Credit Reporting Act 1970[39] which provides an individual with a right to challenge the accuracy of data accumulated by credit reporting agencies in some circumstances; the Fair Credit Billing Act 1976[40] which gives persons a right to delay the issuing of a credit report in circumstances where it is alleged that an error has been made; and the Computer Security Act 1987[41] which provides for the creation of a computer standards program within the National Bureau of Standards, the implementation of government-wide computer security and the training in security matters of persons involved in the management, operation and use of federal computer systems.

Finally, it should be noted that there has been little supplementary State legislation on privacy enacted in the United States, although eight states[42] incorporate a right of privacy into their constitutions.

'Electronic Data Bases: Sleeping Issues' (1987) 2 (No. 2) *International Computer Law Adviser* 13, 17.

33 British Columbia, Manitoba, Saskatchewan, Newfoundland, Quebec and Ontario.

34 Newfoundland, Nova Scotia, New Brunswick, Quebec, Manitoba and Ontario. In relation to common law and statutory privacy rights in Ontario, see Irvine, J., 'The Invasion of Privacy in Ontario — a 1983 Survey', in *Torts in the 80s, Special Lectures of the Law Society of Upper Canada* (1983), 25.

35 5 U.S.C. # 552 (1976 & Supp. IV 1980).

36 For a synopsis of the Privacy Act 1974, see Freedman, W., *The Right of Privacy in the Computer Age* (1987) 16-7.

37 5 U.S.C. #552 (1976 and Supp. IV 1980). The Freedom of Information Act was originally signed into law in 1966, as Public Law 89-487, which was an amendment to the Administrative Procedure Act 1946 s. 3 which provided for public disclosure of executive branch rules, opinions and orders, and public records.

38 For an assessment of the interrelationship between computer technology, privacy and United States federal policy and freedom of information legislation, see Gordon, H., 'The Interface of Living Systems and Computers: the Legal Issues of Privacy' (1980) 2 *Computer Law Journal* 877. In relation to the Freedom of Information Act and the possible effect of computers on the operation of the Act's provisions regarding dissemination of information, see Graham, J. M., 'Fair Administration of the Freedom of Information Act after the Computer Revolution' (1984) 5 *Computer Law Journal* 51.

39 15 U.S.C. #1680-1681i (1976).

40 15 U.S.C. #1666 (1976).

41 P.L. 100-235; A.D. U.S.C.A. #759.

42 Alabama, Arizona, California, Florida, Hawaii, Louisiana, Montana and Washington.

D. *AUSTRALIA*

It can be assumed for the purposes of the present discussion that the common law provides inadequate remedies for individuals whose privacy is invaded as a result of the misuse or abuse of computerized databanks containing personal information.

It is generally accepted, for example, that the common law does not recognize a tort of violation of privacy as a consequence of the High Court decision in *Victoria Park Racing and Recreation Grounds Company Limited v. Taylor and Ors.*[43] It must also be accepted that the equitable action for breach of confidence, whilst providing a remedy in respect of the unauthorized use or disclosure of personal information in some circumstances,[44] is limited by its possible inapplicability where information is accessed without authority by a third party with whom the data subject has no confidential relationship.[45] *Ad hoc* remedies may arise in contract and tort (tort remedies may include negligence, inducing breach of contract, nuisance, trespass, passing off and defamation), but their effectiveness in protecting the individual is limited by the uncertainty of their application from case to case.[46]

(a) *Commonwealth Legislation*

Given that there is inadequate protection afforded to the subjects of computerized information at common law, it becomes necessary to consider the extent to which the Commonwealth has effectively legislated to protect the rights of individuals. This issue requires detailed examination as, obviously, it forms the basis of any effective, national data protection scheme. The issue is particularly significant as it appears the Commonwealth has refrained from exercising its legislative powers to the fullest extent.

(i) *Constitutional Considerations*

The Commonwealth does not have a specific power under the Constitution to legislate with respect to privacy. The extent to which federal legislation can be enacted in this area depends, therefore, upon a specific privacy interest or computer-related activity being embraced by other powers conferred by the Constitution. Hence to the extent that such legislation were to fall within (or

[43] (1937) 58 C.L.R. 479. The Australian Law Reform Commission has stated that 'the decision must be regarded as a major one in considering the prospects of a judicial expansion of common law rights within Australia so as to protect intrusions into personal privacy': Commonwealth, Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, (1979) 11 A.L.R.C. 113.

[44] See, generally, Gurry, F., *Breach of Confidence* (1984).

[45] See *Malone v. Metropolitan Police Commissioner* [1979] Ch. 344. *Cf. Franklin v. Giddins* [1978] Qd. R. 72. Following concerns about the limitations on privacy protection afforded by the duty of confidence expressed by the Australian Law Reform Commission (see *A.L.R.C. Privacy Report*, paras 855-61), the *Privacy Act* 1988 (Cth) introduced amendments applicable to obligations of confidence involving Commonwealth agencies or officers and all obligations of confidence arising by virtue of the law in force in the Australian Capital Territory (ss 89-93).

[46] For a more detailed discussion of the deficiencies of the common law remedies, see Hughes, G., 'Data Protection at Common Law' (1988) 62 *Law Institute Journal* 971.

were to be incidental to the execution of [47]) the trade and commerce,[48] taxation,[49] posts and telegraphs,[50] banking,[51] corporations[52] or insurance[53] powers, for example, truly national application could be achieved. Similarly, federal legislation can be enacted to regulate the public service[54] or, pursuant to the external affairs power,[55] to implement Australia's obligations pursuant to international agreements.

Much of the debate surrounding the introduction of Commonwealth privacy laws has proceeded on the assumption that none of these powers could justify the implementation of legislation regulating the private sector on a national basis. This, however, underestimates the scope of the external affairs power contained in s. 51 (xxix) of the Constitution.

Pursuant to the external affairs power the Commonwealth can implement Australia's obligations under international treaties.[56] Clearly, such legislation will sometimes affect matters within areas which would normally be regarded as the subject of States' residual powers.[57] Uncertainty can arise as to the validity of Commonwealth legislation in such circumstances. Some of this uncertainty may have been alleviated, however, by the diverse majority judgments of the High Court in *Koowarta v. Bjelke-Petersen and Ors*[58] and *Commonwealth of Australia v. Tasmania*[59] (the *Tasmanian Dam* case).[60]

Koowarta's case involved, *inter alia*, a consideration by the High Court of whether certain provisions of the Racial Discrimination Act 1975 (Cth), passed to give effect to the International Covenant on the Elimination of All Forms of Racial Discrimination, represented a valid exercise by the Commonwealth of the external affairs power in s. 51 (xxix) of the Constitution. The majority[61] upheld the legislation.

The *Tasmanian Dam* case involved a consideration of the validity of the World Heritage Properties Conservation Act 1983 (Cth) and the World Heritage (Western Tasmania Wilderness) Regulations made pursuant to the National Parks and Wildlife Conservation Act 1975 (Cth). The legislation purported to implement Australia's obligations pursuant to the Convention for the Protection of the World Cultural and Natural Heritage, adopted by the United Nations

47 *Commonwealth Constitution* s. 51(xxxix).
48 *Ibid.* s. 51(i).
49 *Ibid.* s. 51(ii).
50 *Ibid.* s. 51(v).
51 *Ibid.* s. 51(xiii).
52 *Ibid.* s. 51(xx).
53 *Ibid.* s. 51(xiv).
54 *Ibid.* s. 52(ii).
55 *Ibid.* s. 51(xxix).
56 The treaty will have no domestic application otherwise: *Attorney-General for Canada v. Attorney-General for Ontario and Ors* [1937] A.C. 326; *Bradley v. Commonwealth of Australia and Anor* (1973) 128 C.L.R. 557; *Kioa and Ors v. Minister for Immigration and Ethnic Affairs and Anor* (1985) 62 A.L.R. 321.
57 See, generally, Lumb, R. D., *The Constitution of the Commonwealth of Australia Annotated* (4th ed. 1986) 158-66.
58 (1982) 153 C.L.R. 168.
59 (1983) 158 C.L.R. 1.
60 See, generally, Hanks, P. J., *Australian Constitutional Law* (3rd ed. 1988) ch. 38.
61 Stephen, Mason, Murphy and Brennan JJ.; Gibbs C.J., Wilson and Aickin JJ. dissenting. See also Zines, L., *The High Court and the Constitution* (2nd ed. 1986) 247-8.

Educational, Scientific and Cultural Organisation in 1972 and ratified by Australia in 1974. Again, it was held by the majority[62] that the legislation was valid, thus further emphasizing that the Commonwealth has a broad capacity under s. 51 (xxix) to enact legislation which would not otherwise be within its competence.

Of particular significance in the *Tasmanian Dam* case was the support of two judges for the proposition that the external affairs power could provide a basis for legislation giving effect not only to treaties but also legislation necessary for the 'observance of the spirit as well as the letter of international agreements, compliance with the recommendations of international agencies and pursuit of international objectives which cannot be measured in terms of binding obligations'.[63]

Unfortunately, however, the limits of the Commonwealth power remain ill-defined. On the basis of the majority judgments in the *Tasmanian Dam* case alone, the power is subject to the qualification that the Act must accord with the wording of the treaty or other international instrument in question,[64] that there must be a reasonable proportionality between the object of the international agreement and the content of the Act[65] and that the legislation must generally be 'appropriate for implementation of provisions of the treaty'.[66]

Perhaps most ill-defined of the limits is the degree of international character which the treaty or other agreement must possess in order to justify legislation based on the external affairs power.

In *Koowarta*'s case, for example, Stephen J. favoured the view that such a treaty should be a topic of 'especial concern' to the relationship between Australia and another country, or else of 'general international concern'.[67] Mason J., on the other hand, denied that there was a 'solid foundation for implying a restriction that the treaty must relate to a matter which is international in character or of international concern'.[68]

In the *Tasmanian Dam* case, Mason J. focused on Stephen J.'s analysis of the external affairs power[69] and adopted a broad interpretation in any event. Whilst

62 Mason, Murphy, Brennan and Deane JJ.; Gibbs C.J., Wilson and Dawson JJ. dissenting. See also Zines, *op. cit.* n. 61, 248-52.

63 (1983) 158 C.L.R. 1, 258-9 *per* Deane J.

64 *Ibid.*, 131 *per* Mason J. *Cf.* the apparently narrow interpretation in *R. v. Burgess; ex parte Henry* (1936) 55 C.L.R. 608 by Dixon J. who considered the external power 'necessitates a faithful pursuit of the purpose [of the treaty], namely, a carrying out of the external obligation': *ibid.* 674.

