The Law Reform Commission

Privacy

Summary of Report

Australian Government Publishing Service
Canberra 1983

© Commonwealth of Australia 1983

ISBN for three-volume report: 0 644 01248 and
ISBN for summary: 0 644 01254 4

This is a summary of the three-volume report of the Australian Law Reform Commission on the protection of privacy in Australia.

Copies of the report are available from Australian Government Publishing Service bookshops in each capital city or from Mail Order Sales, Australian Government Publishing Service, G.P.O. Box 84, Canberra, A.C.T. 2601.

Printed by Canberra Publishing & Printing Co., Fyshwick

Contents

Terms of Reference

I, ROBERT JAMES ELLICOTT, Attorney-General, HAVING REGARD TO–

(a) the function of the Law Reform Commission, in pursuance of references to the Commission made by the Attorney-General, of reviewing laws to which the Law Reform Commission Act 1973 applies, namely–
  (i) laws made by, or by the authority of, the Parliament, including laws of the Territories so made; and
  (ii) any other laws, includings laws of the Territories, that the Parliament has power to amend or repeal;

(b) the provisions of section 7 of the Act which provides that, in the performance of its functions, the Commission shall review laws to which the Act applies, and consider proposals, with a view to ensuring–
  (i) that such laws and proposals do not trespass unduly on personal rights and liberties and do not unduly make the rights and liberties of citizens dependent upon administrative rather than judicial decisions; and
  (ii) that, as far as practicable, such laws and proposals are consistent with the Articles of the International Covenant on Civil and Political Rights; and

(c) the provisions, in particular, of Article 17 of the Covenant which provides, inter alia, that 'no one shall be subjected to arbitrary or unlawful interference with his privacy':

HEREBY REFER the following matters to the Law Reform Commission, as provided by the Law Reform Commission Act 1973,

TO INQUIRE INTO AND REPORT UPON–

(1) the extent to which undue intrusions into or interferences 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, with particular reference to but not confined to the following matters:
  (a) the collection, recording or storage of information by Commonwealth or Territory Departments, authorities or corporations, or by persons or corporations licensed under those laws for purposes related to the collection, recording, storage or communication of information;
  (b) the communication of the information referred to in sub-paragraph (a) to any Government Department, or to any authority, corporation or person;
  (c) without limiting the operation of sub-paragraphs (a) and (b), the collection, recording, storage and communication of information obtained pursuant to the Health Insurance Act 1973–1975 and the Health Insurance Commission Act 1973;
  (d) powers of entry on premises or search of persons or premises by police and other officials; and
  (e) powers exercisable by persons or authorities other than courts to summon the attendance of persons to answer questions or produce documents;

(2) (a) what legislative or other measures are required to provide proper protection and redress in the cases referred to in paragraph (1);
  (b) what changes are required in the law in force in the Territories to provide protection against, or redress for, undue intrusions into or interferences with privacy arising, inter alia, from the obtaining, recording, storage or communication of information in relation to individuals, or from entry onto private property with particular reference to, but not confined to, the following:
    (i) data storage;
    (ii) the credit reference system;
    (iii) debt collectors;

(iv) medical, employment, banking and like records;
(v) listening, optical, photographic and other like devices;
(vi) security guards and private investigators;
(vii) entry onto private property by persons such as collectors, canvassers and salesman;
(viii) employment agencies;
(ix) press, radio and television;
(x) confidential relationships such as lawyer and client and doctor and patient;

(3) any other related matter;

but excluding inquiries on matters falling within the Terms of Reference of the Royal Commission on Intelligence and Security or matters relating to national security or defence.

IN MAKING ITS INQUIRY AND REPORT the Commission will:

(a) have regard to its function in accordance with section 6(1) of the Act to consider proposals for uniformity between laws of the Territories and laws of the States; and
(b) note the need to strike a balance between protection of privacy and the interests of the community in the development of knowledge and information, and law enforcement.

DATED this ninth day of April 1976

R.J. Ellicott, Q.C.
Attorney-General

I. HOW THE CONCEPT OF PRIVACY SHAPED THE SCHEME FOR ITS PROTECTION

1. Justifications for Privacy Protection

1.1 Australian society is expressing concern at loss of privacy and existing inadequacies in its protection, and is demanding that steps be taken for more effective maintenance of privacy. (para. 16) There are practical reasons for strengthening protection of privacy interests. Breakdown through technological change of existing controls on invasions of privacy threatens grave injustices to individuals. This can occur through misuse of surveillance and information technology. Computerised data banks encourage misuse of information, even where true, in criminal, health, employment, credit or other records. (para. 36) The remoteness of decision-making through reliance on computerised information and the new information thereby created, hold the potential for harm. In order to control the risk of injustice, the individual needs to be provided with the facility for checking whether the computerised information is relevant, up-to-date, accurate, complete, and not unduly sensitive in view of the purpose for which it is being used. (para. 37)

1.2 If privacy protection were not strengthened, it would be difficult for Australian society to maintain its traditions of individual liberty and democratic institutions in the face of technological change, which has given to public and private authorities to power to do what a combination and socio-legal restraints have traditionally denied them. Privacy protections might be seen as providing a safeguard against political oppression. (para. 38)

1.3 At present in Australia there is no comprehensive, integrated set of legal rules protecting interests in privacy affected by changes in technology and public and business administration. The basic values which underpin privacy interests, such as individuality, personal autonomy, freedom and fairness, receive attention in laws forbidding forcible interference with the person and forcible intrusion upon land in the possession of the individual. Unfair administrative decisions might be subjected to judicial review, through the prerogative writs and the new administrative law. Positive misconduct which directly threatens the basic values of liberty and fairness might readily be redressed under existing laws. But as the conduct threatening their invasion becomes more subtle (although no less corrosive of those basic values) so the law's response is increasingly inadequate. (para. 143) Whether a basis for a 'right to privacy' is found in conceptions of human rights, natural law, religious doctrine, utilitarian equations, cultural imperatives, or political theory, there is an increasing expectation that privacy interests should be better recognised by the legal system. (para. 81)

2. 'Interests' in Privacy

2.1 Privacy protection should be approached through definition of interests commonly grouped under the heading 'privacy interests', and exploration of the extent of their existing legal protections. Privacy interests include:

- the interest in controlling entry to the 'personal space', or 'territorial privacy';
- the interest in freedom from interference with one's person and 'personal space' or 'privacy of the person'; and
- the interest of the person in controlling the information held by others about him, 'information privacy'. (para. 46)

Related to these are the concepts of:

- freedom from surveillance, and from interception of one's communications, or 'communications and surveillance privacy' (para. 46); and
- 'privacies of attention', i.e., the ability to exclude intrusions that force one to direct attention to them rather than to matters of one's own choosing. (para. 49)

3. Recognition of Privacy Interests

Balancing 'Interests' to Achieve 'Rights' to Privacy

3.1 Against the demand for greater privacy protection must be balanced conflicting demands, for example, by government agencies, researchers and commercial concerns for more private information about individuals. Governmental institutions may claim that they need more information about individuals in order better to plan their activities. Private institutions may want more information for legitimate purposes. The task of the Commission has been to identify and evaluate the various interests classed as 'privacy interests', to weigh them against public and commercial interests, and to recommend mechanisms which will achieve a satisfactory resolution of competing claims. (para. 52, 53)

Building upon Existing Protections

3.2 Existing laws in Australia effectively protect only some aspects of the interest in privacy, and then, only to a certain extent. The Commission recommends a more extensive protection, through filling gaps in existing rules, but in a manner which builds upon them and fulfils their policy aims, as law-makers of an earlier period might have done had they had to address problems such as those created by 'the new technology'. (para. 58)

3.3 The law should provide flexible and accessible mechanisms to handle such complaints of privacy invasion as can be detected and brought to the attention of an appropriately equipped privacy protection authority. Furthermore, the law should state society's standards, seek to promote public understanding about the importance for society of a due respect for individual privacy, and provide a warning to potential privacy invaders that such conduct is not acceptable. The draft legislation meets these needs. It reflects an approach to privacy of seeking to add to existing protections, whilst encouraging the continued growth of privacy as a legal concept by the provision of a statutory guardian of peoples' privacy interests. From the experience of such a guardian further legal rights might be developed. (para. 58, 63)

Interests Complementary to Privacy

3.4 The following interests may complement those in privacy, and may be relevant in deciding whether privacy outweighs its competitors, so that a right should be granted in a particular situation.

