PRIVACY PROTECTION IN THE PRIVATE SECTOR: THE FEDERAL GOVERNMENT'S DISCUSSION PAPER

*Moira Paterson**

Paper presented to AIAL seminar, Private sector privacy, Melbourne, 26 February 1997.

Background

Late last year the federal government took its first step towards giving effect to its election commitment to work, as a matter of priority, with industry and the States to provide a co-regulatory approach to privacy within the Australian private sector which was comparable with "best international practice".[1] The Attorney-General's Department released a Discussion Paper *Privacy Protection in the Private Sector*[2] which contains detailed proposals for the introduction of a co-regulatory scheme based on the existing structure of Information Privacy Principles together with provision for the development of binding Codes of Practice. It is the aim of this paper to explore the rationale for extending the *Privacy Act 1988* (Cth) to cover those parts of the private sector that are not already subject to provisions in Part III which govern the credit reporting industry and to provide a brief overview of the scope of the proposed regime.

It should, however, be noted that the Discussion Paper specifically states[3] that the level of detail which it provides is intended to provide for an opportunity for feedback on a wide range of issues and should not be taken as an indication that the Government has taken a firm view in relation to any specific matters. This point was again emphasised by the Attorney-General in a speech which was presented on his behalf at *The New Privacy Laws: A symposium on preparing privacy laws for the 21st century*, in Sydney on 19 February 1997. It is therefore not unlikely given the large number of submissions that have been received and the intensive lobbying that is taking place behind the scenes that any Bill which eventuates will be quite different from the scheme which it proposes.

* *Moira Paterson is a lecturer in law, Monash University.*

Why a private sector Privacy Act?

The rationale for the proposed reforms consists of a curious mixture of human rights and economic concerns which have their origins in the perceived impact of technological developments and in the increased blurring of distinctions between the public and private sectors.

First, and most significantly, the ever accelerating pace of technological development has led to increasing public concerns about personal privacy as demonstrated in a number of public opinion polls. For example, a recent survey commissioned by Mastercard International showed that Australians were concerned about a wide range of privacy issues and, in particular, about the sharing of information between government agencies and between different financial institutions.[4]

These findings, which are similar to those in other polls both in Australia[5] and overseas[6], stem not simply from the rapid pace of technological change but also from the changing nature of the threats to privacy which this poses. Not only have

personal computers become cheaper (and therefore more prolific) and much more powerful but they are now interconnected so as to form a global information infrastructure. This makes it both feasible and attractive for businesses as well as governments to conduct surveillance on a massive scale. Whereas once the main concern was with Big Brother, it is clear that there are also increasing threats posed by the surveillance activities of "Little Brother". Moreover, although the latter may appear to be less sinister given that it is more likely to be concerned with market power than political power, there can be a blurring of the distinction between legitimate marketing strategies and more aggressive attempts at manipulation (as evidenced for example in the context of telemarketing) and there are also concerns about the potential long-term harm that may arise from adverse profiles, whether correct or incorrect.[7]

Moreover, privacy is threatened not only by the potential for large scale transfers and data matching but also by the information which is now routinely gathered as a by-product of that process. There is therefore a need to protect not only the content of information that is being transmitted across the information highway but also the footprints which are created by that traffic.[8] For example, the disclosure that a person visited a particular site may be as much a threat to their privacy as the disclosure of the content of his or her transactions.[9]

As noted by Collin Bennett, the central role of information in our post-industrial economy and the increasingly complicated relationships between individuals and those with the power to manipulate information are at the root of data protection concerns.[10] Information technology not only provides a potential tool for abuse of power but "accentuates the dehumanising and alienating aspects of modern mass society and information technology" contributing to an uneasy sense that "someone out there knows something about me".[11]

These developments create obvious human rights issues. Privacy, although notoriously difficult to define, is without doubt a commodity that is very much valued in our individualistic liberal democratic society. It is therefore increasingly accepted as being a human right or at least a precondition for the effective exercise of other more traditional human rights. In fact it is arguable that we have international obligations arising under the International Covenant on Civil and Political Rights to ensure its adequate protection.[12] The reason why the specific topic of data protection did not feature more prominently on the human rights agenda in past years arguably has much to do with the fact that large-scale surveillance activities have only become technically and economically feasible in recent years.