65 (1983) 158 C.L.R. 1, 260 *per* Deane J.

66 *Ibid.* 172 *per* Murphy J. *Cf. Richardson v. The Forestry Commission and Anor* (1988) 164 C.L.R. 261 in which the *Tasmanian Dam Case* was applied and in which Mason C.J. and Brennan J. reiterated that legislation giving effect to a treaty obligation must be 'capable of being reasonably considered appropriate and adapted to that end': *ibid.* 289. Dawson J. went further, however, expressly supporting Commonwealth legislation which gave effect to the matters of international concern which were relevant to the treaty, even if it extended 'beyond the limits of the treaty': *ibid.* 324. Concern has been expressed that the approach adopted by the High Court, particularly by Dawson J., means 'the external affairs power becomes unlimited in scope': Lumb, R. D., 'The External Affairs Power and Constitutional Reform' (1988) 62 *Australian Law Journal* 679, 682.

67 (1982) 153 C.L.R. 168, 216-7.

68 *Ibid.* 229. On this point, the interpretation adopted by Mason J. was consistent with the other members of the majority, Murphy and Brennan JJ.

69 Attention was directed to the judgment of Stephen J. in *Koowarta*'s case because his view of the external affairs power was the 'narrowest expression of it by the justices who constituted the majority': *ibid.* 122 *per* Mason J.

emphasizing that there was an absence of guidelines to assist in determining what constituted an 'international character', he concluded that 'participation in a convention indicates a judgment on the part of the participating nations that they will derive a benefit from it', and that 'the existence of international character or international concern is established by entry by Australia into the convention or treaty'.[70]

Despite the contrasting approaches of members of the majority, *Koowarta*'s case and the *Tasmanian Dam* case emphasized the capacity of the Commonwealth government to enact broad legislation on the basis of s. 51 (xxix) of the Constitution in circumstances where it lacks any other specific power over the subject-matter. Even in his dissenting judgment in the *Tasmanian Dam* case, Gibbs C.J. acknowledged that there was almost 'no aspect of life which under modern conditions may not be the subject of an international agreement, and therefore the possible subject of Commonwealth legislative power'.[71]

The significance of the diverse interpretations of the scope of the external affairs power in the present context will become apparent below when Australia's international obligations are outlined. Whilst one instrument, the International Covenant on Civil and Political Rights,[72] has treaty status, the other, the O.E.C.D. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ('the O.E.C.D. Guidelines'),[73] does not. The Covenant, it will be observed, is expressed in relatively broad terms, whilst the O.E.C.D. Guidelines are considerably more specific in identifying principles which signatories undertake to implement.

It follows that implementation of the Covenant would only justify the enactment of specific data protection legislation if one were to adopt a liberal interpretation of the required nexus between a treaty and the implementing statute. The requisite nexus would far more readily be established, on the other hand, if one were to accept that implementation of the more precisely worded O.E.C.D. Guidelines (despite being of less than treaty status) could be achieved by reliance upon the external affairs power.

There is one further general qualification on the exercise of Commonwealth power in this regard which needs to be considered: the implied immunity doctrine. The doctrine has its origins in *City of Melbourne v. Commonwealth and Anor*[74] ('the *State Banking* case') in which the majority of the High Court[75] established a limitation on the power of the Commonwealth to bind the States which had emerged from *Amalgamated Society of Engineers v. Adelaide Steamship Co. Ltd and Ors*[76] ('the *Engineers'* case'). In the *State Banking* case, Dixon J. confined the limitation to 'a law which discriminates against States or a law

70 (1983) 158 C.L.R. 1, 125. *Cf.* Brennan J., who, whilst adhering to the view that Stephen J.'s test would be satisfied if an obligation were created by an international treaty, further expressed the view that if an obligation were not imposed, then it would be 'necessary to determine whether the subject affects or is likely to affect Australia's relations with other international persons': *ibid.* 220.

71 *Ibid.* 100.

72 *Australian Treaty Series* (1980) No. 23.

73 Paris, O.E.C.D., 1981.

74 (1947) 74 C.L.R. 31.

75 Latham C.J., Rich, Starke, Dixon and Williams JJ., McTiernan J. dissenting.

76 (1920) 28 C.L.R. 129.

which places a particular disability or burden upon an operation or activity of a State',[77] whilst Rich and Starke JJ. went further, extending the implied limitation to the Commonwealth laws which, although of general application and not confined to State governments, would prevent or impede the performance of 'normal and essential functions of government'.[78]

The parameters of the implied immunity doctrine have since been uncertain. Significant support for the broader interpretation adopted by Rich and Starke JJ. in the *State Banking* case subsequently emerged in *Victoria v. Commonwealth of Australia*[79] ('the *Pay-roll Tax* case')[80] and the *Tasmanian Dam* case,[81] before being comprehensively analysed in *Queensland Electricity Commission and Ors v. Commonwealth of Australia*[82] ('the *SEQEB* case'[83]). The *SEQEB* case has been described as 'important'[84] because the implied immunity doctrine was at last accorded unanimous[85] interpretation.

The *SEQEB* case involved a consideration of whether certain provisions of the Conciliation and Arbitration (Electricity Industry) Act 1985 (Cth), which was enacted to deal specifically with a dispute between the Electrical Trades Union of Australia and certain electricity authorities, was a valid exercise of Commonwealth power. The legislation was held to be invalid on the grounds, *inter alia*, that it discriminated against a State by imposing obligations not applicable to the general community. The obligation took the form of an admonishment to Queensland electricity authorities to, *inter alia*, settle industrial disputes as quickly as possible.

Mason J., for example, surmised that two elements to the doctrine emerged from the authorities:

> (1) the prohibition against discrimination which involves the placing on the States of special burdens or disabilities; and (2) the prohibition against laws of general application which operate to destroy or curtail the continued existence of the States or their capacity to function as governments.[86]

The significance of the doctrine in the present context is that any Commonwealth legislative initiative in the area of privacy, including any Commonwealth laws regulating the storage of computerised information, must be viewed in light of this implied limitation on legislative power, even if one accepts that the external affairs power is an appropriate head under which to enact such laws. If such laws place obligations on State governments in the handling of personal information which is stored in computerised form, one must consider whether this amounts to a discrimination against the capacity of the States to function as governments.

Logic and convenience would clearly favour the imposition by the Commonwealth of certain fundamental privacy obligations on all persons responsible for

77 (1947) 74 C.L.R. 31, 79.
78 *Ibid.* 66, *per* Rich J.
79 (1969) 122 C.L.R. 353.
80 Menzies, Walsh and Gibbs JJ.
81 Mason and Brennan JJ.
82 (1985) 159 C.L.R. 192.
83 The case arose from an attempt by the South East Queensland Electricity Board (SEQEB) to have installation work carried out by independent contractors instead of employees.
84 Current Topics, 'The Metes and Bounds of Commonwealth Legislative Power' (1986) 60 *Australian Law Journal* 55.
85 Gibbs C.J., Mason, Wilson, Brennan, Deane and Dawson JJ.
86 (1985) 159 C.L.R. 192, 217.

handling computerised personal information, whether those persons are in the Commonwealth or State public sectors, or in the private sector. This would, in the circumstances, be a law of general application, not a law applicable only to Commonwealth and State government agencies.

The *SEQEB* case involved a situation in which the legislation placed a special burden on a State. It did not involve a law of general application. It did not lead, therefore, to an analysis of the circumstances in which laws of general application will be considered to constitute an impairment of the proper functioning of government. Assuming, however, that the High Court would affirm the existence of the implied limitation in relation to laws of general application as described above, it would clearly be arguable that a law which obliged State government departments to observe certain security standards and grant certain access rights would amount to an interference with the administration of the State.

Again, logic and convenience would favour the implementation of nationally applicable information privacy principles, expressed in broad terms. These would be, quite simply, principles rather than regulations. Individual States would remain free to specify the manner of regulation and, in some instances, even the broad statements of principle would be expressed as being subject to the existence of State laws on the same subject-matter. It would be a bold determination of the High Court which invalidated a general application of such principles on the grounds that they operated to destroy or curtail the capacity of States to function as governments.

It must now be considered whether the Commonwealth, in implementing privacy-related legislation, has fully exploited its legislative competence. This leads to an inquiry as to Australia's participation in international treaties and agreements pursuant to which it has assumed responsibilities in the area of privacy.

As indicated above, there are two international agreements to which Australia is party and which bear relevance to the question of privacy.

First, the International Covenant on Civil and Political Rights provides, in Article 17:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to protection of the law against such interference or attacks.[87]

The Covenant was ratified by Australia on 12 August 1980,[88] subject to a number of reservations and a declaration in relation to Article 17 which reserved the right to compromise the privacy rights of individuals 'in the interests of national security, public safety, the economic well-being of the country, the protection of public health or morals, or the protection of the rights and freedoms of others'.[89]

The Convention is particularly important in the present context. It was described by the Australian Law Reform Commission in its report on 'Privacy'

[87] The text of the Convention appears in the Human Rights and Equal Opportunity Commission Act 1986 (Cth), Schedule 2. *Cf.* Universal Declaration of Human Rights, (1948) art. 12.

[88] The Covenant had been adopted by the General Assembly of the United Nations on 16 December 1966.

[89] *Australian Treaty Series* (1980) No. 23, annexure.

as 'especially significant'[90] in the quest for a definition of privacy and, indeed, the Law Reform Commission Act 1973 (Cth) obliges the Commission to ensure its law reform proposals are consistent with the articles of the Covenant.[91] It has proved, inevitably, to be one of the bases for the exercise of the Commonwealth external affairs power in the subsequent implementation of privacy legislation.[92]

The second international obligation of significance to the present discussion arises from Australia's membership of the O.E.C.D.[93] As indicated above, on 23 September 1980 the Council of the O.E.C.D. adopted the recommendations of an Expert Group concerning guidelines to be followed in relation to the protection of privacy and transborder flows of personal data.

Australia subsequently adopted the O.E.C.D. Guidelines in 1984. The guidelines are categorised under the following headings:

— Collection Limitation Principle
— Data Quality Principle
— Purpose Specification Principle
— Use Limitation Principle
— Security Safeguards Principle
— Openness Principle
— Individual Participation Principle
— Accountability Principle.