- Interests in Secrecy. (para. 65–7)
- Interests in Confidentiality. (para. 68–70)
- Interests in Reputation. (para. 71–3)
- Interests in Freedom from Discrimination. (para. 74)

Interests Competing with Privacy

3.5 Interests competing with privacy may include those in:

- freedom of expression;
- freedom of information;
- protection of the revenue;
- prevention and detection of crime and apprehension of offenders;
- protection of economic, trade and state secrets;
- respect for confidential relationships;
- protection of financial, property and staff management interests;
- maintenance of national security and an effective defence capability;
- protection of diplomatic relations; and
- protection of significant managerial interests, for example, the need for effective conduct of audits, examinations and efficiency reviews.

The objective of the report is to provide a proper level of legal protection for privacy interests without subjugating these other important interests. (para. 75)

4. Genesis of the Protective Scheme

4.1 Claims to better protection privacy interests are in fact claims to better protection of interests already to an extent protected by various branches of the legal and government systems. Against these claims must be balanced competing assertions of the need for greater powers to invade privacy in the interests of law enforcement, research, freedom of expression and information, and other important public and private interests. Protection of privacy is already largely bound up in laws protecting interests in secrecy, confidentiality, reputation, freedom from discrimination, and fairness in consumer transactions. The delicate balance of interests achieved in these areas would be radically upset by a law for the protection of privacy passed on the assumption that it is a single integrated concept. The term privacy is in fact an ordinary language word used to describe a wide variety of disparate and often competing aspirations. A scheme for its better protection, in order not to detrimentally upset the delicate balance of competing claims achieved in various areas of legal and government administration where privacy interests have surfaced and been identified, must build upon the rules developed in those areas, and the experience of those who administer them.

II. HOW TECHNOLOGICAL CHANGE AND NEW METHODS OF ADMINISTRATION AND DOING BUSINESS HAVE PUT PRIVACY AT RISK

5. Dangers to Privacy

Introduction

5.1 Privacy interests are under threat particularly from the following features of contemporary society:

- extension of powers granted to administrative officials;
- new business practices;
- rapid development of technological means for penetrating 'place' and 'space';
- development of computers to handle personal information; and
- extensive and expanding use of computers in public and private administration.

Each is a comparatively recent development. The new technology has already removed many of the traditional physical defences against invasion of privacy: the barriers of matter and distance, and the limitations of time and space. (para. 84–5)

Official Powers

5.2 In part, the need for changes to the existing framework of protection of privacy interests arises from the larger powers claimed by public officials, including powers of arrest, entry, search, seizure, inspection, summons, interrogation and surveillance. As society has become more inter-dependent, and the role of government has expanded, people have come to expect more from the government. To satisfy their demands, the government's claim to intrusive powers increases. There must be proper checks and impartial scrutiny if privacy is not to be unduly eroded. (para. 86)

New Business Practices

5.3 *Intrusive Marketing Practices.* The growing threat to privacy is also a product of new methods of business activity, such as unsolicited mail and telephone advertising. Mail and telephone solicitation is widely practised for commercial, charitable and religious purposes. While the technique of direct marketing is tolerated and, indeed, appreciated by many people, it causes great anxiety for others. (para. 88)

5.4 *Private Investigators and Security Officers.* Intrusions by insurance investigators and other private agents are other prominent examples of business practices which involve dangers to privacy. Safeguards must be implemented to prevent investigators from intruding unduly into the private lives of others. Similarly, security officers guarding shops and factories cannot be allowed an unlimited authority to take whatever action they consider to be appropriate in the circumstances. Some external standard or safeguard must exist. (para. 89)

5.5 *Modern Credit System.* While the emergence of credit facilities has obvious advantages, a modern credit system and the trail left behind by users of credit cards would enable the compilation of detailed personal profiles on individuals. An enormous range of information can now be assembled concerning each single consumer. Once stored on computer it may be readily analysed in conjunction with information about other individuals, transmitted to other data storage systems, and used for an infinite variety of purposes over an indefinite period of time. (para. 90–1) A mix of information obtained from organisations working in any area privy to a credit bureau arrangement can be expected to influence decision-making in all of them. These decisions should not be made on the basis of information which is, for example, irrelevant, inaccurate or out-of-date. It is desirable that enforcement procedures exist whereby the information held by credit bureaus, and by credit grantors themselves, is susceptible to challenge and correction. (para. 90–2)

New Surveillance Technology

5.6 Highly sophisticated surveillance technology is readily and cheaply available. It allows the penetration of physical barriers useful for the protection of privacy. It renders traditional legal protections inadequate. (para. 93) Overt surveillance through technical devices may be offensive and disconcerting, particularly where it is continuous and inescapable. (para. 99)

Information Processing Technology

5.7 *Pace of Change and Impact in Information Technology.* Whereas most of the effects of information processing technology are positive, the 'computer revolution' and its marriage with improved and expanded telecommunications systems, 'computications', is marked by new dangers for privacy. The dangers arise largely from the mushrooming technological development rendering traditional safeguards obsolete. (para. 101–2) The new information technology comprises the aggregation of computers, telecommunications and, increasingly, robotics. The great technological changes of the beginning of the 20th century were the development of the automobile, aviation and electricity and other energy industries. As the century closes, the pervasive industry is that of 'informatics'. (para. 112)

5.8 *Privacy Concerns Generated by the Informatics Industry.* The informatics industry has brought enormous improvements and efficiencies which incidentally cause concern for privacy. The sources of concern have been identified many times. The most prominent are:

- *Amount.* Computers can store vastly increased amounts of personal information and can do so virtually indefinitely.
- *Speed.* Recent technology has increased enormously the speed and ease of retrieval of information.
- *Cost.* The substantial reduction in the cost of handling, storing and retrieving personal information has made it possible to keep vast amounts of personal information indefinitely.
- *Linkages.* The possibility of establishing cross-linkages between different information systems is now perfectly feasible.
- *Profiles.* It is now readily possible, if access can be gained to numerous personal information bases, to build up a composite 'profile' which aggregates the information supplied by different sources. If decisions are made on the basis of this information, they may be erroneous or unfair.
- *New Profession.* The new information technology is in the hands of a new employment group not subject to the traditional constraints applicable to the established professions nor yet subject to effective regulation by a code of fair and honourable conduct.
- *Accessibility.* If proper safeguards are built in, information held in the computerised office can be more secure from unauthorised access than the conventional office. But proper safeguards are not always provided, and establishment of cross-linkages between different information systems increases the vulnerability of information systems to technologically sophisticated attack.
- *Centralisation.* Although, technologically, computerisation linked with telecommunications may facilitate decentralisation of information, it is prone, by linkages, to ultimate centralisation of control.
- *International.* The advent of rapid progress in international telecommunications and the exponential growth of transborder flows of personal information make it simple to store intimate personal information on the citizens of one country in another country, not readily susceptible to the enforcement of protective laws yet instantaneously accessible by reason of the new technology. (para. 119)

Need for Privacy Protection

5.9 *Quantifying the Level of Interference.* Widely publicised cases illustrating omissions, defects and weaknesses in existing protections for privacy, fall within the following broad categories:

- misrecorded credit information;
- incomplete criminal records;
- poor record security;
- the quandary of access to confidential records of government departments;
- persistence of general search warrants;
- survival of outdated provisions of entry and search;
- the absence of any rules governing the use of optical surveillance;
- the absence of any effective law on information protection and information security.

It is impossible to obtain an accurate quantification of the extent of unjustified interference with privacy in Australia. Also, it must be acknowledged that the law can provide only a partial response to invasions of privacy. Nevertheless, wherever complaints mechanisms are made available, they are invariably put into heavy use. The experience of the New South Wales Privacy Committee (NSWPC), and of the Commonwealth and State Ombudsmen, together with computerists' and the public perception of need, as measured in surveys (para. 139–141), indicate that privacy invasion is a real problem for Australian society, the incidence of which is rising. (para. 134)

Classes of Intruders into Privacy

5.10 Any person may cause injury or offence by his intrusive conduct, but special problems arise from intrusions into privacy committed by persons acting as:

- government investigators;
- commissions of inquiry and other government fact-finders;
- private and public police;
- private investigators;
- commercial operators;
- direct marketers;
- journalists and reporters;
- charitable collectors;
- care providers, and controllers and managers of people; and
- researchers.