For reasons which I will explain, the same factors have made privacy protection a matter of concern to business. The economic pressures for reform come from two separate directions - the need to ensure that initiatives involving the use of new technologies are not hindered by public concerns about potential privacy invasions and the need to ensure that the free flow of information into Australia is not hindered by transborder data flow (tbf) restrictions in overseas privacy legislation.

Concerns about the former have been a significant factor in prompting data protection initiatives in Victoria. The Treasurer and Minister for Multimedia, Alan Stockdale, in announcing the formation of Victoria's Data Protection Advisory Council, noted that the success of the proposed electronic service delivery system would largely depend on Victorians trusting that the information which they sent "would not be misused or accessed by unauthorised persons". In a similar vein a recent US Government report has noted that "if consumers feel

that their personal information will be misused or used in ways that differ from their original understanding, the commercial viability of the NII could be jeopardised as consumers hesitate to use advanced communication networks".[13]

In the case of the latter, concerns have been fuelled in particular by the recent EC Directive which requires member states to impose restrictions of the outflow of personal data to countries which do not have adequate privacy regimes, but it should also be noted that two neighbouring countries, Hong Kong and Taiwan have enacted privacy laws which contain similar measures.[14] In addition, the Canadian government has made a commitment to extend its privacy laws to the private sector[15] and may well include transborder data flow restrictions in any such legislation.[16]

The EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which was finalised in July 1995, requires member states to amend their laws within three years so as to prohibit the international transfer of personal data unless the transferor is able to ensure that adequate standards of privacy protection will apply.[17] If Australia does not extend its privacy regime to the private sector, then any business within the EC which wishes to send personal data to an Australian business would be required to ensure that it satisfies the criteria for exportation to countries which lack adequate privacy safeguards. In most cases this would require the imposition of contractual safeguards, a potentially costly exercise which is likely to place Australian businesses at a competitive disadvantage vis a vis those in countries such as New Zealand which have adequate private sector privacy laws.

Another justification for the extension arises from the need to protect the large body of personal information which is held by the many private organisations that are now performing what were once regarded as government functions. This development has resulted in part from the privatisation of bodies which were once within the umbrella of the Privacy Act and in part from the trend towards the outsourcing of government functions which has occurred as the government implements policies designed to downsize and thereby improve the efficiency of its operations.[18] Furthermore, as the boundaries between the private and public sectors have become more blurred there has been an increase in the outflow of personal information from the public to the private sector. There are also many examples of apparently irrational anomalies. For example, a person may have a right of access to his or her medical records in the possession of a public hospital but not a private one even though there is no inherent difference in the type of information or the circumstances in which it was generated. Likewise, the employment records of federal government employees are protected by the Privacy Act whereas those of other employees receive no equivalent protection.

Two final factors which are of particular relevance to business are the need to ensure uniformity in the face of proposed initiatives by individual states[19] and the desire of those businesses which have taken active measures to protect personal privacy to reduce the potential for less reputable players to tarnish the reputation of their industries.

The Discussion Paper

The scheme which is presented in the Discussion Paper follows the co-regulatory approach used in the New Zealand *Privacy Act 1993* which became fully operational in the private sector in mid-1996. It basically provides for an extension of the Information Privacy Principles (IPPs) which presently apply to the public sector under the *Privacy Act 1988* but with provision also for the making of legally binding Codes of

Practice to operate in place of the IPPs. This scheme provides for data protection via the imposition of general standards rather than detailed prescriptions of conduct while allowing for those standards to be modified in respect of specific industries or specific types of information.

Who does it affect?

The Privacy Act is to be extended to cover all individuals and organisations, whether incorporated or not, in the private sector as well as all of the Commonwealth public sector.[20] It does not, however, apply in respect of persons who hold information in a domestic capacity in respect of personal, family and household affairs.[21] The two main types of records which are likely to be affected by the proposed extension are customer data (including past, current and potential customers) and employee data.