It will be observed below that the formulation of guidelines in relation to privacy practices is integral to the evolution of legislation for the protection of privacy interests. Guidelines provide a reference point against which subsequent legislative and administrative action can be assessed. The O.E.C.D. Guidelines have been described by the Australian Law Reform Commission as 'the most notable'[94] of various privacy recommendations by international bodies. The Commission emphasized that it was 'desirable that Australia's solutions to common problems should be so far as is possible compatible with those developed in countries with which Australia is inextricably involved and with which it shares common interests'.[95]

To what extent, then, do the International Covenant on Civil and Political Rights and the O.E.C.D. Guidelines support the enactment of privacy legislation based on the Commonwealth's external affairs power and, more specifically, legislation regulating the storage of computerized personal information in the private sector?

As indicated above, the International Covenant on Civil and Political Rights has treaty status and the only question is, therefore, whether its reference to 'privacy' is sufficient to justify particularized regulation of computerized data storage. Except in the case of international transborder data flows, the regulation

90 *A.L.R.C. Privacy Report*, *op. cit.* n. 6, para. 1032.
91 Law Reform Commission Act 1973 (Cth) s. 7(b).
92 This legislation, in the form of the Privacy Act 1988 (Cth), is discussed below.
93 For background information as to the formulation of the Guidelines, see Kirby, M. D., 'International Protection of Privacy and Controls over Transnational Data Flow' (1981) 55 *Australian Law Journal* 163.
94 *A.L.R.C. Privacy Report*, *op. cit.* n. 6, para. 587.
95 *Ibid.*

of data storages could fall outside the concept of 'general international concern' enunciated by Stephen J. in *Koowarta*'s case.[96] It would, however, fall comfortably within the concept of 'international character' espoused by Mason J. in the *Tasmanian Dam* case and, given the privacy implications of computerized databanks as discussed above, would be suitably consistent with the words and objects of the Convention.

In relation to the O.E.C.D. Guidelines, fewer difficulties would arise with regard to 'international character'[97] or the need for consistency of domestic legislation with the words and objects of the international agreement.[98] The real issue is whether the Guidelines, not having treaty status, nevertheless justify the use of the external affairs power. It has been argued above that they do.

(ii) *Commonwealth Privacy Reports*

Two reports have directly examined in some detail the need for Commonwealth legislation in the area of privacy. The Australian Law Reform Commission's Privacy Report dealt with a range of perceived privacy intrusions, including threats posed by the computerization of data.[99] The Senate Standing Committee's 'Report on the Feasibility of a National ID Scheme; the Tax File Number', published in 1988, was confined to a consideration of the implications of proposed Commonwealth legislation regarding the use of tax file numbers, but this led to a detailed consideration of the need for privacy legislation. Collectively, the reports are referred to here as the 'Commonwealth Privacy Reports'.

The Australian Law Reform Commission's Privacy Report was published in 1983. Under its Terms of Reference, dated 9 April 1976, the Australian Law Reform Commission was directed to report upon 'the extent to which undue intrusions into or interference with privacy arise or are capable of arising under the laws of the Commonwealth Parliament or of the Territories, and the extent to which procedures adopted to give effect to those laws give rise to or permit such intrusions or interferences'.[100] Although not confined to practices in the public sector, the Commission was directed to make particular reference to the extent to which the collection, recording or storage of information by Commonwealth

96 Note that in early 1979, the Australian Law Reform Commission acknowledged that implementation of Article 17 of the International Covenant on Civil and Political Rights might justify a new code of law governing, *inter alia*, privacy, although in this regard it 'may be dangerous to place much reliance on the Covenant at this stage': Commonwealth, Australian Law Reform Commission *Unfair Publication: Defamation and Privacy*, (1979), *op. cit.* n. 43, para. 337.

97 Note, in particular, that the preamble to the Guidelines recognizes that 'automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices': *op. cit.* n. 73, 7.

98 As the Guidelines do not specifically refer to criminal sanctions, a query might arise as to whether they would justify the extension of Commonwealth criminal offences beyond the federal public sector. However, the reference to 'lawful and fair means' in the Collection Limitation Principle (*ibid.* Part 2, 7) necessitates the creation of criteria to determine lawfulness and, hence, a legislative delineation between criminal and non-criminal practices.

99 Two earlier reports of the Australian Law Reform Commission addressed the then current state of Australian privacy laws in a relatively cursory fashion. Commonwealth, Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, (1979) 11 A.L.R.C. Pt III; Australian Law Reform Commission, *Privacy and the Census*, (1979) 12 A.L.R.C. paras 9-14.

100 Ellicott, R. J., Attorney-General (Cth), to the Law Reform Commission pursuant to the Law Reform Commission Act 1973 (Cth), Terms of Reference on the Matter of Privacy, (9 April 1976) para. (1).

or Territory departments constituted an undue interference with privacy[101] and to advise specifically on changes in the law which were required in order to provide protection against or redress for privacy intrusions arising out of interference with data storage systems.[102]

The Commission examined, *inter alia*, recent developments endangering privacy, with particular reference to the impact of technology. Information-processing technology was seen as significant in this regard,[103] the report noting that 'the informatics industry has brought enormous improvements and efficiencies which incidentally cause concern for privacy'.[104]

Taking account of concerns expressed by a number of bodies[105] the Commission concluded that there was a 'need for new laws bolstering existing protections of privacy interests' and that this was in part due to the 'extensive and expanding use of computers to process personal information in public and private administration'.[106]

The report rejected 'traditional legal remedies' as an effective means of protecting privacy interests.

> Because of the sensitive and personal nature of some complaints of privacy invasion, the traditional and proper openness of court procedures may dissuade even those with the necessary funds, patience and courage from pursuing the person who has interfered with their privacy.[107]

The Commission concluded that whilst statutory torts or crimes relating to 'interference with privacy' would be inappropriate, legislation would nevertheless be needed to establish standards and administrative mechanisms.[108] The report also urged that any such initiatives should be uniform with international standards: 'Australian information and protection of privacy laws should not be significantly different from those applied overseas'.[109]

It followed that the Commission strongly favoured the adoption by federal Parliament of a 'short legislative statement of basic principles by reference to which information practices could be assessed and complaints of interference with information privacy could be investigated by the Privacy Commissioner and other agencies'.[110]

The report recommended the adoption of information privacy principles, drawn primarily from the O.E.C.D. Guidelines, which were incorporated into a

101 *Ibid.* para. 1(a).
102 *Ibid.* para. 2(b)(i).
103 This was not regarded as the only development of relevance, however. Reference was made, for example, to developments in new surveillance technology: *A.L.R.C. Privacy Report*, *op. cit.* n. 6, paras 9-100. Note also the references to 'future technology and future risks', *ibid.* paras 119-133, including document facsimile transmission, optical fibre technology, satellite technology, radiated subscription television, telex and interactive information services, cable television and telephone-based systems.
104 *Ibid.* para. 118.
105 Specifically, the New South Wales Privacy Committee: *Ibid.* paras 135-6; the Commonwealth Ombudsman, *ibid.* para. 137; State Ombudsman, *ibid.* para. 138; the Australian Computer Society, *ibid.* para. 141; and the Committee of Inquiry into Technological Change *ibid.* para. 142.
106 *Ibid.* para. 143. Other factors were the extension of intrusive powers granted to officials, new and increasingly evasive business practices, and the rapid development of technological means for penetrating 'place' and 'space'.
107 *Ibid.* para. 1038.
108 *Ibid.* para. 1087.
109 *Ibid.* para. 1089.
110 *Ibid.* para. 1200.

schedule of the Commission's Draft Privacy Bill 1983. It was not proposed, however, that a breach of the privacy principles would be a criminal offence[111] or would give rise to civil compensation.[112]

It should be emphasized that the Draft Privacy Bill 1983 did not directly address computerized information. Clearly the formulation of the Information Privacy Principles was influenced by modern technological developments and these principles would have an impact upon the collection, use, disclosure and storage of electronic data, but they did not specifically relate to computerized information.

In one sense, the Australian Law Reform Commission's report on Privacy was to form the basis for future development of Commonwealth privacy initiatives. Nevertheless, legislative action was slow to unfold and was accompanied by a number of false starts. Before examining the Commonwealth legislative response, it is appropriate to examine the other Commonwealth privacy report of significance.

In October 1988, the Senate Standing Committee on Legal and Constitutional Affairs published its 'Report on the Feasibility of a National ID Scheme; the Tax File Number'.[113] In October 1987 the Senate had referred to the Committee a number of questions regarding, *inter alia*, the implications of the Australia Card Bill 1986 (Cth), the prospects of introducing comprehensive privacy legislation in Australia and the extent of personal data held on Australian citizens by Commonwealth government and private sector agencies and organizations.

Whilst it is not helpful to analyse the report in detail at this point, it should be noted that one chapter of the report was devoted to the subject of 'privacy'.[114]

There was little analysis of the notion of 'privacy' or the deficiencies exhibited at common law. It was acknowledged, however, that computerized information represented a significant threat to privacy interests:

> The explosion in computer technology, which has assisted in storage and accessing of data on a large scale, has provided undoubted benefits but has brought about the risk of widespread cross-referencing of data. These concerns, in addition to concerns about the accuracy and use of personal data, have brought the Committee to recommend that appropriate privacy legislation be enacted in Australia without further delay.[115]

Reservations were expressed by some members of the Committee, however, as to the desirability of extending privacy legislation to the private sector, both because of the perceived constitutional uncertainties as to the Commonwealth legislative power[116] and because regulation of the private sector 'would simply not yield benefits in any way commensurate with the costs of doing so'.[117] Due to this division of opinion, the Committee merely recommended that the 'question of the possible regulation of the private sector by privacy legislation be

111 *Ibid.* para. 1403.
112 *Ibid.* para. 1401.
113 Commonwealth, Senate Standing Committee on Legal and Constitutional Affairs, *Feasibility of a National ID Scheme; the Tax File Number* (1988) (*Senate TFN Report*).
114 *Ibid.* paras 7.1-7.76.
115 *Ibid.* para. 7.11.
116 *Ibid.* para. 7.14.
117 *Ibid.* para. 7.24. Proponents of this view considered that personal information held by the private sector was widely dispersed, generally held in much smaller databanks and less subject to linkage: *ibid.*

referred to the privacy watchdog, which the Committee recommends be established, for investigation'.[118]

The report is vulnerable to criticism in a number of respects. In particular, its failure to analyse adequately the extent and implications of data holdings in both the public and private sectors, and its failure to analyse closely the potential security risks involved in computerised information storages, was suggestive of a report prepared either in haste or in ignorance. The failure of Committee members to recommend unanimously privacy legislation in the private sector was regrettable and the consoling recommendation that the issue be referred to the proposed 'privacy watchdog' was uninspiring. Nevertheless, the report does represent an acknowledgement, albeit largely unsubstantiated, of the threat posed by computerization to the security of information storages, and the need for privacy legislation of some kind to facilitate regulation.