The risks to privacy interests from intrusive conduct by persons from these classes are accentuated because of the organised and systematic nature of their invasions, and their growing use of new technological devices and management techniques. (para. 144)

Government Investigators

5.11 *Intrusive Official Powers.* Commonwealth officials have myriad powers of intrusion. What emerges from a review of them (para. 152–174) is the lack of consistent principle and the omission in many instances of rudimentary and fundamental protection. The very disparity in the legislative provisions, though doubtless in part explained by the varying circumstances dealt with, illustrates the need for greater order and more consistent preconditions and checks upon the conferring by statute of intrusive official powers. (para. 151, 175)

5.12 *Commissions of Inquiry and Other Government Fact-finders.* The range of personal information held by primary record-keepers in areas prone to the exercise of official powers of access to private information (para. 176–224) is extended by the powers of various commissions, boards, committees and other bodies set up under legislation to find facts and make determinations on behalf of the Commonwealth Government. Any investigative power, whether exercised by an inquiring body

or an investigating official, which allows access to information held by a record-keeper, potentially threatens the privacy interests of both record-keeper and record-subject. (para. 225)

5.13 *Conclusions about Official Powers.* The issues raised by the Commission's review of official powers are:

- Whether so large a range of such extensive powers is really necessary to achieve the Commonwealth's legitimate law enforcement and revenue protection goals.
- Whether sufficient care has been taken, in creating the powers which exist, to define and protect the basic civil rights of those subject to their exercise.
- Whether introduction of further powers of intrusion into yet more aspects of the private life of the individual would result in an undue erosion of personal privacy in Australian society. (para. 236–7)

Private Sector Intruders

5.14 The risks of invasion of privacy from private sector intruders, such as private police (para. 238–244), private investigators (para. 245–8), commercial operators (para. 249–251), direct marketers (para. 252–260), journalists and reporters (para. 261–2), charitable collectors (para. 263), and care providers, and managers and controllers of people (para. 264–277), are not new. What has changed is the technology now readily available to assist the privacy invader. (para. 278)

5.15 Invasions of information, personal or territorial privacy brought about by the new technology will generally go undetected, such is the nature of the activity. Old intrusive methods of investigating and marketing held the risk of detection, because they required a direct approach. The new technology has removed the necessity for a direct approach. While the risks to privacy from intrusive practices were once reasonably redressed within the existing framework of legal protection, the new technology has presented many new problems and greatly multiplied old ones. There is widespread concern that serious intrusions of these kinds can occur with impunity, especially where the commercial or institutional interest is strong enough and its victim sufficiently powerless to make talk of a right to privacy virtually meaningless. (para. 279)

III. HOW THE COMMONWEALTH CAN LEARN FROM OTHER LAW-MAKERS

6. An Emerging Pattern of Laws Protecting Privacy

Developments in the States and at the International Level

6.1 The past 10 years has seen remarkable legislative activity by European and North American legislatures, by Parliaments in the region, and in the States (para. 588), seeking to devise controls and standards in the interests of privacy protection. (para. 586, and Table F) International bodies have formulated recommendations for protection of privacy, and to achieve an appropriate accommodation between it and other no less highly valued interests. Australia is part of an interdependent international community. It is faced with common problems, including privacy protection, the vulnerability of its information handling networks, and criminal activity organised on an international basis. It is 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. (para. 587)

Deriving a View of Fundamental Rights

6.2 Human rights documents, while not exhibiting a uniform approach to mechanisms for their protection, nevertheless show that there is a reasonably consistent view of what should be regarded as fundamental civil and political rights. Treaties have been made relating to protection and advancement of human rights. Their privacy provisions indicate the minimum international standards in this field. (para. 590–1)

6.3 Privacy is not defined in any of the international instruments. However the concept extends to matters which are the concern of this report, such as official intrusions, instrusive commercial and other activities, secret surveillance, information privacy and respect for the privacy of correspondence. (para. 594) Considerations referred to in the international declarations are those to which the Commission must have regard in assessing the compatibility of existing federal law and practice in Australia with the right to privacy. (para. 601)

OECD Guidelines for Information Privacy

6.4 *Development and Adoption.* The Council of the OECD has adopted a recommendation of an Expert Group concerning guidelines to be followed governing protection of privacy and transborder flows of personal data. The OECD guidelines state that 'basic principles of national application' should be regarded as minimum standards, capable of being supplemented by additional measures for the protection of privacy and individual liberties. (para. 602, 603) These have helped shape the Commission's recommended principles for information privacy protection (para. 590–603).

Overseas Laws on Invasive Commercial Activities

6.5 In an attempt to protect the consumer from unfair commercial activity which erodes his privacy interests, overseas inquiries have proposed, and overseas legislatures have enacted, laws aimed at controlling:

- marketing techniques which intrude into his private space or private life, or which use his personal history, independently of his knowledge or consent, and in circumstances where he is powerless to avoid or escape from the intrusion;
- loss of freedom of choice between alternative methods of transacting business according to the degree to which the various methods are potentially threatening to privacy interests;
- deprivation of consumer rights, including privacy rights, through unfair agreements waiving or varying the essential elements of the relationship between the consumer and the commercial institutions with which he deals; and

- deception as to the privacy risks involved in various alternative payment and other business systems procured by false or misleading advertising. (para. 608)

Overseas Laws on Secret Surveillance

6.6 Overseas laws and law reform proposals recognise as basic the principle that a person should not be subjected to secret surveillance of his private space, private life, and personal history. If human behaviour, conversations, and other private matters are to be monitored by third parties, this should normally be done openly, in circumstances where there is no reasonable expectation of privacy, or with the consent of a party being monitored. Overseas laws recognise that secret surveillance devices might be used in certain circumstances by law enforcement officers for law enforcement purposes. In the case of secret surveillance otherwise than through interception of the mail or telecommunications, a wide range of public officials might legitimately be authorised to engage in secret surveillance, provided they do so pursuant to a judicial warrant, and observe certain basic civil rights of the subject. In the case of interference with the mail and telecommunications, however, the classes of officials who might lawfully engage in secret interception are normally more narrowly circumscribed than is the case with other private communications between suspects, and the range of offences for which interception is permissible is usually limited to those of a most serious nature, because of the specially damaging effects of their perpetration upon the community as a whole. (para. 609)

Official Powers

6.7 In assessing laws controlling officials in their exercise of intrusive powers, the requirements of the International Covenant on Civil and Political Rights (ICCPR) need to be considered. (para. 611) Privacy interests might be invaded by intrusive official activity, of which one aspect is the police power to conduct criminal investigations. Existing branches of law controlling criminal investigative activity were reviewed by the Commission in its report on *Criminal Investigation*. Principles were formulated in that report against which existing laws incidentally protecting privacy from intrusive police activity, and proposals for change, might be evaluated and assessed. These principles might be extrapolated to the whole area of official investigative activity. (para. 612) The New Zealand Public and Administrative Law Reform Committee recently presented its report containing general principles which it has formulated, to which powers of entry should generally be expected to conform. The Commission has drawn upon each of these sets of principles in developing standards for devising and reviewing powers of entry. (para. 613)

Overseas Laws on Abuses by Care Providers and Controllers and Managers of People

6.8 It has been recognised in overseas laws and reform proposals, and in international instruments, that vulnerable classes of people living and working in institutional settings should be entitled to independent investigation of their complaints of violations of basic human rights, in particular in this context, the right to privacy; that their complaints should be redressed, if substantiated, through independent guardians; that they should have that degree of access to justice enjoyed by the non-institutionalised person; and that the making of complaints concerning living and working conditions should not lead to retribution or other unfair treatment. (para. 614)

Response by the States

6.9 The common law in Australia (para. 619, 640) provides a basic level of protection for the fundamental values from which privacy is derived. While no branch of the common law specifically addresses privacy interests, it provides them with strong incidental protection where other historically more significant interests are at risk. One of the internationally accepted standards for proper information handling practice is that an individual is entitled, in the interests of his privacy, to protection from disclosure of his personal information, unless with his consent, lawful authority, or pursuant to a publicly known usage or common and routine practice. The common law already provides this protection where the information is 'confidential'. (para. 640)

6.10 State governments have also been active in their response to the privacy threat, although usually in the name of protecting other related interests, and through mechanisms only incidentally concerned with privacy. Protection, whether direct or incidental, is provided in the States through:

- *Ombudsmen.* (para. 620)
- *Consumer Protection Laws.* (para. 621)
- *Privacy Committee.* (para. 622)
- *Territorial Privacy Protection.* (para. 623–6)
- *Access and Challenge to Credit Reports.* (para. 627)
- *Secret Surveillance Laws.* (para. 630)
- *Lie Detectors.* The New South Wales Parliament has recently enacted legislation to forbid the use of lie detectors (polygraphs) and voice stress evaluators. (para. 631)
- *Freedom of Information Laws.* Of the Australian States, only Victoria has provided information privacy rights. (para. 632)
- *Secrecy Provisions in Public Service Legislation.* (para. 639)
- *Human Rights Protections.* When privacy interests are invaded, it is rare that the complaint does not involve a claim to vindication of other related grievances. This is particularly so in the institutional and employment contexts. (para. 641) Many of the private activities and environments provoking concern because of their apparent disregard of human rights, including privacy, are in fact already heavily regulated. (para. 646)