Employers are to be required to take all reasonable precautions and exercise due diligence, including taking account of possible thoughtlessness, inadvertence or carelessness on the part of employees and agents and will be vicariously liable for any breaches which occur in the absence of such measures. As one might expect, employees and agents are to be individually liable in other cases.[22]

What aspects of privacy does it regulate?

Data protection

The scheme provides for enforceable privacy protection in respect of all manual and automated records which contain personal information.[23] The terms "personal information" and "records" follow the terminology which is used in the existing *Privacy Act*. "Personal information" is defined as meaning any information or opinion about an identifiable individual or one whose identity can reasonably be ascertained. The information or opinion does not have to be recorded in a material form and does not necessarily have to be true in order to fall within the definition. The term "record" is not confined to documents but also covers data bases, photographs and other pictorial representations. It does not, however, include generally available collections of letters and other articles while in the course of transmission by post.

Other privacy intrusions

Although the main emphasis is on data protection, there is also provision for the regulation of other intrusions on privacy. The Privacy Commissioner is to be given the power to issue guidelines for the avoidance of acts and practices such as telemarketing or optical surveillance that might have an adverse effect on individual privacy, even where no record is involved.[24] The Commissioner will have the power to investigate and make recommendations to resolve disputes in relation to matters covered by guidelines but no right of proceedings in the Federal Court as is the case in respect of the data protection provisions.

The media is specifically acknowledged as a special case which warrants separate attention because of the considerable difficulties that are involved in attempting to strike an appropriate balance between freedom of expression and privacy.

How does it protect personal information?

The Information Privacy Principles

The existing IPPs in section 14 of the *Privacy Act 1988* are to form the basis of the statutory standard for data protection.[25] These principles were developed from draft principles outlined in the Australian Law Reform Commission's Report on Privacy[26] and have their origins in the principles contained in the OECD Guidelines, although they differ from these in some respects.[27] They are primarily concerned with ensuring the fairness and openness rather than

attempting to prevent the use of data for surveillance purposes. In other words they play a similar role to the rules of procedural fairness that have been developed in the context of judicial review which are not concerned with the substantive content of the decisions the subject of review although they are designed to provide an appropriate context for the making of substantively correct decisions.

Data collection

The first three principles are concerned with the collection of information.[28] Principle 1 prohibits the collection of information unless it is collected for a lawful purpose directly related to a function or activity of the collector and its collection is necessary for, or directly related to, that purpose. It also prohibits the collection of information by unlawful or unfair means. It should be noted that it does not impose any limitation on the purposes for which information may be collected provided that they are directly related to a function or activity of the collector, irrespective of any criterion of intrusiveness.[29]

Principle 2 imposes limitations on the solicitation of personal information from individual data subjects and, in particular, data collectors to take such steps (if any) as are reasonable to ensure that the individual is generally aware of the purpose for which the information is being collected, any law which requires or authorised its collection and who, if anyone, it is likely to be passed on to.

Principle 3, which deals with the solicitation of information generally, requires that the data collector should take all reasonable steps to ensure that, having regard to the purpose for which the information is collected, it is relevant, up to date and complete and does not intrude to an unreasonable extent upon the personal affairs of the individual concerned. Once again it should be noted that there are no constraints on the purposes for which information can be collected and no criterion for assessing reasonableness. In the case of the *Freedom of Information Act 1982* (Cth) the requirement of reasonableness in the context of the personal information exemption provision in section 41 has been interpreted by the Federal Court as requiring a balancing of the public interest in the disclosure of the information against the potential harm to personal privacy.[30] In the case of the private sector it is arguable that this may involve a weighing up of the private interest of the record keeper having regard to the extent to which the collection of that information is necessary for the carrying out of a lawful function or activity of the collector against the harm to the privacy of the individual concerned.

Security safeguards

The next provision, Principle 4 deals with the issue of security. Record keepers are required to ensure that that records are protected by such security safeguards as are reasonable in the circumstance, against loss, unauthorised access, use modification, disclosure or other misuse. The steps that are required may range from the placing of locks on doors and filing cabinets to the imposition of firewalls and other safeguards to prevent hacking and the encryption of data that is sent via the Internet. Record keepers are also required to take all possible steps to guard the security of records given to other persons in connection with the provision of a service to the record keeper. This would be of relevance, for example, where customer records were processed externally.