(iii) *Privacy Act 1988 (Cth)*

Privacy legislation was enacted by the federal government in 1988, after a false start in 1986.

The Privacy Bill 1986 (Cth) and the Privacy (Consequential Amendments) Bill 1986 (Cth) were drafted as cognate legislation to the Australia Card Bill 1986 (Cth), amidst public concern that the introduction of a national identification card would compromise the privacy of individuals. It was, in particular, feared by many that a computerized national databank would be created, facilitating both authorized and unauthorized access to personal information relating to Australian citizens. As one opponent of the Australia Card proposal stated in the House of Representatives:

> It is the unique capabilities of the computer age and of computers that make what the Government proposes so dangerous. The computer has a unique capacity to search, process and match information.[119]

The legislation was not specifically directed at computerized information. Nevertheless, the role of computers in gathering information was clearly a factor which influenced the drafting of the legislation in 1986, or at least influenced public concern which led to the drafting of the legislation:

> With the greater range of services being provided by the Government, the greater is the accumulation of personal information about individuals. More than anything else, the capacity of modern computers to search and process information offers the greatest potential for invasion of personal privacy by misuse.[120]

Accordingly, the privacy legislation was intended to

> regulate the collection, handling and use by Commonwealth departments and agencies of information about individuals so as to provide them with a level of privacy protection that is consistent with efficient Government administration.[121]

118 *Ibid.* para. 7.27.
119 Commonwealth, *Parliamentary Debates*, House of Representatives, 14 November 1986, 3136 (Mr Spender).
120 Commonwealth, *Parliamentary Debates*, House of Representatives, 23 October 1986, 2656 (Mr Bowen).
121 *Ibid.*

Subsequently the Australia Card legislation, together with the privacy legislation, was defeated in the Senate.[122] The government then developed, as a politically more acceptable alternative, the concept of the extended tax file number system. In 1988, Part VA of the *Income Tax Assessment Act* 1936 (Cth) was enacted, providing for the compulsory inclusion of tax file numbers in employment declarations[123] and compulsory disclosure in connection with certain forms of investment.[124]

The tax file number system was not an innovation, having been used in tax administration since 1936. The extended use of tax file numbers, however, was designed 'to improve the efficiency and effectiveness of the Australian Taxation Office's income matching system'[125] and meant that privacy concerns would still be aroused within the community and that the amendments would still have to be accompanied by privacy legislation perceived as effective. It was against this background that the Privacy Act 1988 (Cth), which received assent on 14 December 1988 and commenced on 1 January 1989, was introduced as cognate legislation to the Taxation Laws Amendment (Tax File Numbers) Act 1988.[126]

As intended with the unsuccessful Privacy Bill 1986, the Privacy Act was enacted pursuant to the Commonwealth's external affairs power and implements Australia's obligations under Article 17 of the *International Covenant on Civil and Political Rights* and the O.E.C.D. Guidelines. As with the 1986 Bill, the legislation avoided a definition of 'privacy' and instead established Information Privacy Principles based on the recommendations of the Australian Law Reform Commission, together with guidelines governing the collection, storage, use and security of tax file number information. Although not directed specifically at computerized information, the Act clearly embraces automated databanks.[127]

Although inspired by concerns over the use of tax file numbers, the Act also introduces privacy controls directed at Commonwealth agencies, subject to a number of specified exceptions.[128] The Act addresses 'interferences with privacy' which are deemed to occur if an act or practice of a Commonwealth agency breaches an Information Privacy Principle,[129] if there is a breach of the

122 For an encapsulation of the Opposition's attitude to the legislation, see the speech of Senator Baume, Commonwealth, *Parliamentary Debates*, Senate, 9 December 1986, 3591-5. For a broad analysis of the issues involved in the Commonwealth government's Australia Card proposal, see, *e.g.*, Marshall, 2 *Journal of Law and Information Science* 111.

123 Income Tax Assessment Act 1936 (Cth) Pt VA Div. 3.

124 Income Tax Assessment Act 1936 (Cth) Pt VA Div. 4.

125 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 September 1988, 860 (Mr Keating).

126 Note that on 5 June 1987, the Australian Democrats introduced a Privacy Protection Bill in the Senate. The Bill was intended principally for use 'as a basis for discussion and consultation': Commonwealth, *Parliamentary Debates*, Senate, 9 November 1988, 2271 (Senator Macklin).

127 *E.g.*, the definition of 'record' in s. 6(1) includes 'a database (however kept)' and the definition of 'personal information' includes 'information or an opinion forming part of a database'. Nevertheless, the definition of 'personal information' was still subject to criticism in the Senate on the basis that it did not include unique identifiers other than names or information which is computer linked to personal information: Commonwealth, *Parliamentary Debates*, Senate, 9 November 1988, 2271 (Senator Haines).

128 Privacy Act 1988 (Cth) s. (1).

129 The Information Privacy Principles are set out in s. 14.

tax file number guidelines relating to tax file number information[130] or (as a result of amendments introduced in 1991) if there is a breach of data-matching guidelines.[131] Pursuant to amendments which received assent in 1990 but have not yet been introduced, a credit reporting infringement will also amount to an 'interference with privacy'.[132] The legislation does not affect personal information in the private sector, except to the extent that tax file number information or credit information falls within that category.

It is not proposed to carry out a detailed examination of the Information Privacy Principles contained in the Act as this has been adequately addressed elsewhere.[133] In brief, the Act provides that a Commonwealth agency shall not do an act or engage in a practice which breaches one of the principles.[134] The Principles are formulated under the following headings:

— Manner and purpose of collection of personal information
— Solicitation of personal information from individual concerned
— Solicitation of personal information generally
— Storage and security of personal information
— Information relating to records kept by record-keeper
— Access to records containing personal information
— Alteration of records containing personal information
— Record-keeper to check accuracy *etc.* of personal information before use
— Personal information to be used only for relevant purposes
— Limits on use of personal information
— Limits on disclosure of personal information

As indicated above, the Act embraces the private sector in two respects: through the extended tax file number system; and, pursuant to amendments enacted in 1990 (but yet to come into effect), through its regulation of the credit industry.

The proposed credit industry regulation is discussed in more detail below in the context of the Privacy Amendment Act 1990 (Cth). With respect to tax file numbers, the Act specifies that tax file number recipients shall not do an act or engage in a practice breaching the guidelines relating to tax file number information.[135] Interim guidelines were initially set out in Schedule 2, to remain in force until formal guidelines had been issued by the Privacy Commissioner. Revised guidelines issued by the Commissioner became effective on 16 October 1990.

The tax file number guidelines are formulated under the following heads:

— General
— Use and disclosure of tax file number information
— Obligations of the Commissioner of Taxation

130 Section 17(1) requires the Privacy Commissioner to issue guidelines concerning the collection, storage, use and security of tax file number information.
131 Privacy Act 1988 (Cth) s. 13(ba).
132 *Ibid.* s. 13(d).
133 *E.g.*, Greenleaf, G., 'The Privacy Act 1988: Half a Loaf and Other Matters' (1989) 63 *Australian Law Journal* 116.
134 Privacy Act 1988 (Cth) s. 16.
135 *Ibid.* s. 18.

— Obligations of the Department of Social Security
— Collection of tax file number information
— Storage, security and disposal of tax file number information
— Incidental provision of tax file numbers
— Staff training
— Meaning of terms

Controversial features of the revised guidelines were the nomination of the Department of Social Security as an authorized tax file number information recipient, and the inclusion of the option of other government departments being authorized as recipients. It thereby became clear that tax file number information could be used for purposes far more extensive than originally indicated. Although guideline 1.1 states that 'the tax file number is not to be used as a national identification system by whatever means', and although its stated purpose is to simply improve the efficiencies in income tax collection, there remain significant grounds for concern over potential privacy infractions.

The Act creates the office of Privacy Commissioner[136] within the Human Rights and Equal Opportunity Commission. The Commissioner's functions are defined in relation to 'interferences with privacy', 'tax file numbers' and (since 1990) 'credit reporting' respectively. This introduces an immediate limitation on the scope of the Commissioner's powers: there is no general authority to investigate or publicize breaches of privacy other than those involving a possible breach of the Information Privacy Principles (including the data-matching provisions discussed below), the tax file number guidelines or credit reporting practices.

The Commissioner's functions in relation to 'interferences with privacy' include investigating alleged breaches of the Information Privacy Principles, examining (on request by a Minister) proposed legislation, promoting the Information Privacy Principles, providing advice, issuing guidelines[137] and encouraging corporations to develop programs for handling records of personal information in a manner consistent with the O.E.C.D. Guidelines.[138]

Similarly, with or without a request by a Minister or agency, the Commissioner's functions include the examination of proposals for data-matching or data-linkage 'that may involve an interference with the privacy of individuals'.[139] These provisions where initially described as 'exceedingly important because the rate at which technology is developing can mean many invasions of privacy quite uncontemplated'[140] at present.

136 *Ibid.* s. 19.
137 It was announced, for example, on 31 May 1989 that the Attorney-General had directed the Privacy Commissioner to develop a code of conduct for the credit industry: Mr Lionel Bowen, Press Release, 31 May 1989. Amendments to the Privacy Act, discussed below, were subsequently proposed by the government. Note also that in October 1990, the Commissioner published data matching guidelines.
138 Privacy Act 1988 (Cth) s. 27(1).
139 *Ibid.* s. 27(1)(k).
140 Commonwealth, *Parliamentary Debates*, House of Representatives 2 November 1988, 2246 (Mr Macphee).

The Act establishes an investigation process to be adopted by the Privacy Commissioner[141] and a procedure for issuing written determinations which may include the awarding of compensation for any loss or damage suffered as a result of a breach of privacy principles.[142] The power to award compensation is significant as the absence of a specific remedy in damages for data subjects was considered to be one of the principal defects of the Privacy Bill 1986.