Implications of the Privacy Decade for Commonwealth Law-Making

6.11 More needs to be done for effective protection of privacy than mere reliance upon existing fragmented mechanisms concerned primarily with other aims and policies, and only incidentally, with privacy. An expert privacy body should have a mandate which is not limited to privacy should have powers of a kind needed to encourage greater respect for this and other related human values. The privacy guardian should be part of a broader human rights protection body. The guardian should have powers in both public *and* private sectors, for the same kinds of abuse and injury to privacy can occur in each. Short-term inquiries into privacy are limited by terms of reference reflecting contemporary assessments of the situation. Parliaments, on their own initiative, and on the initiative of their law reform bodies, can thus only go so far, on the information made available to them through such inquiries, towards meeting needs for protection of privacy. These needs are continually shifting. The expert privacy protection body must have a law reform inquiry function. It must address new needs, deduced from aggregation of experience of complaints and its own investigative and inquiry role, as they arise. And it must be equipped to propose new laws for speedy implementation by Parliament to fill the gaps in privacy protection in Australia as they are clearly established. (para. 648)

IV. HOW THE COMMONWEALTH CAN CONVENIENTLY BUILD UPON EXISTING LAWS PROTECTING PRIVACY

7. Federal Privacy Laws

Significance of Existing Federal Laws Protecting Related Interests

7.1 When privacy interests are invaded, the complaint usually involves a claim to vindication of related grievances. It is thus pertinent, in a reference limited to the Commonwealth public sector and the private sector in the Territories (para. 7), to consider the extent to which the federal institutions have developed or established laws and guidelines, and created specialised bodies for the protection of interests related to that in privacy. Such bodies, in their efforts to improve protection under a heading of abuse not classified as 'privacy', can protect that interest. (para. 649) The need for new laws can only be assessed on the basis of a thorough review of what already exists.

Heads of Existing Protection in Federal Jurisdiction

7.2 The following protections already exist:

- *Trespass*. The common law of trespass to person and property applies in federal jurisdictions, such as the A.C.T., and to Commonwealth government officials pursuing their activities in the States. The problem is that government officials may in the past have been, and might in the future be given, powers of arrest, entry, inspection or summons which are unnecessary, or unnecessarily intrusive. (para. 653)
- *Ombudsman*. The Commonwealth Ombudsman's powers are circumscribed in a number of respects, the most significant being that the Ombudsman cannot overturn a Commonwealth public authority's decision and substitute his own. (para. 654)
- *Complaints against Police*. The Complaints (Australian Federal Police) Act 1981 lays down detailed procedures for handling complaints against police. Complaints which may be made
- under the Act include complaints about invasions of privacy by the Australian Federal Police (AFP). (para. 655)
- *Human Rights Commission*. The establishment of the HRC under the Human Rights Commission Act 1981, is part of the Commonwealth's implementation of the ICCPR. The International Covenant covers a wide variety of human rights, including protection of privacy. The HRC thus already posseses privacy protection functions in relation to the Commonwealth public sector and the A.C.T. The HRC's functions include investigation and conciliation of complaints about breaches of any human right and, either on its own initiative or at the request of a Commonwealth Minister, reporting as to laws that should be made or action taken by the Commonwealth on matters relating to human rights. (para. 656)
- *Public Service Guidelines*. The Australian Public Service Board's guidelines encourage public servants with intrusive powers to exercise them with regard to privacy considerations. (para. 657)
- *Control of Commercial Activity*. Unfair commercial activity destructive of privacy interests in areas of Commonwealth responsibility is governed by a body of legislation, comprising Commonwealth Acts and Territory Ordinances, broadly similar to State consumer protection legislation. (para. 658)
- *Intrusive Activity by Private Agents and Others*. There is no separate and identifiable body of law in Australia governing search, seizure and entry by private individuals engaged to provide security, to investigate matters on behalf of others, to collect debts or otherwise to perform the functions of private agents. Protection from invasion by such persons of 'territorial' and 'personal' privacy is to be found in the general law, whether civil or criminal, protecting the person and property of others. This body of law applies irrespective of the occupational training or status of the person guilty of the invasion. The basic rules to be applied are those protecting

the person and property of an individual from interference by others, and governing the circumstances in which actions may be taken in defence of one's person or property, or the person or property of others. (para. 659–661) The common law rules controlling intrusions have been supplemented in some areas of activity by statutory protections. But even when taken together, these legal protections do not provide a comprehensive protection for privacy. They fail adequately to address the implications of an unequal imbalance of power as between frequently armed security personnel, usually experienced in the application of force, and those who come into the vicinity of the persons or property which the security personnel are engaged to protect. (para. 662) In a legal system which has no constitutional or statutory bill of rights, the tort of trespass provides a theoretical means of maintaining or refining civil liberties. But the reality is that for most people the costs of court proceedings and the inconvenience and loss of time involved, will make it impossible to sue a powerful defendant to vindicate a civil right, such as the perceived right to privacy. (para. 669)

- *Search with 'Consent'*. The rule that interference with the person is unlawful unless with consent, or justified by a wider legal power, such as citizens' arrest or defence of property, provides inadequate protection from the excesses of private agents in carrying out their police role. This is so because of the failure of the law to take account of the realities of the situation of vulnerable individuals, exemplified in dealings with private security. (para. 673)
- *Harassment by Private Agents*. Legislation in all the States and the Northern Territory provides for some control over the activities of private agents. This legislation is neither uniform in the range of activities to which it applies, nor in the extent of controls exercised over those people to whom it applies. (para. 680) None exists in the A.C.T. While it might be argued that licensing would discourage 'disreputable' persons from pursuing these occupations, any privacy protection achieved by this means would be incidental to other aims. For the purpose of preventing undue infringements upon individual privacy, certain activities of private agents need to be controlled. (para. 684)
- *Covert Investigation of Private Matters*. The existing framework of common law and statutory rules affecting aspects of the activities of private investigators presents little deterrent to unscrupulous agents who are prepared to go to any lengths to obtain the information which they are being paid to provide. Particular anti-social activities commonly engaged in by the professional in practising his profession should be prohibited by law. (para. 685)

- *Unordered Goods and Services*. The Trade Practices Act 1974, and State and Northern Territory legislation, contain provisions designed to protect individuals who receive unsolicited goods or services. The effectiveness of existing legislation has been doubted. Regardless of any deficiencies from the perspective of consumer protection, existing legislation fails to address directly the privacy problem. (para. 692)
- *Door-to-Door Sales, Hawking and Charitable Collections*. The physical intrusion arising from the use of door-to-door sales and solicitation techniques is a cause of concern to many people. The uninvited salesman, canvasser or collector intrudes physically into the privacy of the home or its surrounds. Privacy was not the princial concern of the legislative controls on these activities. (para. 694)
- *Abuses by Care Providers, and Controllers and Managers of People*.
  - *Informed Consent*. The basic principle of the common law providing incidental protection to privacy interests threatened by improper practices in treatment and therapy, and in scientific, educational, medical and other research, is that of 'informed consent'. This emphasises the social value that is at stake, *viz.*, respecting the subject's claim to ultimate control over his destiny, including his medical destiny. But its protection is limited, especially where research is conducted by social scientists from disciplines which lack a sound and well established

ethical code of practice, and in experiments for non-therapeutic purposes. (para. 705, 712, 713)

- *Helping Agencies*. As with the States, a measure of control in the interests of privacy upon employment, institutional and research practices is achieved through the Ombudsman. In addition, the HRC has the function of protecting privacy interests, in company with with the other rights protected by the ICCPR. Guidelines drawn up by governmental bodies which attempt to secure the inviolability of the person are rare. Patients' and students' rights are gradually being established in hospitals and schools which respect the inherent dignity and personality of individuals. The pattern of activity has been that of challenge by government inquiry and response by government administration. (para. 714)

• *Intrusive Employment Practices*. The weakness of the common law rules protecting the liberty and privacy of the individual from invasion by private security guards and agents also renders largely nugatory its protection in institutional settings, particularly, that of employment. (para. 719)

- *Medical Examinations and Psychological Testing*. Psychological and medical assessments might be both intrusive and a threat to the subject's information privacy. Such practices would be classified as invasion of a human right presently susceptible to review by the HRC. (para. 720)
- *Surveillance*. Optical surveillance devices may be used to keep employees and others under surveillance. (para. 721) There is at present no legal prohibition upon secret optical surveillance. (para. 722)
- *Recording and other Interception of Employees' Telephone Conversations*. Monitoring systems which use telephones to intercept employee conversations pose privacy problems in whatever contexts they are employed. (para. 724)
- *Security Searches and Interrogation*. Despite the fact that the restraint and interrogation may have been grossly unfair, there will generally be no realistically available remedy. (para. 725)