Access and amendment

There are also three further principles which provide rights of access and amendment which are designed to give individuals greater control over their personal information in the sense of being aware of what is held and being able to ensure that it is factually correct and up to

date. Principle 5 provides that a record keeper is required to take all reasonable steps to enable any person to ascertain whether he or she has possession or control of any records that contain personal information and, if so, the nature of that information, the main purposes for which it is used and the required steps for obtaining access. This is, however, subject to exception in cases where the record keeper is required or authorised to refuse to comply with such a request under the provisions of any Commonwealth law that provides for access to documents.

In addition to the duty to provide information in relation to specific requests, record keepers are required to maintain records that set out details of any personal record held including their nature, the purpose for which they are kept, the classes of individuals about whom they are kept, the period for the they are kept, the persons who are entitled to have access to them, including any conditions governing their entitlement to have access and necessary steps for obtaining access. These records must be available for inspection by members of the public and copies of them must be provided to the Privacy Commissioner in June each year.

Following on from this, Principle 6 provides for a specific right of access to personal records in the possession or control of a record keeper subject to the restrictions on access in other Commonwealth legislation.

Principle 7 contains closely related amendment rights and provides that a record keeper who has possession or control of a personal record is required to take all steps by way or of making appropriate corrections, deletions and additions as are reasonable in the circumstances to ensure that the information is accurate, relevant, up to date complete and not misleading. Once again this right is subject to any limitations arising under other Commonwealth laws. A record keeper who is not willing to amend a record must, if so requested, take all reasonable steps to attach to the record a notation setting out details of the requested amendments.

Restrictions on use

The safeguards in the access and amendment provisions are supplemented by a series of further principles which regulate the use of personal information by record keepers. Principles 8 and 9 require record keepers to check that personal information is relevant, accurate etc before using it and to confine its use to purposes to which the information is relevant. In a similar vein, Principle 10 imposes a number of further important limitations on the use personal information. For example, the record keeper who has obtained information for a particular purpose is preclude form using that information for any other purpose (other than one which is directly related) unless the individual concerned has consented to the other use, the record keeper has reasonable grounds for believing that use of the record for that other purpose is necessary to prevent or lessen a serous and imminent threat to the life or health of the individual concerned or of another person There are also exception in cases where use of the information for the other purpose is required or authorised by or under law, whether it is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty, or for the protection of the public revenue. In the case of these further exceptions the record keeper is required to include in the record a note of that use.

Finally, Principle 11 imposes a number of important limitations on the disclosure of personal information to persons, bodies or agencies to whom the information subject could not reasonably have the information to be passed on. A record keeper is preluded from disclosing information to any such persons or bodies in the absence of consent by the

individual concerned except where the record keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person, where disclosure is required or authorised by or under law or whether the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue. (In the case disclosure which is made of the purposes of law enforcement/ protection of public revenue the record keeper is required to include a note in the record to that effect.) This principle also prohibits persons, bodies or agencies to whom information is disclosed under this principle from using or disclosing the information for a purpose other the purpose for which it was given to them.

Destruction of records

In addition to these existing principles, the Discussion Paper proposes the inclusion of an additional IPP which provides that records are not to be kept for longer than is required for the purposes for which the information may lawfully be used.[31] This reflects the principle that information which is collected for specific and limited purposes should not be retained indefinitely, particularly given the fact that its accuracy is likely to diminish over time.

Implementation

It should be noted that that the first three IPPs, which regulate the collection of data, are to apply only in respect of information that is collected after the commencement of the proposed legislation. The remainder, including the access and amendment provisions will apply to all information irrespective of when it was collected.