The Act also enables the Commissioner to make public interest determinations in circumstances where it is considered that despite the fact that an act or practice of an agency may possibly breach an Information Privacy Principle, the public interest involved in the breach outweighs to a substantial degree the public interest in adhering to the Principle.[143] An agency may apply for such a determination[144] and a procedure is established for the publication of the application,[145] the drafting of a determination[146] and, if requested, a conference about the draft determination.[147]

(iv) *Privacy Amendment Act 1990 (Cth)*

In 1989, amendments were proposed to the Privacy Act which were intended to regulate the practices of credit reporting agencies and credit providers in relation to personal credit information.[148] The 1989 Bill lapsed with the dissolution of Parliament prior to the March 1990 federal election, but was subsequently restored to the Notice Paper on 1 June 1990 in the form of the Privacy Amendment Bill 1990. The Bill was passed on 20 December 1990 and received Royal Assent on 24 December, 1990 but, as stated above, is yet to come into force.

The Privacy Amendment Act is significant not only as a manifestation of governmental concern over credit reporting practices, but also as an indication of the extent to which the Privacy Act can be applied to the private sector, even if one takes a narrow view of the Commonwealth's legislative competence in relation to privacy.[149] In this instance, the Commonwealth has relied upon the corporations power in s. 51 (xx) of the Constitution and, to a lesser extent, the trade and commerce power in s. 51 (i), the posts and telegraphs power in s. 51 (v) and the banking power in s. 51 (xiii). The drafting process has also emphasized, however, the cumbersome approach to legislation which is required

141 Privacy Act 1988 (Cth) ss 36-47.
142 *Ibid.* ss 52(1) and (2).
143 *Ibid.* s. 72.
144 *Ibid.* s. 73(1).
145 *Ibid.* s. 74.
146 *Ibid.* s. 75.
147 *Ibid.* ss 76 and 77. For criticism of this provision, see Greenleaf, G., 'The Privacy Act 1988: Enforcement and Exemptions' (1989) 63 *Australian Law Journal* 285, 286-7.
148 The Privacy Amendment Bill 1989 (Cth) was introduced into the Senate on 16 June 1989: Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4215-6. It was subsequently amended 'following wide consultation': Press Release, Senator Bolkus, 5 October 1989. The Bill was reintroduced on 22 December 1989 and then referred to Committee.
149 The Privacy Commissioner described the first draft of the Bill as 'significant for privacy protection in Australia in that it involves the first possible extension of the Privacy Act to cover a major private sector industry': Privacy Commissioner, *First Annual Report, on the Operation of the Privacy Act* (1989) 15.

if one does not subscribe to the view that the Commonwealth has considerable powers to legislate for privacy pursuant to s. 51 (xxix), the external affairs power.

The Act now, as a result of the amendments, addresses the activities of 'credit reporting agencies' and 'credit providers'. A credit reporting agency is defined essentially as a corporation which keeps records of personal information which are provided to others regarding credit eligibility, credit history or repayment capacity of natural persons, as opposed to corporations.[150] A credit provider is, essentially a building society, credit union or bank involved in the provision of loans.[151] Reflecting the Commonwealth's inability to interfere with State affairs, State banks not involved in interstate activity are excluded.[152] The Act then proceeds to address the activities of credit reporting agencies when carrying on a 'credit reporting business'.[153]

The Act contemplates a Code of Conduct relating to credit information files and credit reports, to be issued by the Privacy Commissioner.[154] Credit reporting agencies and credit providers are prohibited from doing any act or engaging in any practice which breaches the Code. The Code will be devised after consultation with 'government, commercial, consumer and other relevant bodies and organizations'.[155]

In addition, the legislation introduces a number of specific provisions which regulate the handling of 'credit information files' and 'credit reports'.[156] Under s. 18E, credit information files will now be restricted to information which is reasonably necessary to service a credit application, with obligations and restrictions being placed upon both credit reporting agencies and credit providers in this regard. Matters such as political affiliations, criminal records and character assessments must be excluded. A 'maximum permissible period' of five to seven years is introduced in s. 18F for the retention of information on credit information files, the precise period varying with the type of information contained in the file.

Obligations are placed on credit reporting agencies and credit providers to ensure, in the case of credit information files or credit reports as the case may be, that the contents are accurate, up to date and complete, and that they are protected by appropriate security safeguards.[157] Credit reporting agencies and credit providers are required to take reasonable steps to allow access by subjects to credit information files and credit reports, with rights of alteration and notation being specified.[158]

150 Privacy Act 1988 (Cth) ss 5(b) and 11A.
151 *Ibid.* s. 11B.
152 *Ibid.* s. 12A.
153 See definition in Privacy Act 1988 (Cth) s. 5(b). The definition excludes information which is publicly available and is restricted to information retained for the purpose of advising in relation to credit eligibility, credit history or credit repayment capacity.
154 *Ibid.* s. 18A. The Code will be a 'major feature of the regulatory scheme for the consumer credit reporting industry': Commonwealth, *Parliamentary Debates*, Senate, 16 June 1989, 4217 (Senator Richardson), commenting on the Privacy Amendment Bill 1989 (Cth).
155 *Ibid.* s. 18A(2).
156 For definition of 'credit information file' and 'credit report', see Privacy Act s. 5(b).
157 Privacy Act 1988 (Cth) s. 18G.
158 *Ibid.* ss 18H and 18J.

Under ss 18K, 18L and 18M, credit reporting agencies and credit providers are restricted as to when and to whom they can disseminate and use the information, with accurate records being kept of authorized disclosures and particulars being provided by credit providers to applicants as to the basis of a refusal of an application by an individual for credit.

It will now be an offence for credit reporting agencies or credit providers to provide a false or misleading credit report;[159] it will also be an offence for any person to obtain unauthorized access to credit information files or credit reports or to obtain access by a false pretence.[160]

The powers of the Privacy Commissioner are extended to ensure he or she can investigate acts or practices of credit reporting agencies or credit providers which may constitute a credit reporting infringement. The Commissioner will also undertake a range of other functions necessary to ensure compliance with the Code of Conduct and, generally, to promote the security and accuracy of personal information contained in credit information files.[161]

(v) *Data-matching Program (Assistance and Tax) Act 1991 (Cth)*

Anticipating adverse public reaction to the extended use of tax file number information as announced in the August 1990 Budget, the government introduced the Data-matching (Assistance and Tax) Bill into the Senate on 15 November 1990. The legislation, which further amends the Privacy Act, was subsequently passed on 20 December 1990 in the form of the Data-matching Program (Assistance and Tax) Act.[162] It received assent and came into force on 23 January 1991.

The Act seeks to regulate data-matching as between the Department of Community Services and Health, the Department of Employment, Education and Training, the Department of Social Security and the Department of Veterans' Affairs by imposing steps to be followed in 'data-matching cycles'. Section 5(2) provides that an agency will not be in breach of the Tax File Number Guidelines in the Privacy Act so long as it complies with the data-matching provisions as set out.

Pursuant to s. 6, no more than nine 'data-matching cycles' are permitted in any one year and only one matching cycle is to be in progress at any one time. These 'cycles' represent a six-step procedure prescribed by s. 7, pursuant to which the sequences to be followed by 'source agencies', 'matching agencies' and 'assistance agencies'[163] in searching for discrepancies in information supplied by or relating to taxpayers or recipients of relevant government benefits are set out.

The Act attempts to prevent unrestrained matching or the creation of a *de facto* computer databank or both. Under s. 8, for example, transfer of data between agencies by on-line computer connections is prohibited; under s. 10, 'source

159 *Ibid.* s. 18R.
160 *Ibid.* ss 18S and 18T.
161 *Ibid.* s. 28A.
162 No. 20 of 1991.
163 For definitions of these terms, see Data-matching Program (Assistance and Tax) Act 1990 s. 3.

agencies' which have obtained information through a data-matching program but which have not made a decision to examine or investigate that information within 90 days must destroy the data. The actual examination or investigation must be completed within 12 months of receipt of the data.

With certain exceptions, an agency must provide persons with 21 days' notice that, pursuant to information obtained through the data-matching program, it intends to amend benefits or issue a tax assessment or amended assessment.[164]

Agencies involved in data-matching programs are required to comply with data-matching guidelines issued by the Privacy Commissioner and, until these have been issued, interim guidelines appended to the Act are to be followed.[165] The Privacy Commissioner's guidelines are to be issued by 30 September 1991.[166]

The Privacy Commissioner is specifically given the power to investigate breaches of the guidelines.[167] Although direct powers of enforcement are limited as the Commissioner can only make recommendations to the Minister,[168] the act further provides that a breach of the data-matching procedures also constitutes a breach of the Privacy Act,[169] thereby triggering the more assertive powers of investigation and determination already possessed by the Commissioner.

The rationale for implementing the legislation, which has a two-year sunset clause,[170] is that major social security and taxation fraud can be eliminated by matching data on income, family structure and tax file numbers. For many, however, this is a manifestation of earlier fears that the Australia Card would lead the creation of a government-controlled computer dossier on all citizens.

(iv) *Conclusion Regarding Privacy Act*

The Privacy Act has been praised for its flexibility:

> The Act allows the Commissioner, individual citizens, the courts, and even the Parliament each to 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.[171]

In reality, however, the Act represents only a tentative approach to the protection of computerized data specifically. There is an apparent lack of willingness to embrace comprehensively the private sector and, as a result, the Act fails to implement a truly national privacy protection scheme. The entire legislative experience is hence open to the not uncharitable criticism that it has been largely a political exercise lacking in either adequate forethought or genuine intent.

At a more specific level, there appears to have been inadequate recognition of the threats to privacy posed by the computerization of personal information. As emphasized above, computerized data storages pose unique threats which, it

164 *Ibid.* s. 11.
165 *Ibid.* s. 12(1).
166 *Ibid.* s. 12(2).
167 *Ibid.* s. 13(2).
168 *Ibid.* s. 13(4).
169 *Ibid.* s. 14(1).
170 *Ibid.* s. 21.
171 Greenleaf, G., 'The Privacy Act 1988: Enforcement and Exemptions', (1989) 63 *Australian Law Journal* 285, 287.

is argued, cannot adequately be dealt with by broadly expressed privacy legislation intended to embrace manually stored data as well.

(vii) *Freedom of Information Legislation*

The Commonwealth, along with some States and Territories, has enacted freedom of information legislation which, as indicated above, is an integral part of any data protection scheme. The Commonwealth legislation is discussed in more detail below.