• *Intrusive Institutional Practices*. The HRC is already active in this area. But ethical codes supposedly guarding against scientific, medical, educational and other research by professionals are too often disregarded. So also is the requirement of informed consent for treatment, therapy and other activities which interfere with the person. And there is no legal restraint upon the secret optical surveillance of inmates in institutions for research, study and other related purposes. (para. 726)

Key to Privacy Protection

7.3 Evaluation of the work of the fragmented, and at present, largely unco-ordinated efforts of boards, committees and other bodies concerned with consumer protection, human rights and related interests, provides the key to privacy protection in Australia. A great amount of work has already been done towards strengthening protection for the entire range of human interests, of which privacy is one. Protection of privacy is in most instances best approached through measures which reflect the nature and needs of particular organisations, their activities, and their role in relation to those who are affected by them. But there should be a basic statement of rights and liabilities, enforceable in the courts, and which particular guidelines and standards, sensitive to the needs and aims of particular organisations and activities, then elaborate or extend. The key to privacy protection in Australia thus lies through strengthening of existing law, encouraging existing bodies already active in the area to expand and elaborate their work in the context of protection of human rights, and stimulating new involvement by bodies with power to address human rights and related issues in particular areas. It is not desirable, at least at this stage, to attempt to create an entirely new and separate body of jurisprudence about privacy. (para. 731) A statutory guardian for privacy should assist consumer protection, welfare, community, professional, and government organisations to ensure that the law,

and particularly the protection which it already *incidentally* provides for privacy interests, becomes more accessible and more relevant to the needs of ordinary people. (para. 733)

8. Federal and State Laws on Secret Surveillance

8.1 The common law gives only limited protection against surveillance. Thus, it is in statutory schemes that protection of privacy from intrusion through surveillance must be found. Such schemes protect the privacy of communications carried by the postal and telecommunications systems. But the tradition of respect for the privacy of communications carried by these systems has been eroded over recent years. Telecommunications legislation now permits interception for installation and maintenance purposes, enforcement of the telecommunications legislation, national security, and investigation of narcotics offences. Postal legislation now permits opening for general law enforcement purposes and for national security. Recent legislation in the field of surveillance outside the post and telecommunications area restricts the use of listening devices in national security cases and in the investigation of some narcotics offences. General controls over listening devices exist only in the mainland States and there is no legislation, either Commonwealth or State, dealing with optical surveillance. (para. 734–5)

8.2 A number of problems and areas of special concern exist:

- Commonwealth legislation regulates the use of listening devices in matters related to national security and the investigation of narcotics offences only. State legislation regulates listening devices otherwise. There is no such legislation in Tasmania, the A.C.T. or the Northern Territory. The laws of the mainland States are by no means consistent in their approach. They do not apply to Commonwealth officers using listening devices in the course of their duty or, at best, their application is a matter of considerable doubt and obscurity.
- Legislation regulating telecommunications interception by law enforcement officers does not sufficiently protect privacy interests in the following respects:
  - there is no specific requirement to consider whether alternative, less privacy invasive, investigative procedures are appropriate or practicable;
  - there is no requirement that the grounds supporting an application for authority to intercept be put in writing;
  - there is no requirement that a warrant authorising interception state with particularity the offence, persons or places that are to be the subject of surveillance;
  - the maximum time limit of a warrant exceeds that provided by most comparable overseas legislation and necessarily exposes many innocent people over a great period of time to unexpected invasions of their privacy;
  - there is no requirement that Parliament be informed of the extent of such surveillance. Whatever the arguments against such disclosure in matters relating to national security, it is difficult to imagine that the publication of such information related to law enforcement would have any detrimental effect.
- The privacy of communications passing over the OTC system is inadequately protected by legislation.
- Recommendations for breakdown in the monopoly of Telecom Australia have clear implications for telecommunications privacy.
- There is no legislation anywhere in Australia to regulate the use of optical devices for secret surveillance.
- All the provisions regulating opening and examination of mail are in the Postal Services Regulations. Some of these regulations are invalid. Powers to open mail should be conferred by the Act, not by regulations.

- The width of the general law enforcement role of Australia Post officers gives considerable cause for concern. They should not be *de facto* policemen.
- The power of Customs officers to open letters not suspected of containing any goods and not suspected of breaching the provisions of the Customs Act goes too far. (para. 785)

9. Federal and State Laws Controlling Personal Information

Collection of Information

9.1 Information privacy interests may be endangered by a record-keeper's collection practices. It is in this context that interests in privacy, and in freedom from discrimination, overlap. Commonwealth initiatives aimed at combating discriminatory practices incidentally protect interests commonly regarded as falling under the umbrella of privacy. (para. 788) But there are many gaps, particularly in the areas of:

- compulsory collections. (para. 793)
- coercion and deception. (para. 794)
- third party sources of personal information. (para. 797)

Existing General Controls on Use of Personal Information

9.2 There are, at present, few statutory controls, or departmental, industry, professional or other guidelines, which specifically attach themselves to the *use* of personal information by its collector (as opposed to disclosure of that information to third parties). There are certain controls on the use of particular categories of information where that information is very sensitive in a political sense, or involves national security or defence. (para. 799–800) Federal administrative law also affords some control over the use of personal information. The rule that the requirements of natural justice be observed, as well as being directed to procedural fairness, has the effect of requiring as much relevant information as possible to be provided to the decision-maker before the decision is made. These rules thus indirectly serve information privacy interests. (para. 801) Use of information by both officers and temporary employees of the Public Service is controlled by the Public Service Regulations. (para. 802)

General Law Controlling Disclosure of Personal Information

9.3 The main body of law controlling disclosure of personal information by both public and private sectors is to be found in the law reports. While the subject of personal information has no general remedy for invasion of privacy interests through its 'improper' disclosure, various common law and equitable remedies provide incidental protection. These remedies apply in relation to misuse by both private and public sectors. (para. 805) They include:

- defamation. (para. 806–810)
- negligence. (para. 810–4)
- passing off. (para. 815–8)

Limitations of Civil Remedies

9.4 The arguments against creation of a new statutory tort of invasion of privacy inevitably point up inadequacies in the existing system's incidental protection through established tort remedies. The deficiencies in the tort remedy approach include:

- *Lack of Awareness*. Any legal remedy — including a tort action — addresses the relatively rare situation where a data subject becomes aware of mishandling of information concerning him.
- *Cost*. The ordinary person is unlikely to pursue a tort action because of the heavy cost of private litigation.

- *Trauma*. In the case of an invasion of privacy, resort to a court may involve a quite traumatic abandonment of privacy by the litigant in order to remedy the infringement of it.
- *Retrospective Action*. Whereas the adoption of fair information practices affects future conduct, court decisions in most instances operate only retrospectively.
- *Unsuited to Task*. Courts are not well placed to resolve the competing interests involved in claims of invasion of privacy.
- *Inappropriate Remedies*. Damages are largely inappropriate as a means of redress for privacy invasion. The courts are understandably reluctant to issue the more appropriate remedy of the injunction to restrain infringements of personal interests, especially where this will interfere with freedom of expression. (para. 819)

9.5 A further limitation upon the capacity of the torts system to protect information privacy interests is its concentration upon one aspect only of the range of conduct endangering such interests, *viz.*, improper disclosure of personal information. Other areas of information mishandling are simply not addressed by the torts system, in particular, mishandling through improper practices in the context of:

- collection,
- access and challenge,
- internal use, and
- storage and destruction of personal information. (para. 820)

Copyright

9.6 The major limitation of copyright as an incidental protector of privacy is that, being a proprietary right, some tangible opus must exist. It is of very limited use in the protection of information privacy. (para. 823)

Privacy Protection through the Law of Contract

9.7 Many of the clearly established categories of confidential relationships in which privacy interests are seriously at risk because of the new technology are contractual. But this need not necessarily be so. Furthermore, the clients of Commonwealth Government departments and agencies generally have no contractual relationship with those with which they deal, reducing the impact of contract law as a privacy protector in that significant context. (para. 826)

Duty of Confidence

9.8 The Commonwealth has already moved to protect certain information privacy interests under the Freedom of Information Act 1982. Under that Act there is an exemption to the right of access where it would result in breach of another person's legal right to maintain the confidentiality of the information to which a person is seeking access. Thus, it is important to examine existing law relating to protection of confidential information, not only for its significance in protecting information privacy interests from invasion through improper disclosure of personal information, but also, for the extent to which existing access rights are qualified by the need to protect the confidences of others. (para. 827)