Codes of Practice

An important feature of the proposed scheme is the provision for the development of Codes of Practice which is intended to allow for the principles to be tailored to meet the needs of a particular part of the private sector. These Codes may be developed not only in respect specific industries, professions and callings but also in respect of specified organisations, specified activities and specified information and in relation to specific classes of all of these. They are intended to have the same binding effect as the IPPs which would apply in all cases where there was no Code in operation.[32]

The Codes of Practice are intended to serve two separate but complementary purposes. First they may prescribe how any one or more of the IPPs are to be applied or complied with by the record keepers who it regulates. This would serve to add clarity and specific content to the IPPs thereby avoiding unnecessary uncertainty. Secondly, they may be used to modify the application of any one or more of the IPPs by imposing standards that are either more or less stringent, subject to a prohibition against any limitation or restriction of rights of access and correction. Such modifications might exempt any action from an IPP either unconditionally or subject to conditions, impose controls on data matching, set guidelines for the imposition of charges in relation to access and amendment, prescribe procedures for dealing with complaints alleging breaches of the Code (other than ones which limit or restrict the Privacy Commissioner's powers to receive, investigate and endeavour to settle complaints) or provide for review of, or expiry of, the Code.[33]

Codes of Practice are to be issued by the Privacy Commissioner. However, while it is possible for her to issue them on her own initiative, it is envisaged that particular organisations, industries or could initiate and develop their own Codes and then apply to the Commissioner to have them issued.[34] The scheme provides for a number of procedures which are designed to ensure

that all interested parties are adequately consulted before any Code is issued and that they have an adequate opportunity to become familiar with its terms before it comes into effect. Codes cannot come into operation until at least 28 days after they are issued and are subject to disallowance by Parliament.[35]

There is also an alternative procedure for the urgent issuing, amendment or revocation of Codes which allows the Privacy Commissioner to dispense with the requirements for public notice and the taking of written submissions. However, any resultant Code, amendment or revocation would be regarded as temporary only and would remain in force for no longer than 1 year.[36]

Public Interest Determinations

The Privacy Commissioner is to continue to have the power make public interest determinations which authorise practices that might otherwise amount to a breach of either an IPP or a Code of Practice. This would provide an alternative to the development of Code which would be available in one-off cases that raise special factors.[37]

Access to and Correction of Personal Information

In addition to requiring compliance with the IPPs or with a Code of Conduct where this is applicable, the new scheme will provide for a scheme of access to, and amendment of, personal records which is analogous to that which is currently provided in relation to personal records in the possession of public bodies under the FOI legislation.[38]

Some of the key features of this scheme include a procedure for the making of requests for access and decisions in relation to those requests (including time limits), exemption provisions which set out the categories of documents that are exempt from access, rules which set out a schedule of charges for complying with requests, requirements to provide reasons for refusal and procedures concerning forms of access, access information not held in written form and provision of copies of documents from which exempt information has been deleted. Apart from the matters noted below these are in most respects similar to the requirements in the *Freedom of Information Act 1982*.

There is provision for fees to be charged for the provision of access and the making of amendments. These must be reasonable and linked to the reasonable cost of complying with a request. Very importantly, fees would not be able to be charged for the making of requests for the making and processing of requests including the work involved in deciding whether or not to grant a request, and if so, in what manner.[39]

The time limits imposed are 14 days for the notification of receipt of a request and 30 days for the notification of a decision. There is, however, provision for an extension of the 30 day time limit up to a maximum of 60 days in cases where a large quantity of the information is sought or needs to searched and it would unreasonably interfere with the operations of the business concerned to meet of the time limit or where the extent of consultation necessary makes it impossible to provide a proper response within the time limit.[40]

Insofar as the controversial question of exemption provisions is concerned, the Discussion Papers simply states that they would address a number of specific matters. These are the inability to locate information (ie, the situation where the information is not held by the recipient of a request, does not exist or cannot be found); the privacy interests, safety and physical or mental health of individuals; trade secrets and other in confidence information, evaluative or opinion material; legal professional privilege; contempt of court, the safe custody and rehabilitation of individuals and the

resource costs to the individual or organisation of complying with requests. These categories already exist in the context of requests for access to information under the *Freedom of Information Act 1982* (Cth) and state Freedom of Information Acts but their transposition to the context of private sector access rights will not be a simple exercise given the extensive use of the public interest criterion in the FOI legislation. While it may be possible to use a similar criterion in the case of private sector access rights, this will require a balancing of very different criteria (ie, the privacy interests which underlie the provision of access and amendment rights as against the interest in ensuring that businesses are able to conduct their businesses in an efficient manner).