(b) *State Initiatives*

There have been various initiatives — *ad hoc* and inconsistent — undertaken at State level which have been directed at preserving privacy rights of individuals. A majority of these initiatives have not been concerned specifically with the regulation of computerized databanks but, nevertheless, most have been inspired wholly or in part by community concern over the implications of computerized information storages.

These initiatives can be divided into three categories: first, report of State-appointed committees charged with examining privacy related issues; second, certain legislative proposals (including unsuccessful Bills); third, voluntary guidelines which have been issued or proposed at State level as a possible substitute for statutorily entrenched privacy principles.

(i) *Reports*

There have been numerous reports issued over the past two decades, some of more significance than others.

New South Wales

In 1972 the Minister of Justice for New South Wales, in accordance with a resolution of the Standing Committee of Commonwealth and State Attorneys-General, referred a study to Professor W. L. Morison on the question of the protection of the privacy of individuals, having regard to the increased means of collecting, storing, retrieving and disseminating information. The resultant report[172] was completed on 27 February 1973.

Although not concerned solely with the implications of the computerization of information, the Morison Report acknowledged computerization as one source of privacy concerns. It nevertheless strenuously resisted the notion of any legislative initiative which would distinguish computerized information from information stored in other forms.[173]

The report concluded that whilst legislative intervention in the broad area of privacy protection was desirable, this should be limited to the creation of a statutory body. The body would be charged with gathering information and

[172] New South Wales, Morison, W. L., *Report on the Law of Privacy* (1973) (*Morison Report*).
[173] *Ibid.* paras 94, 107 and 115.

recommending legislation in the general area of privacy law reform and in the numerous specific areas of privacy concern (including data collection) outlined in the report. The recommendation led to the creation of the New South Wales Privacy Committee, discussed below.

Ideally, the report suggested, privacy bodies would be established federally and in all States, drawing membership from a cross-section of the community and establishing sub-committees to consider specific privacy issues (again including data collection). A data collection sub-committee should deal with the 'general issues raised by data collections for privacy and with specific complaints in relation to the operation of data collections where these have not been made the subject of consideration by a sub-committee in a particular area of data collection'.[174] Legislation should provide for ministerial regulation of privacy committee powers.

Western Australia

In Western Australia, the Minister for Justice established on 20 November 1975 a Committee to Examine Issues Relating to Privacy and Data Banks. The Committee was chaired by the Commissioner of the Public Service Board, K. E. Mann, and it published its report ('the Mann Report') on 30 March 1976.[175]

The Committee was directed to confine its enquiries to information held by government departments, instrumentalities and hospitals, unlike the Morison Report which dealt with the question of privacy generally. Like the Morison Report, however, the Mann Report was not confined to issues arising out of computerized information (the term 'data bank' was to also embrace 'microfilm records and all types of manual records'[176]) but inevitably discussed the implications of the computerization of personal information.

On the subject of computers specifically, the Committee 'found no evidence of improper use of computers with respect to privacy in the Government sector in Western Australia'[177] and could identify no difference in the 'inherent dangers of computers with respect to privacy' when compared with manual recording systems.[178] There were, however, certain 'practical implications' of computerized recording systems.

In addition to proposing guidelines for determining the use and availability of personal information,[179] the report concluded by recommending that the Western Australian Parliamentary Commissioner should, with the assistance of a part-time committee, perform in the government area the role proposed in the Morison Report for a privacy body.[180] It was further envisaged that such a committee 'could provide valuable experience for the creation, if and when that is thought desirable — of a larger body to be concerned with the whole area of

174 *Ibid.* para. 107.
175 Western Australia, *Report of the Committee to Examine the Question of Privacy and Data Banks* (1976) (*Mann Report*).
176 *Ibid.* para. 4(b).
177 *Ibid.* para. 108.
178 *Ibid.* para. 110.
179 The guidelines are discussed further below.
180 *Mann Report*, *op. cit.* n. 175, para. 142.

privacy in the way that Morison envisages'.[181] The recommendation was not, however, acted upon.

South Australia

In South Australia, three reports of significance were produced, in 1973, 1980 and 1987.

The Law Reform Committee of South Australia produced an 'Interim Report Regarding the Law of Privacy'[182] in 1973 and a 'Report Regarding Data Protection'[183] in 1980. The Privacy Committee of South Australia published a discussion paper entitled 'Privacy: a Review and Proposals for Reform'[184] in 1984 followed by a final report[185] in 1987.

The 1973 report acknowledged the threat to privacy posed by computer databanks, recommended the creation of a general right of privacy and recommended the introduction of controls on the recording, storing, retrieval and dissemination of data. The 1980 report recommended that South Australia should adopt the recommendations of the Lindop Committee which provided the foundation for the proposed English Data Protection Act, save that, unlike the English legislation which was to materialize in 1984, it would not be confined to computerized data. The 1987 report again recommended the regulation of both manual and automated information storage systems and the implementation of information privacy principles governing both the public and private sectors — unlike the recommendations of the previous reports, however, the recommendations of the 1987 report have since been implemented in part.

Victoria

In Victoria, the Legal and Constitutional Committee has published two papers which bear relevance to the concept of privacy as legal right.

In 1987, it published its 'Report on the Desirability or Otherwise of Legislation Defining and Protecting Human Rights'.[186] In 1990, it published its 'Report upon Privacy and Breach of Confidence'.[187]

The 1987 report considered the desirability of State Parliament enacting legislation defining and protecting human rights in Victoria. The report recommended the adoption of an unenforceable declaration of rights and freedoms and does not warrant further discussion at this point. The 1990 report concentrated on the deficiencies of the law of breach of confidence but incidentally recommended

181 *Ibid.* para. 145.
182 South Australia, Law Reform Committee, *Interim Report Regarding the Law of Privacy* (1973).
183 South Australia, Law Reform Committee, *Fiftieth Report: Regarding Data Protection* (1980).
184 South Australia, Privacy Committee, *Privacy: a Review and Proposals for Reform* (1984).
185 South Australia, Privacy Committee, *Report to the Attorney-General of South Australia* (1987).
186 Victoria, Legal and Constitutional Committee, *Report on the Desiribility or Otherwise of Legislation Defining and Protecting Human Rights* (1987).
187 Victoria, Legal and Constitutional Committee, *Report on Privacy and Breach of Confidence* (1990).

the introduction of comprehensive data protection legislation of Victoria.[188] Subsequently, on 17 August 1990, the Victorian Attorney-General referred the matter to the Victorian Law Reform Commission, requesting the provision of a further report on the subject, including a draft Bill to implement the Commission's recommendations.

(ii) *Legislative Initiatives*

State legislative initiatives fall into three categories — legislation specifically addressing the right of privacy, legislation regulating the activities of credit bureaux and legislation introducing a statutory privacy guardian. It is not proposed here to analyse the contents of these initiatives but rather to outline the framework within which they have been enacted, thereby emphasizing the *ad hoc* nature of the initiatives and the inevitability of inconsistency.

Privacy legislation

With respect to privacy legislation, the first initiative came in Victoria in the form of the Information Storages Bill 1971, a private member's bill which unsuccessfully sought to introduce a form of freedom of information. The Bill was inspired by the perceived advent of the computer age, although its subject matter was not so confined. The Bill was subsequently rejected in a report from the Victorian Statute Law Revision Committee in 1975.[189]

In Tasmania, an attempt to introduce privacy legislation in 1974 proved unsuccessful when the Privacy Bill 1974 was referred to a joint committee of the Tasmanian Parliament. The deliberations of the Committee ceased when parliament was prorogued later that year.

Similarly, in South Australia, a Privacy Bill was introduced into the House of Assembly on 10 September 1974 but was defeated on second reading in the Legislative Council on 20 November 1974.

Both the Tasmanian and South Australian bills sought to introduce a right of privacy, the principal difference being that the Tasmanian bill refrained from defining the concept of 'privacy'.

A more successful initiative took place in South Australia in 1989 when a Cabinet Administrative Instruction came into effect,[190] implementing the recommendations of the South Australian Privacy Committee Report of 1987, discussed above. This is, of course, not a 'legislative' initiative as such but it does provide evidence that a significant degree of information privacy, at least in the public sector, can be achieved at State level. The Instruction sets out

[188] Victoria, Legal and Constitutional Committee, *Report upon Privacy and Breach of Confidence* (1990) 47.

[189] Victoria, Statute Law Revision Committee, *Report upon the Proposals Contained in the Information Storages Bill 1971 together with Extracts from the Proceedings of the Committee and an Appendix* (1975). The Report was tabled in the Victorian Legislative Assembly on 11 November, 1975: see Victoria, *Parliamentary Debates*, Legislative Assembly, 11 November 1975, 8314.

[190] No. 1 of 1989.

information privacy principles[191] governing acts and practices involving 'personal information' and is based on the information privacy principles formulated by the Australian Law Reform Commission.

Finally, in Western Australia, the Opposition introduced a Data Protection Bill into the Legislative Assembly on 12 October 1988, seeking to replicate the English Data Protection Act 1984 and thereby addressing directly and exclusively the problems posed by computerized information banks. Subsequently, on 13 August 1990, the Western Australian government announced an intention to introduce legislation to 'protect personal information held by government bodies' but to date no legislation has been drafted. Clearly, the problems posed by information banks (including computerized information banks) have been recognized in Western Australia and an initiative of some sort can be anticipated in the not too distant future.

Credit bureaux regulation

It was noted earlier that credit bureaux regulation has long been a source of concern to the community and has prompted Commonwealth intervention. It need only be indicated here that, at State level, initiatives to regulate the credit bureaux industry — as a direct result of the threats of computerization — had previously emerged in the form of the Invasion of Privacy Act 1971-81 (Qld),[192] the Fair Trading Act 1987 (S.A.)[193] and the Credit Reporting Act 1978 (Vic.).[194]

(iii) *Statutory privacy guardians*

The Privacy Committee Act 1975 (N.S.W.)[195] embodied the essential recommendations of the Morison Report, formalizing the establishment of the New South Wales Privacy Committee and defining the scope of the Committee's activities.