9.9 The action for breach of confidence provides a civil remedy for use or disclosure of information which is not publicly known and which has been entrusted to a person in circumstances imposing an obligation not to use or disclose that information without the authority of the person from whom it has directly or indirectly been obtained. Its precise basis, elements, ambit and application have been the subject of much judicial and academic attention. Gaps have been found, and proposals for statutory reform have been advanced (para. 828), particularly in the following areas:

- *Information Capable of Protection*. Breach of confidence law is concerned with the protection of facts which are 'confidential', i.e., which are not in the public domain. (para. 855)
- *Circumstances Importing a Duty of Confidence*. The information must also be imparted in

confidence or acquired by a confidant 'in his character as' such, or acquired by reprehensible means. (para. 856)

- *Test Case*. Few actions have been brought for breach of confidence outside the areas of trade secrets and a limited number of professional relationships. (para. 857)
- *Breach of Duty of Confidence*. In order to prove breach of confidence, it might be necessary to penetrate the management and record-keeping systems of a large and powerful organisation. (para. 858)
- *Defences*. There is undesirable uncertainty associated with the extent to which 'public interest' might be relied upon to justify an unauthorised disclosure of personal information. Those undertaking clinical data trials, epidemiological research projects and other projects dependent upon a large supply of personal information, should not be encouraged to justify them by reference to an expansive concept of 'public interest', but through legislation specifically authorising a particular activity. (para. 859)
- *Standing*. A fundamental rule of the law of breach of confidence would prevent it from ever providing effective protection for information privacy interests as such — at least if unassisted by some legislative broadening of its boundaries. This is the *general rule* that only the person to whom the legal duty of confidence is owed is entitled to enforce the confidence. That rule operates to defeat privacy claims whenever the confided information pertains to a third party, and that communication is not itself a breach of confidence. (para. 860)
- *Remedies*. Like the tort actions incidentally protective of privacy interests, the action for breach of confidence can only operate in the face of a threatened breach, or where the breach has already occurred. Proper protection of information privacy should be principally concerned to prevent the misuse of information in advance. (para. 861)
- *Continuing Uncertainty*. Each of the principal aspects of the present law is still subject to some uncertainty, although it appears to be developing in a reasonably consistent, yet flexible, fashion. (para. 862)

Conclusions about the Duty of Confidence as it Protects the Privacy of Key Relationships

9.10 The law relating to breach of confidence more directly and comprehensively protects information privacy than any other legal remedy. Its strength lies in the wide and flexible coverage which its rules afford and in the balance it achieves between privacy and other competing interests. It applies to a potentially wide range of relationships. Damage is not required for a remedy to be available. It recognises flexible defences which appropriately balance public interests competing with the claim to non-disclosure. Its deficiencies are its remaining uncertainties, the inevitable slowness with which they are being resolved, and the standing rule, which acts as an arbitrary cut off point for remedying invasions of privacy flowing from breaches of confidence. And it is limited to the context of unauthorised use or disclosure of information. It does not address aspects of information handling such as 'collection', or 'security'. (para. 930)

Reform of the Duty of Confidence

9.11 *Building on the Duty of Confidence*. The best way to protect information privacy from *unauthorised use or disclosure* of personal information is to build upon the legal duty of confidence. It would be going too far in the interests of privacy to enact in legislative form all of those proper information handling principles relating to the handling of personal information recognised by international instruments and overseas laws, in particular, that controlling improper use or disclosure, and to provide civil or criminal remedies for their breach. To provide, for example, an enforceable right in a record subject to non-disclosure of personal information held about him by any record-keeper, except with his consent, or by authority of law, would be too radical an alteration in the present framework of legal rules, provided principally by the law of defamation, injurious falsehood, passing off, copyright, and breach of confidence. (para. 932)

A Statutory Tort?

9.12 A statutory tort of breach of confidence is not required in Australia, at least for the purpose protecting interests of privacy. (para. 934–5) The balance of advantage lies in favour of making statutory clarifications and minor modifications to the general law of confidence rather than codifying it. For the rest, the law can safely be allowed to develop through judicial decision-making on a case by case basis. In particular, there would be dangers in attempting to formulate through statute a list of the available defences to an action for breach of confidence, as this might inhibit judicial development where a record-keeper challenges his liability of what on initial analysis seems a breach of confidence, on the ground of some wider public interest. (para. 936)

10. Flow of Information in the Public Sector

Statutory Controls: A Summary

10.1 The Crimes Act 1914, s. 70 and s. 79, and the Public Service Act 1922, s. 51(1) and the Public Service Regulations, reg. 35, provide the general framework for controlling disclosure of personal information by government officials working in record-keeping systems for which there is no special legislation. Most government departments and agencies have established guidelines controlling their internal operations which control the flow of information acquired by the agency. Such guidelines may specifically address privacy concerns, or may deal with them only incidentally. Public sector information flow may involve disclosure to the private sector. This is controlled by the same general limitations which apply to internal government use. However, the threat to privacy interests may be greater. Although much of the legislation which permits disclosure of information to the private sector imposes a duty upon the recipient to restrict its further disclosure, the wider the dissemination of personal information, the harder it is to enforce any restrictions on its further use. (para. 937) The basic framework might be criticised as allowing discretionary secrecy. And that which allows 'discretionary secrecy' also allows 'discretionary disclosure'. The Chief Officer of a Commonwealth department or agency governed only by the Public Service Act 1922 and the Crimes Act 1914 might purport to authorise disclosure of personal information inimical to the privacy interests of the subject. (para. 948)

10.2 Provided the disclosure is 'authorised', and there is a 'duty to communicate' or no 'duty not to disclose' (whatever these phrases might mean), s. 70, s. 79 and reg. 35 impose no restriction in the interests of privacy. There will also be many situations where some might think disclosure is justified on the basis of the greater interest of the subject or of the public, notwithstanding that there was no consent to the disclosure, and the further use of the information was unrelated to the original purpose of its collection. Again, s. 70 and reg. 35 provide no protection for disclosures which would be in the public interest and which, by any standard, would be regarded as justified by the community at large. (para. 949)

Specific Laws

10.3 As well as the general laws restricting disclosure of public sector information, some areas of record-keeping are covered by specific laws. As with the general secrecy provisions, disclosure of information by government agencies controlled by particular legislation depends largely on the discretion of the Chief Officer of the agency involved, and a concept of the employee's 'duty'. (para. 950)

Commission's Approach to Control of Flow of Public Sector Information

10.4 The legislative framework for control of public sector use of personal information can only be viewed as inadequate as a protector of private interests if it is forgotten that, as an essential strand, it includes the law relating to the duty of confidence. New laws are not needed for the protection of private rights in this context. But existing law needs to be more widely known and better understood. (para. 952)

The ramifications of existing law establishing duties of confidence for public sector use of personal information do not seem to be sufficiently understood by those working within, or dealing with, government departments and agencies. The draft Bill which accompanies this report seeks to meet these needs. (para. 953)

11. Adjudication of Disputes and Disclosure of Personal Information

11.1 Administration of Commonwealth systems of courts and tribunals, and initiation and pursuit of proceedings therein, give rise to a vast bulk of personal information concerning litigants, witnesses and others, some of which may be highly sensitive. Some of this information might have been impressed with the quality of confidence (see s. 9.9) prior to its flowing into the judicial or tribunal systems. (para. 954)

11.2 The courts have recognised the need to preserve confidential relationships. They have developed rules controlling interference with those relationships through mishandling of personal information by record-keepers — the duty of confidence. The need to preserve confidential relationships is also recognised in relation to court proceedings by the law of evidence relating to privileged communications, and rules of practice and procedure. Rules of evidence can only protect privacy interests in so far as those interests are threatened by disclosure of personal information in court. Some communications are guaranteed a certain level of protection from court disclosure. Some courts and tribunals are closed to the public. And there are general powers to close courts and tribunals, or to prohibit publication of information divulged therein. Such legislation allows the courts to resolve the tension between public interests in open justice and full judicial access to all the information relevant to achieving a just solution in a dispute between persons, on the one hand, and private interests, such as those in privacy and confidentiality, on the other. (para. 977)

11.3 It is proposed, however, that the statutory guardian recommended by this report should have power to monitor this and other areas of public administration in the interests of privacy, and to report to Parliament where concerns arise which need to be resolved through legislative intervention. (para. 978)