Finally the recipient of a request for access would be required to be satisfied about the identity of the person making the request and to ensure that any information indeed for that person was received only by that person or his or her properly authorised agent.

Transborder Data Flows

In addition to being required to comply with the IPPs and/ or Codes, record keepers are subject to a number of restrictions concerning the transfer of data to non-Australian residents in countries with inadequate levels of privacy protection. These do not apply to transfers to Australian residents who are themselves subject to the IPPs governing storage and security, access and correction and use and disclosure.

Transfers to non residents in such countries without the consent of the data subjects would, in general, only be permissible where the record keeper has in place adequate contractual safeguards. However, a record keeper who transfers information out of Australia in reliance on contractual safeguards would be liable for any breach of the IPPs in relation to storage and security and use and disclosure of the information. There are also a number of limited exceptions to the general prohibition against data transfers in cases where the transfer of a record is in the interest of the data subject, in the public interest or required or authorised by law.

It is envisaged that those countries which have adequate laws would be specified by regulation. In order to qualify for inclusion a country would need to have in place a law which is substantially similar to, or serves the same purpose as, the (proposed) Australian privacy regime. Account would be taken of any reciprocal specification of Australian privacy laws.

Those countries which would be likely to qualify as having adequate privacy protection include the majority of EC member states, New Zealand, Hong Kong and Taiwan.[41] One glaring exception is the United States which continues to be implacably opposed to the concept of comprehensive private sector privacy laws. It should, however, be noted that in addition to the federal public sector Privacy Act there is also a patchwork of federal and state statutes which provides varying degrees of protection in respect of specific industries.[42]

Implementation

Finally, the proposed scheme provides for delayed implementation in order to give businesses adequate time to get their affairs in order and to allow for the development of Codes if these are required. Although all of the IPPs are to come into operation as soon as the proposed legislation is enacted, only IPPs 4-7 (the principles which relate to storage and security and access and correction) are to be enforceable immediately. In the case of the remainder there will be no right to bring proceedings in the Federal Court in relation to breaches, although the Commissioner is to have the power to receive complaints, to conduct investigations and to make

recommendations, including a recommendation to develop a Code.

Conclusion

The introduction of a comprehensive Australian privacy regime is required as a necessary response to the widespread use of surveillance technologies and the blurring of the boundaries between the public and private sector. It is important both in order to ensure adequate protection of human rights and to protect the economic interests of the Australian business community.

The proposed adoption of a co-regulatory scheme based on Information Privacy Principles and binding Codes of Practice follows the New Zealand model and therefore has the obvious advantage of using a system that has been successfully tried and tested and one in respect of which there is a growing body of useful information.[43]

While it is arguable that the IPPs have become outdated in the light of technological developments and that they are in urgent need of reform if they are to operate successfully in the context of the private sector, any attempt to reformulate them is likely to take a lengthy period and may therefor need to be postponed in order to avoid any undue delay in the implementation a private sector law. It is to be hoped that the government does not allow the reform process to become stalled for too long and that any legislation which emerges is not unduly emasculated as a result of the lobbying efforts of groups that are too short sighted to see that effective privacy regulation in the Australian private sector is not only inevitable but also in the interests of the vast majority of Australian businesses.

Endnotes

1 The relevant parts of the Coalition Government's Law and Justice Policy are extracted in (1996) 3 *Privacy Law & Policy Reporter* 4.

2 Cth of Aust, Attorney-General's Department; *Privacy Protection in the Private Sector*, September 1996.

3 At p 4.

4 See the Mastercard Report, 'Privacy and Payments: A Study of Attitudes of the Australian Public to Privacy - Summary and Findings' (1996) and the summary of its findings in Roger Clarke, 'Public attitudes to privacy - Mastercard's Australian survey' (1996) 3 *Privacy Law & Policy Reporter* 141.