The Committee's activities include researching any matters relating to the privacy of persons, making reports and recommendations regarding the desirability of legislative or administrative initiatives, making reports and recommendations to individuals regarding the privacy interests of other persons, investigating complaints about violations of privacy, disseminating information and undertaking educational work relating to privacy.[196] One significant contribution of the Committee was to be the initial publication in 1977 and subsequent formalization in 1986 of its 'Guidelines for the Operation of Personal Data Systems'.[197]

In Queensland, the Privacy Committee Act 1984 sought to replicate the New South Wales Privacy Committee although the Act differs from the New South

191 Information Privacy Principles Instruction (S.A.), Pt II.
192 No. 50 of 1971, as amended.
193 No. 42 of 1987, superseding the Fair Credit Reports Act of 1974-5 (S.A.).
194 No. 9151 of 1978.
195 No. 37 of 1975, amended by No. 218 of 1986 and No. 48 of 1987.
196 Privacy Committee Act 1975 (N.S.W.) s. 15(1).
197 New South Wales, Privacy Committee, BP. 31 (1986).

Wales Act in a number of important respects, particularly in relation to the powers and functions of the respective committees.

Finally, in South Australia a Privacy Committee was constituted by proclamation in 1989.[198] The Committee's functions include advising the Attorney-General on the need for legislation or administrative action to protect individual privacy, publishing information as to appropriate methods of privacy protection, monitoring the information privacy principles,[199] monitoring access to personal records,[200] improving access to government records for research purposes, referring written complaints concerning violations of individual privacy to 'appropriate' authorities and carrying out 'such other functions as are determined by the Attorney-General'.[201]

(c) *Freedom of Information Laws*

As stated above, one fundamental aspect of the traditional concept of privacy is the right to have access to information which is stored about oneself, and the right to amend that information if it is inaccurate or misleading.

This right is embraced, for example, by the 'Individual Participation Principle' contained in the O.E.C.D. Guidelines according to which an individual should have the right:

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him
  (i) within a reasonable time;
  (ii) at a charge, if any, that is not excessive;
  (iii) in a reasonable manner; and
  (iv) in a form that is readily intelligible to him;
(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
(d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

More recently, this principle has been reflected in the Privacy Act 1988 (Cth) in the form of Information Privacy Principles 6 and 7.

Rights of access to and amendment of personal information are addressed, to some extent, by Commonwealth freedom of information legislation, by State legislation in Victoria and New South Wales, by ordinance in the Australian Capital Territory and by Cabinet Administrative Instruction in South Australia.[202]

198 South Australia, Privacy Committee of South Australia, *S.A. Govt Gazette*, 6 July 1989, p. 6 (*South Australian Privacy Committee Proclamation*).
199 The information privacy principles are referred to above.
200 The administrative freedom of information scheme in South Australia is discussed below.
201 *South Australian Privacy Committee Proclamation*, *op. cit.* n. 198, para. 2.
202 Note that it has been recommended in Queensland that an Electoral and Administrative Review Commission be established and that it conduct, *inter alia*, an 'investigation into Freedom of Information legislation and its desirability': Queensland, *Report of Commission of Inquiry into Possible Illegal Activities and Associated Police Misconduct* (1989) para. 3.11.2 ('*Fitzgerald Report*). Note also that freedom of information legislation has been foreshadowed in Western Australia: Media Statement, Premier Carmen Lawrence, 13 August 1990.

The Freedom of Information Act 1982 (Cth) (the 'Commonwealth Act')[203] came into operation in December 1982[204] and has since been the subject of considerable amendment.[205] The Freedom of Information Act 1982 (Vic.) (the 'Victorian Act')[206] came into force in July 1983 and has also been the subject of subsequent amendment.[207] The Freedom of Information Ordinance 1989 (A.C.T.)[208] commenced in May 1989[209] and the Freedom of Information Act 1989 (N.S.W.)[210] (the 'New South Wales Act') came into force in July 1989. The South Australian Administration Instruction also came into effect on 1 July 1989.

It should be emphasized that despite the conceptual connection between freedom of information legislation and the fundamental privacy rights of individuals, neither the Commonwealth nor the State Acts were enacted as an express response to concerns about the privacy rights of information subjects. It should also be emphasized that the legislation relates only to government-held information, whether in manual or computerized form.

As a qualification of the general right of access granted by the legislation,[211] a number of documents are exempted from the process in each jurisdiction.

Part IV of the Commonwealth and Victorian Acts[212] and schedule 1 of the New South Wales Act list the documents which are subject to exemption. The nature and extent of these exemptions is critical to an assessment of the implications of the legislation on the privacy of individuals.

Exemption *per se* is not necessarily inconsistent with the protection of privacy:

> A regime under which anyone can inspect a public sector document clearly has potential for invading 'information privacy' — the claim of the individual to control the dissemination of personal information about himself. Government departments and agencies hold vast amounts of information, much of which is extremely sensitive, about most Australians.[213]

203 For a general commentary on the Commonwealth Act, see Pearce, D. C. (ed.), *The Australian Administrative Law Service* (1979) Ch. 7; Pearce, D. C., *Commonwealth Administrative Law* (1986), Ch. 7; Flick, G. A., *Federal Administrative Law* (2nd ed. 1984) 2001ff; Bayne, P. J., *Freedom of Information* (1984); Aronson M., and Franklin, N., *Review of Administrative Action* (1987) Ch. 12.

204 Freedom of Information Act 1982 (Cth) s. 2.

205 See, *e.g.*, Australian Broadcasting Corporation (Transitional Provisions and Consequential Amendments) Act 1983 (Cth), Freedom of Information Amendment Act 1983 (Cth), Public Service Reform Act 1984 (Cth), Australian Trade Commission (Transitional Provisions and Consequential Amendments) Act 1985, Intelligence and Security (Consequential Amendments) Act 1986, Freedom of Information Laws Amendment Act 1986 (Cth), Privacy Act 1988 (Cth).

206 For a general commentary on the Victorian Act, see Kyrou, E. J., *Victorian Administrative Law* (1985) 501ff.

207 See, *e.g.*, Public Service (Amendment) Act 1984 (Vic.), Statute Law Revision Act 1984 (Vic.), Administrative Appeals Tribunal Act 1984 (Vic.), Adoptions Act 1984 (Vic.), Infertility (Medical Procedures) Act 1984 (Vic.).

208 No. 46 of 1989.

209 The Ordinance largely mirrors the Commonwealth Act, and will therefore not be given independent consideration in this article.

210 A Freedom of Information Bill was first introduced into the House of Assembly on 2 June 1988. The process of public consultation then took place before the legislation was introduced on 10 November 1988. For a review of this process, and the amendments made as a result, see New South Wales, *Parliamentary Debates*, House of Assembly, 10 November 1988, 3162-6.

211 Freedom of Information Act 1982 (Cth) s. 11; Freedom of Information Ordinances 1989 (A.C.T) s. 10; Freedom of Information Act 1982 (Vic.) s. 13; Freedom of Information Act 1989 (N.S.W.) s. 16.

212 Freedom of Information Act 1982 (Cth) ss 32-47; Freedom of Information Ordinances 1989 (A.C.T.) ss 32-47; Freedom of Information Act 1982 (Vic.) ss 28-38.

213 *A.L.R.C. Privacy Report*, *op. cit.* n. 6, para. 987. The report further observes that if information were made generally available by governments, Principle 10 of the O.E.C.D. Guidelines ('Use

Some documents are excluded because they are in the possession of authorities which are completely exempt from the operation of the Act.[214] Other documents may be excluded by virtue of their contents.[215]

There are three grounds for exemption in particular which are fundamental to striking a balance between the right of the community to gain access to information, and the right of information subjects to keep some information free from intrusion. These involve documents relating to business affairs,[216] documents relating to personal affairs[217] and documents containing information obtained in confidence.[218]

Another important aspect of freedom of information legislation is the right to amend personal records. Both the Commonwealth and State legislation contain provisions[219] for the amendment of personal records by the information subject. These measures are clearly consistent with any perception of fundamental privacy rights.[220]

Although the principal purpose of the amendment provisions is to ensure that personal files are accurate for the benefit of persons with authorized access to those records, they have the incidental positive effect of increasing the likelihood that information extracted without authority will also be accurate. Whilst this is not one of the stated intentions of the measures, it is important in the context of computerized databanks of information which are significantly more susceptible than manual record systems to the threat of unauthorized access.

Finally, it should be indicated that freedom of information rights were introduced in South Australia by Cabinet Administrative Instruction, effective from 1 July 1989.[221]

Limitation Principle') would be breached. It has been suggested that the exemptions in the Commonwealth Act are 'the necessary minimum counterbalance to the radical innovation of granting a general curiosity right to official information': Rose, A. D., 'Exemptions Under the Freedom of Information Act: An Official's Viewpoint' (1983-4) *Federal Law Review* 137, 142.

214 Freedom of Information Act 1982 (Cth) s. 4(1) (definitions of 'agency' and 'prescribed authority') and s. 7 (reference to Schedule 2); Freedom of Information Ordinances 1989 (A.C.T.) s. 6; Freedom of Information Act 1982 (Vic.) ss 5, 6; Freedom of Information Act 1989 (N.S.W.) Schedule 2.

215 It should be noted that Ministers and agencies can, at their discretion, grant access to an exempt document: Freedom of Information Act 1982 (Cth) s. 14; Freedom of Information Act 1982 (Vic.) s. 16; *cf.* Freedom of Information Act 1989 (N.S.W.) s. 5(4).

216 Freedom of Information Act 1982 (Cth) s. 43; Freedom of Information Ordinances 1989 (A.C.T.) s. 43; Freedom of Information Act (Vic.) s. 34; Freedom of Information Act (N.S.W.) s. 25.

217 Freedom of Information Act (1982) (Cth) s. 41; Freedom of Information Ordinances 1989 (A.C.T.) s. 41; Freedom of Information Act 1982 (Vic.) s. 33; Freedom of Information Act 1989 (N.S.W.) schedule 1, cl. 6(1).

218 Freedom of Information Act 1982 (Cth) s. 45; Freedom of Information Ordinances 1989 (A.C.T.) s. 45; Freedom of Information Act 1982 (Vic.) s. 35; Freedom of Information Act 1989 (N.S.W.) schedule 1, cl. 13.

219 Freedom of Information Act 1982 (Cth) Part V; Freedom of Information Ordinances 1989 (A.C.T.) Part V; Freedom of Information Act 1982 (Vic.) Part V; Freedom of Information Act 1989 (N.S.W.) Part 4.

220 It is interesting to note the observation, in this context, that whilst the Commonwealth Act has been 'spectacularly successful in providing access to personal information', there has nevertheless been 'little call for correction of errors in these personal records': Bell, R. H., 'Freedom of Information: the Commonwealth Experience' (1988) 47 *Australian Journal of Public Administration* 296, 301.