12. Access, Challenge and Correction of Personal Records

Information Privacy Rights

12.1 Unlike their counterparts at the State level, the Commonwealth Parliament and Government have been active in conferring 'information privacy rights' upon those subject to their powers, whether through new statutory law, in particular, the 'new administrative law' (para. 981), or through departmental and agency guidelines and internal procedures. In two areas, existing bodies of law and practice come close to meeting the proper information handling standards reflected in overseas laws, *viz.*, access to and disclosure of personal information. (para. 979) But there are serious inbuilt limitations on the extent to which 'new administrative law' can effectively protect the information privacy. (para. 933)

Rights of Access by the Data Subject

12.2 The Freedom of Information Act protects personal information by providing, in some circumstances, a right of access by the person concerned to documents containing personal information about himself. But this should be seen in context. The Freedom of Information Act is not a Privacy Act. It is an Act intended to open public sector information to the world at large. The interests to be balanced are the interests of the public at large against the interests of individuals (whose privacy might be unreasonably invaded), corporations (whose business secrets and other confidential information might be unreasonably disclosed) and public administration (which might be substantially prejudiced if certain information were disclosed). Because the Act is directed to

disclosure to any person, the individual whose records are kept by an agency is in the same position as any other person when it comes to getting access. He must rely on exactly the same provisions of the Act, and surmount exactly the same obstacles under the Act, as anyone else who wishes to gain access to documents about himself. (para. 1001)

Challenge

12.3 The other aspect of access, the fundamental principle of privacy protection, is the right to challenge and correct incomplete, out-dated or otherwise misleading information held in records. This aspect is also included in the Freedom of Information Act. However, there are some significant limitations on the right. (para. 1003) As might be expected in an Act which is not specifically designed to protect privacy interests (except incidentally), there are a number of deficiencies. Comprehensive privacy legislation is still needed properly to protect privacy so far as Commonwealth public sector information is concerned. (para. 1004)

Departmental and Industry Guidelines allowing Access, Challenge and Correction

12.4 Various sets of guidelines, applying in both the public and private sectors, recognise that employees and other personal record-subjects should be given access to personal records concerning themselves, for example, the set of guidelines developed by the Australian Public Service Board allowing public servants access to their personal records. (para. 1005)

Conclusions about Existing Rights of Access, Challenge and Correction

12.5 While the new federal administrative law, including the Freedom of Information Act 1982, provide an essential background for introduction of information privacy rights (para. 1009), the system does not go far enough in protecting information privacy interests. This is not its primary purpose. The strong claim of the individual, whether resident or citizen, to a right of access to information about himself has received only limited recognition, and the existing right is limited to the Commonwealth public sector. In order for information privacy interests to receive adequate protection, the subjects of personal information held in both public *and* private sectors should be provided with accessible and flexible access, challenge and correction rights. (para. 1010)

13. Storage and Destruction of Personal Information

Existing Regulatory Framework

13.1 Those informal guidelines which exist in the private sector are isolated and piecemeal attempts to come to terms with the data security problem, principally, in the interests of protecting the revenue and secrets of the record-keeper, rather than the privacy interests of his subjects. (para. 1011) The Auditor-General is one of several Commonwealth authorities with power to develop standards for the security of public sector information in the interests of privacy. (para. 1012) The Australian Public Service Board also has a function of providing advice and assistance to departments on measures to improve management systems and efficiency. (para. 1013)

13.2 In responding to the privacy problems created by extensive computer use at the Commonwealth level, it is important to draw upon the experience and expertise of the Bureau of Statistics, the Australian Public Service Board, the Auditor-General, and other Commonwealth agencies with powers or responsibilities in the area. These bodies have already developed guidelines in the interests of privacy protection. If there were a central agency, a privacy guardian, with the power to co-ordinate and develop such initiatives, they could provide the basis for a regulatory framework essential for protection of the integrity of personal data used by all Commonwealth departments and agencies. (para. 1016)

Archival Policy

13.3 One of the international privacy protection standards, in relation to the removal of information

from systems, is that the record-keeper should not keep personal information once it is no longer relevant to the purposes which govern the collection of the information or to any continuing relationship between the record-keeper and the record-subject. There have been few voluntary initiatives from the private sector to meet this standard. In contrast, the Commonwealth Government has, at least administratively, been extremely active. The exhaustively developed archival policy of the Commonwealth Government contrasts with the haphazard guidelines and practices of private sector record-keepers. (para. 1017)

Assessment of Government Archival Policy and Archives Practice

13.4 The Australian Archives provides vital data for research in fields such as demography, anthropology, health and education, based on use of information about historical samples of individuals. These processes would be hindered if the records available were incomplete. But for the future, as Archives' policies and practices become more highly developed, systematic and exhaustive in their coverage, procedures must be instituted to ensure that privacy interests receive appropriate weight in the balance of competing claims. The individual's interest in privacy must be balanced against the value to the nation of its archival resources. Safeguards built into existing policy and practice, providing for exemptions and exclusions in the case of highly sensitive material, attempt to achieve a satisfactory balance of these competing interests. But a statutory guardian for privacy, through handling of complaints and monitoring of current practices, should continually check and review this balance. (para. 1030)

14. Conclusions about Existing Privacy Protections

14.1 The report traces the flow of personal information generated in particular sectors of record-keeping activity through to other sectors, to different branches of particular sectors, into the court and tribunal systems, and in the case of public sector information, to its deposit with Australian Archives. The background laws controlling this flow are primarily concerned with protections of such interests as secrecy in some areas of government and public administration, maintenance of trade secrets, and maintenance of confidential and other important personal relationships, against harm from a record-keeper's unauthorised use or disclosure of the information. Outside the area of unauthorised use or disclosure, some attention has been paid to development of principles for maintenance of the security of information. Laws and practices are also being developed to secure the orderly process of archiving information acquired by the Commonwealth public sector. And there is a new body of statutory law providing rights of access and challenge to information held by government agencies. The framework of existing laws, practices and procedures limiting use, safeguarding security, and encouraging individual participation in the handling of personal information needs to be supplemented, not only to secure better protection of privacy interests threatened by misuse, inadequate security, and denial of access, but also, to secure a suitable threshold level of privacy protection in areas at present largely untouched by laws, standards or guidelines for the handling of personal information. Of particular concern from this point of view are the processes of collection, and the maintenance of quality of personal information used by record-keepers. Encouragement should be given to the adoption of standards requiring record-keepers to specify the purposes for which their data might be used, and to be open about developments, practices and policies with respect to the personal information which they hold. (para. 1031)

V. HOW THE SCHEME FOR PRIVACY PROTECTION SHOULD BE FLEXIBLE, SENSITIVE AND MULTI-FACETED

15. Basic Responses to the Privacy Problem

Need for a Statutory Guardian

15.1 As a basic response to the privacy threat, a statutory guardian, in the form of an administrative body with the specific function of advocating privacy interests, should be established. Further legislation to protect some aspects of privacy interests presently under threat is also needed.

Functions of the Statutory Guardian

15.2 The basic functions which the proposed guardian would perform are:

- inquiry into, and conciliation and resolution of, disputes;
- monitoring activity and technological advances that might interfere with privacy;
- fixing standards and publishing guidelines;
- providing community education about privacy; and
- advising government, industry and the professions.

The privacy guardian should be set in an interdisciplinary, generalist context. Privacy is an expression of more fundamental values. Thus, the body with the functions that are needed to protect privacy interests should not be limited to their protection. It should be able to consider privacy problems in the context of the other values and interests needing protection in a society undergoing rapid social and technological change. (para. 1049) When decisions are being made about a new information system or a new form of intrusive conduct, the advantages of the proposal from the point of view of increased efficiency to areas such as health administration and law enforcement will generally be fully considered, but the extent to which the proposal interferes with privacy might not. This will be one of the key functions of the statutory guardian.