5 The other major Australian study was commissioned by the Privacy Commissioner in 1990-1994; see HREOC, *Information Paper Number 3: Community Attitudes to Privacy* (August 1995).

6 See, for example, Louis Harris & Assocs and Alan F Westin, *The Equifax Report on Consumers in the Information Age* (1990); Ekos and Research Associates, *Privacy Revealed: The Canadian Privacy Survey* (1992).

7 The most obvious example is the difficulty involved in living down an adverse credit rating in a context where the rating itself makes it difficult to obtain credit and therefore the means for creating a more positive rating.

8 For a useful discussion of the use of the information highway to generate marketing profiles see US Department of Commerce, National Telecommunications and Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (October 1995) Appendix A.

9 See, for example, the discussion of direct marketers' uses of mouse-click patterns and Internet trails in Andy Kessler. 'Tracking Mouse Droppings' *Forbes ASAP*, Aug 28, 1995 67 cited in US Department of Commerce, National Telecommunications and Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (October 1995).

10 Collin J Bennett, *Regulating Privacy* (Ithaca, New York: Cornell University Press, 1992) 15-17.

11 Id 27-28.

12 Article 17 of the International Covenant on Civil and Political Rights to which Australia is a signatory, states that "no one shall be subjected to arbitrary interference with his privacy" and requires that individuals should have "the right to the protection of the law against such interference". In addition the OECD Guidelines require the adoption of eight principles of good data practice which form the basis for the IPPs in the Privacy Act 1988 (Cth) as discussed below.

13 US Department of Commerce, National Telecommunications and Information Administration, *Privacy and the NII:*

Safeguarding Telecommunications-Related Personal Information (October 1995) 28.

14 See clause 33 of Hong Kong Personal Data (Privacy) Ordinance which was enacted on 3 August 1995 and Article 24 of the Taiwanese Computer-Processed Personal Data Protection Law which took effect on 13 August 1995.

15 In a speech given at the Eighteenth International Conference on Privacy and Data Protection in Ottawa on September 18, 1996 the Canadian Minister of Justice, Allan Rock, stated that: "By the year 2000, we aim to have federal legislation on the books that will provide effective, enforceable protection of privacy rights in the private sector".

16 It should be noted that in the case of Quebec, the only Canadian province which has a privacy law that applies to the private sector, Article 17 of An Act Respecting the Protection of Personal Information in the Private Sector 1993 contains a limited restriction of the flow of information outside Quebec by requiring data-keepers to take all reasonable steps to ensure that the privacy of the data is protected. Furthermore the inclusion of tbf restrictions is the norm rather than the exception in the case of countries which have privacy legislation that extends to the private sector. The only notable exception is the New Zealand Privacy Act 1993.

17 See Graham Greenleaf 'The European Privacy Directive - Completed' (1995) 2 *Privacy Law & Policy Reporter* 81; Graham Greenleaf 'European privacy Directive and data exports' (1995) 2 *Privacy Law & Policy Reporter* 105.

18 External contractors are not subject to the requirements of the Privacy Act 1988 (Cth) although the Privacy Commissioner has published advisory guidelines, *Outsourcing and Privacy: Advice for Commonwealth Agencies Considering Contracting Out (Outsourcing) Information Technology and Other Functions (August 1994),* which contains recommended clauses for inclusion in outsourcing contracts. For a useful discussion of the accountability problems which are posed by the outsourcing of government services see Anne Marks, 'Outsourcing and Administrative Law in the Commonwealth Public Sector' in Kathryn Cole (ed), *Administrative Law and Public Administration: Form vs Substance* (AIAL, 1996).

19 On 19 February 1997, at The *New Privacy Laws: A symposium on preparing privacy laws for the 21st century*, in Sydney, the NSW Attorney-General stated that his government intends to enact a public sector Privacy Act and that this would be extended to encompass the NSW private sector in the event that the Commonwealth government fails to enact such laws within a reasonable time. Likewise, the Victorian Treasurer and Minister for Multimedia is considering a report prepared by the Data Protection Advisory Council.