221 South Australia, Cabinet Administrative Instruction No. 2 (1989), *Access to Personal Records Instruction*.

The substantive provisions of the Instruction relating to rights of access and amendment are based on the Victorian Act. In essence, the Instruction provides 'every person' with a right of access to records of 'agencies'[222] upon written request.[223] Various classes of records are exempted by Part III of the Instruction[224] and these exemptions include records affecting personal privacy,[225] records relating to trade secrets and other commercial information,[226] and records containing material obtained in confidence.[227] In each case, the exemption adopts the wording of the Victorian Act. Part IV of the Instruction addresses rights of amendment of personal records and, again, is based directly on the Victorian legislation.

It must be acknowledged that freedom of information laws and practices in any form serve a useful purpose. It may be regrettable that such rights as exist are confined to the public sector, and it may be regrettable that administrative difficulties have emerged and in some instances have not been rectified, but nevertheless those jurisdictions which have the benefit of freedom of information practices clearly provide a greater recognition of the privacy rights of individuals than those jurisdictions which do not.

The most significant adverse implications of existing Australian freedom of information practices are, arguably, their inconsistency and their non-universality. The inconsistencies are disappointing because they exemplify the difficulties inherent in achieving uniform legislation of any nature. The non-universality of freedom of information legislation is even more disturbing, as it shows a lack of philosophical commitment by all Australian jurisdictions to this aspect of privacy recognition and protection. The negative aspects of non-universality are exaggerated by the fundamental difference in approach between South Australia, on the one hand, and the jurisdictions which have legislated for freedom of information on the other.

In the context of the regulation of personal information stored on computers, one can only conclude that such *ad hoc* regulation as exists in Australia is more satisfactory in those jurisdictions where legislation exists. Unfortunately, the widespread non-implementation of freedom of information legislation indicates that it is unlikely that future uniform legislation to regulate the flow of information, in computerized or other form, will ever be achieved in this country.

E. *Conclusions and Suggestions*

The above analysis demonstrates numerous instances in which the existing legal regulation of computerized information banks is, for a variety of reasons, deficient. Clearly, consistent national legislation would provide the most effective response to this deficiency. It is therefore necessary to consider the

222 *Ibid.* cl. 5. For a definition of 'agency', see *ibid.* cl. 3(1).
223 *Ibid.* cl. 8.
224 *Ibid.* cls 19-31.
225 *Ibid.* cl. 24.
226 *Ibid.* cl. 25.
227 *ibid.* cl. 26.

substantive requirements of any such regulatory scheme and, in turn, it is necessary to consider what is to be protected under such a scheme.

Above all, persons about whom information is stored electronically require an acknowledged right of privacy in relation to that information. It is not a satisfactory rebuttal to assert that electronic data subjects are conceptually no different from manual data subjects. The nature of the threat to privacy is itself unique.

The case for national statutory entrenchment of such a privacy right is strengthened by the reality that intrusions involving telecommunication links can be effected with relative ease across jurisdictional boundaries. It follows that Commonwealth legislation of far broader application (and more specific definition) than presently exists is required and, in areas where this is considered to be unachievable for any reason, must be supplemented by consistent State and Territorial legislation. To the extent that such State or Territorial action is required, the emphasis must be on strict uniformity, as opposed to simple 'harmony'.

The case for strict uniformity is built upon three considerations: logic, practicality and urgency.

Logic dictates that the individual jurisdictions comprising the Commonwealth of Australia should appreciate the need for legislation of this nature and the absurdity of diverging from the outset in the regulation of an activity which poses a common threat to all jurisdictions, which has developed to a common degree in all jurisdictions and which, because of the prospect of transborder perpetration, can only be completely effective if residents of all jurisdictions are subject to the same regulation.

At a practical level, effective regulation of electronic databanks on a national scale could be significantly jeopardised in the event that one or more jurisdictions either refrain from regulation at all or, alternatively, adopt a divergent form of regulation which could be susceptible to exploitation if perceived as being more or less severe than other jurisdictions.

The urgency of the problem further strengthens the case for strict uniformity. As this article has emphasized, the implications of computerized information storages have been acknowledged in one form or another by various Australian jurisdictions for nearly two decades, but procrastination occasioned by difficult philosophical and legal considerations has resulted in the current under-regulation. If the States and Territories were at this point individually to review their respective needs and approaches to the problem, further delays and inevitable inaction would certainly follow. A common commitment to uniformity would, equally inevitably, minimize the delays inherent in individual formulations of policy.

What rights and obligations should emanate from a scheme providing for national regulation of electronically stored information? In general terms, it is necessary to redress the vulnerability of the data subject, in both the private and public sectors, to the unique capabilities of the computer to store, collate and transmit information. Accordingly, again in general terms, regulation of electronic data storages must place an obligation on the data controller to keep the

information secure from unauthorized intrusion; the data subject must be aware of the nature and extent of any matching of information from diverse computerized sources; there must be a prohibition on the unauthorized dissemination of data; the data subject must have a right to inspect and amend pertinent records; and a remedy in damages must be available against persons responsible for breaching these fundamental privacy rights.

Finally, as discussed above, the right of access to information held about oneself, and the right to amend inaccurate information so held, is fundamental to any concept of 'privacy' and, more specifically, any regulation of the electronic storage of personal information. Consequently, in any consideration of the imposition of a national scheme for the protection of electronic data, it is imperative that the adequacy of our freedom of information laws be reviewed. In this context, deficiencies requiring rectification emerge at a number of levels which do not require recapitulation at this point.

If national regulation of computerized information storages were to be achieved, it would ideally involve all-embracing Commonwealth legislation, complemented where appropriate by strictly uniform State and Territorial legislation. The preferred method of achieving this, and the most realistic course to follow, are the subject of speculation below. It must be appreciated, however, that there are factors other than mere identification of the problem which will influence the final outcome.

First, there is the fundamental constitutional issue. Does the Commonwealth government have the legislative capacity to rectify each of the deficiencies identified above? What considerations might militate against an adventurous exercise of Commonwealth power in this regard? What are the prospects of a referral of legislative power by the States to the Commonwealth if significant doubts as to Commonwealth legislative competence otherwise persist? The perceived limitations on Commonwealth power to legislate in this area have already been discussed. Regrettably, one must anticipate that unless a federal government is persuaded that an issue is of national urgency and of widespread community concern, it will most likely be disinclined to risk the appearance of legislative and administrative ineptitude associated with the invalidation of a statute by the High Court. Consequently uniform State legislation, or perhaps a referral of power to the Commonwealth by the States, should be regarded as a greater likelihood but, again, it would require recognition and appreciation by the various jurisdictions of a problem which has, to date, not been the subject of intense legislative or political activity.

Second, just as there are significant obstacles to an effective exercise of comprehensive Commonwealth legislative power in this area, so too are there political and pragmatic difficulties inherent in the formulation of uniform State and Territorial legislation on this or, indeed, any other subject matter. Not only is mutual acknowledgement of the problem required, but also a mutuality of philosophy. Unfortunately, it has been demonstrated above that commonality in approach to the legal problems raised by computerized information storages has been negligible.

Finally and, arguably, most fundamentally, there is the philosophical question

of whether the activities under discussion warrant regulation at all, at least on a uniform, national scale. It is argued here that a strong case exists in support of national regulation of computerized information storages. It must be accepted, however, that the historic inaction in some jurisdictions, and the diverse reactions in others, evinces an uncertainty as to the seriousness of the problem and the validity of distinguishing between electronic and manual information storage methods. So long as this uncertainty remains, the legal deficiencies outlined above will continue unredressed.

If the Commonwealth is not prepared to exercise its legislative competence in respect of the matters under discussion, an alternative option would involve uniform State and Territorial legislation. It is conceivable that although the individual Australian jurisdictions might not be willing to surrender legislative power to the Commonwealth under s. 51 (xxxvii) of the Constitution, they might nevertheless consider uniform legislation to be politically and philosophically acceptable.

Pragmatically, uniformity as between States, the Territories and the Commonwealth is not as attractive an option as the enactment of embrasive Commonwealth legislation. The formulation of legislation of necessity becomes a more cumbersome process, and subsequent divergences as between the parties to the scheme are inevitable as time passes.

Politically, however, this approach may be more acceptable, even if strict uniformity is ultimately unachievable in relation to some (or all) aspects of the legislation involved.

Uniform legislative schemes have not been common in Australia, even though they are proposed periodically on the basis that they represent a pragmatic solution to the constitutional limitations on Commonwealth powers in circumstances where national regulation of an activity has clear advantages.

Arguably, a further option exists. This would involve the implementation of 'harmonious' legislation in all jurisdictions. The concept of 'harmonious' legislation in this context involves the enactment of laws by the individual jurisdictions, the form and content of which are left totally to the discretion of the individual governments concerned.

The immediate benefits of such an approach are not difficult to identify. Each government would undertake to ensure it had in place adequate legislation relating to the privacy of information subjects, freedom of information, and criminal sanctions for unauthorized access to computerized information.

The disadvantages of a commitment by jurisdictions to a mere genus of legislation, as opposed to strictly uniform laws, are readily apparent. An obligation to achieve mere 'harmony' could be satisfied by one State enacting specific legislation relating to computerized information storages, and by another creating a general right of privacy. Some jurisdictions might choose to create a remedy in damages, and others might specify more limited means of redress in the event of privacy infractions. Some States might adopt the federal Information Privacy Principles, some might adopt alternative principles and some might define the right in question without adopting privacy principles at all. Some States might provide a role for a privacy commissioner, some might alternatively

entrust privacy protection to their ombudsmen and some might envisage the enforcement of rights only through the courts. Some States might introduce criminal sanctions to reinforce the scheme; some might not. In these circumstances, jurisdictional disputes become inevitable.

It follows that the implementation of laws regulating the storage of personal information in computer databanks cannot be adequately achieved within any Australian jurisdiction in isolation from the other jurisdictions. It is a reflection of a modern, technological world that the rights and expectations of individuals can be offended across territorial boundaries. A co-operative approach between all jurisdictions is required.

As stated at the outset, computerized information storage represents one of the great technological advances of the twentieth century. Like all significant technological advances, the benefits must be balanced against any adverse impact upon individuals who are affected. In this instance, the technological advance poses a threat to the privacy of individuals. This threat can be minimized by adequate regulatory intervention and the basis for such intervention has been suggested above. In the absence of a comprehensive and co-ordinated regulatory scheme, the law and the law makers will have failed in their principal task, namely, to protect the quality of life of individual members of the community.