20 The State public sectors are excluded for obvious constitutional reasons.

21 See p 7.

22 See p 6.

23 See p 5.

24 The following provide discussion of some of the current privacy issues that extend beyond data protection in the traditional sense Tim Dixon,, 'Workplace video surveillance - controls sought' (1995) 2 *Privacy Law & Policy Reporter* 141; Sheldon W Halpern, "The Traffic in Souls: Privacy Interests and the Intelligent Vehicle Highway Systems" (1995) 11(1) *Santa Clara Computer and High-Technology Law Journal* 45-73; NSW, Privacy Committee of New South Wales, *Electronic vehicle tracking* (Sydney : The Committee, 1990); NSW, Privacy Committee of New South Wales, *Drug testing in the workplace* (Sydney : The Committee, 1992).; NSW, Privacy Committee of New South Wales, *Electronic vehicle monitoring*(Sydney : The Committee, c1990); NSW, Privacy Committee of New South Wales, *Invisible eyes : report on video surveillance in the workplace* (Sydney : The Committee, 1995); Nigel Waters, Street Surveillance and privacy" (1996) 3 *Privacy Law & Policy Reporter* 48; Robin Whittle 'Calling number display: AUSTEL's PAC report' (1996) 3 *Privacy Law & Policy Reporter 8.*

25 See pp 6-12.

26 ALRC, *Privacy*, Report No 22 (Canberra: AGPS, 1983).

27 For a useful discussion of the origins of these principles and critique of them from the standpoint of technological change see John Gaudin 'The OECD Privacy Principles - can they survive technological change? Part 1' (1996) 3 *Privacy Law & Policy Reporter* 143.

28 Further guidance concerning the application of these principles to the public sector may be found in HREOC, Plain English Guidelines to Information Privacy Principles 1-3: Advice to Agencies about Collecting Personal Information (October 1994).

29 See, for example, Roger Clarke 'Flaws in the Glass; Gashes in the Fabric' paper presented to *The New Privacy Laws: A symposium on preparing privacy laws for the 21st century*, Sydney, 19 February 1997 3-4.

30 See *Colakovski v Australian Telecommunications Commissioner* (1991) 100 ALR 111.

31 See p 12.

32 It is expected that Codes will only be developed in a fairly limited range of contexts as has been the case in New Zealand where only three codes have been issued so far: the GCS Information Privacy Code which covers

a government-owned enterprise that supplies computer processing to number of government departments, the Superannuation Schemes Unique Identifier Code 1995 and the Health Information Privacy Code 1994. Further codes which are in the process of being drafted are a Telecommunications Code and a Police Code. In addition, the Credit Industry is still discussing the need for a separate code, with a final decision yet to be made.

33 See pp 13-14.

34 See p 12.

35 Codes are to be treated as disallowable instruments for the purposes of s 46A of the *Acts Interpretation Act* 1901 (Cth) and, if disallowed, would be treated as if they had never been made. Once issued a code could be amended or revoked by the Privacy Commissioner.

36 See pp 15-16.

37 See p 16. This procedure already exists in the *Privacy Act* 1988, Part VI. See also the Public Interest Determination Procedure Guidelines issued by the Privacy Commissioner.

38 See pp 16-21.

39 See p 17.

40 See p 18.

41 Those EC countries which do not have adequate laws at the moment are required by the Directive to have such laws in place by mid 1998. In addition, it should be noted that Quebec already has an across the board privacy regime and that Canada has committed to having such a law by the year 2000 (see fn 16).

42 For a useful overview see Henry H Perritt, Jr, *Law and the Information Superhighway* (New York: John Wiley & Sons, 1996).

43 See, for example, the useful advice contained in a paper titled 'The New Privacy Laws: Exemptions and Exceptions to Privacy Principles' which was presented at *The New Privacy Laws: A symposium on preparing privacy laws for the 21st century*, in Sydney on 19 February 1997 by Blair Stewart, the Manager of Codes and Legislation, Office of the Privacy Commissioner, New Zealand. See Elizabeth Longworth's article 'Developing industry codes of practice and policies for the Australian private sector' (1996) 3 *Privacy Law & Policy Reporter* 196.