Existing Administrative Structures

15.3 *Ombudsman's Role.* There are two Commonwealth institutions already in existence with power to protect privacy, the Commonwealth Ombudsman and the HRC. The powers of other Commonwealth institutions are too specialised to warrant consideration as a privacy guardian. The Commonwealth Ombudsman is a statutory officer. Limitation of the Ombudsman's jurisdiction to the public sector is significant. There are strong reasons for retaining this focus of attention. To extend his role to the private sector would distort his primary role as a public sector 'bureaucracy watchdog'. But the administrative body needed to protect privacy clearly must be able to operate both in the public and private sectors. There is no adequate logical, philosophical or practical basis for differentiating between the two sectors in protecting privacy interests. It would be confusing and wasteful to have separate bodies for each sector: the Ombudsman only for public sector privacy concerns; another body only for private sector concerns. (para. 1050-4)

15.4 *Functions of Human Rights Commission.* The HRC already possesses privacy protection functions in the areas covered by the Commission's Reference — the Commonwealth public sector and the Territories. In summary, the HRC's functions are:

- the investigation and conciliation of complaints about human rights;
- the monitoring of Commonwealth government activity related to human rights;
- the monitoring of private sector activity in the Territories (other than the Northern Territory) related to human rights;
- advising the Commonwealth government on matters relating to human rights;
- public education; and
- research into human rights. (para. 1052)

15.5 Extensions of the HRC's functions necessary to accommodate this Commission's proposals will not distort its basic role. Through the co-operative arrangements made with the States and the Northern Territory, it will be able to further develop expertise and experience in the area of privacy. The facility for consultative committees to advise the HRC will also assist in achieving national coverage of the principles of privacy protection which this Commission recommends should be adopted. The HRC should be charged with administrative and other functions necessary to implement the recommendations in this report. In particular, the HRC should be specifically empowered to publish guidelines in particular areas or to help overcome problems of more general application. Guidelines should be regarded as refinement of the general principles enunciated in this report. They should not be restricted to information privacy concerns. The areas of direct marketing, or the exercise of official powers of intrusion, are areas where detailed guidelines will prove useful. (para. 1054)

15.6 *Consultation with Human Rights Commission.* Ministers should involve the HRC in consideration of draft legislation which may threaten privacy interests. Arrangements might include forwarding policy proposals and draft legislation to the HRC for comment or even involving officers of the HRC in interdepartmental committees and working groups considering proposed legislation. It would also be open to the Parliament and its committees to draw on the expertise and experience of the HRC when privacy issues arise in draft legislation. In particular, the Senate Standing Committee for the Scrutiny of Bills and the Senate Standing Committee on Constitutional and Legal Affairs, both of which have responsibilities in relation to human rights, including privacy, may develop a close working relationship with the HRC. In addition, the HRC should provide a standing source of information and advice to departments and other public sector bodies on privacy issues. (para. 1056)

15.7 As the experience of the HRC in dealing with privacy issues expands, it might come to the view that the more flexible mechanism for particular codes of practice is needed. It might conclude, for example, that the primary or subordinate legislation are not appropriate but that the informal and unenforceable guidelines do not go far enough. It may recommend a new way of implementing particular codes of practice. It should be a matter for the HRC to determine the most suitable way to implement any particular proposed standard that it formulates. (para. 1057)

Privacy Commissioner

15.8 *Allocation of Functions.* Although the HRC is the obvious body to exercise the administrative functions which arise from this Commission's recommendations, it is not appropriate simply to repose all of those functions in the HRC as a whole. It is necessary to have a member of the HRC, a Privacy Commissioner, specifically designated to exercise some of these functions. (para. 1058) There are real benefits to be gained from having a specific, publicly identifiable person who has the primary responsibility for dealing with privacy complaints. (para. 1059-60)

15.9 *Privacy Commissioner as Member of the Human Rights Commission.* The Privacy Commissioner should be a full-time member of the HRC. The Privacy Commissioner's membership of the HRC would benefit the Commission and enhance his own ability to carry out his functions. His work would benefit from the wider perspectives available through the HRC's involvement with all human rights concerns all over Australia. The decisions he will have to make will be more soundly based if he has the benefit of intimate access to the HRC and, through it, to other bodies in and outside Australia concerned with human rights in general. (para. 1061)

15.10 *Value to the Human Rights Commission.* As a member of the HRC, the Privacy Commissioner would play an important role in the development of privacy policies consistent with general developments in the field of human rights. His experience of the problems and difficulties affecting privacy makes it essential that he be involved in the continuing task of formulating the standards and guidelines which the HRC will issue. It will be necessary, too, for the HRC to use his experience while advising government. The level of involvement which is needed to ensure that his experience is used to the full will not be reached unless he is a member of the HRC. Finally, there is a danger that

generalist bodies such as the HRC may consider questions only in the abstract. The Privacy Commissioner's practical experience in tackling a particular human right and in evaluating claims for privacy against claims for other legitimate and competing human rights will have significant practical value to the HRC as it addresses wider, non-privacy concerns. (para. 1062)

15.11 *Directions*. The Privacy Commissioner, under the Commission's recommendations, should have the power to issue binding and enforceable orders. These orders should be appellable to the Administrative Appeals Tribunal. It is inappropriate that this power, to be conferred by statute, be governed as well by a direction power from the HRC as a whole. Nevertheless, it is desirable that the HRC be kept fully and closely informed on the way in which the Privacy Commissioner performs his functions. He should be required to provide the HRC with reports on his activities unless the HRC has indicated otherwise. (para. 1065)

15.12 *Relationship with Ombudsman*. Provision should be made for the Privacy Commissioner to refer complaints to the Commonwealth Ombudsman. The Commonwealth Ombudsman, for example, might be the more appropriate body to deal with some complaints about interferences with privacy (or other human rights) by public officials. In appropriate cases, if the complainant agrees, there is no reason why the Ombudsman should not investigate a complaint, made initially to the Privacy Commissioner, that a Commonwealth or Territory authority has interfered with privacy. There is no reason why a similar complaint made to the Ombudsman should not be investigated by the Privacy Commissioner, if that is more appropriate. The secrecy provisions of the Ombudsman Act 1976 should be amended to allow both the Privacy Commissioner and the Ombudsman, with the agreement of the complainant, to transfer complaints, and the results of investigations. (para. 1066)

16. Implementation Issues

16.1 *The following are the issues to be canvassed in devising an appropriate scheme:*

- *Need for Legislative Standards and Protections*. More is needed for privacy protection than guidelines and statements of aims. There is already a long tradition of protecting privacy interests by law. In some matters at least, legislative standards and protections for privacy are needed. (para. 1067)
- *Limits of Legislation*. However, the formal apparatus of the law is not always the most appropriate to protect privacy interests. In particular instances, the need for flexibility in the face of rapidly changing technology makes detailed statements of legislative duties inappropriate. There is a place for codes and guidelines, as well as legislation. A well designed regime to protect privacy will provide each, where appropriate. (para. 1069)
- *Conciliation and Negotiation*. An important way of implementing privacy principles is to provide a mechanism for ensuring conciliation and negotiation between a complainant and an alleged privacy invader. Success depends upon the skill and effectiveness of the negotiator. It can be rendered ineffective when the party in the dominant position — the privacy invader — is simply unwilling to be deterred from a course of conduct, or even to engage in meaningful negotiations. To guard against this latter possibility, the Privacy Commissioner should be able to call conferences at which attendance of the parties involved would be mandatory. For many complaints, conciliation and persuasion are appropriate and effective. Some complainants may not wish to use court-based remedies, even where available — they may fear that the courts are not able to cope sensitively with the information or behaviour which is at the core of the dispute or they may be deterred by the costs, delay and other pressures associated with court litigation. (para. 1070)
- *Publicity*. Another means of ensuring that privacy principles are implemented is publicly to name those who flagrantly or persistently violate them. Care needs to be taken, especially where the reason for publication is only the breach of unenforcable, non-statutory guidelines, that the

publication of names of 'privacy invaders' is not an interference with the privacy, and other rights, of those who breached the guidelines. And publication might not deter some people. More importantly, the effectiveness of publicity as a sanction is not certain. The extent of publicity usually depends on the views of editors and journalists on whether the item will interest the public. Finally and most importantly, there is no appeal. Even a correction or retraction might be difficult to obtain, especially once the item has ceased to be newsworthy. (para. 1071)

- *Public Education.* Of greatest importance to the implementation of the privacy regime is education of those whose activities may interfere with privacy. As well as the HRC's public education function in relation to general human rights the steps already taken within the Australian Public Service as a result of the introduction of freedom of information legislation will provide a useful model for public education in both the public and private sectors. Because the recommendations in this report go beyond the public sector and affect private sector activities in the A.C.T., the HRC should give consideration to an intensive public education program, including, where appropriate, the conduct of seminars, and production of pamphlets, video cassettes and films, within the A.C.T. and more generally. (para. 1072)
- *Licensing.* Another means of ensuring that privacy principles are implemented is to prohibit the carrying out, without approval, of a particular activity that may interfere with privacy. (para. 1073) For reasons explained below (s. 25.6), licensing is not recommended.
- *A General Tort.* The 'general tort' option involves creating a right to claim damages in respect of any 'interference with privacy'. (para. 1075) The case in favour is that it would:
  - cover almost all the privacy situations which could be conceived, even those which have not yet become apparent;
  - give a remedy to all those seriously prejudiced by intrusions into privacy;
  - allow juries to set the standard in a constantly changing area of human values;
  - provide an effective remedy for any unreasonable behaviour, including governmental activities;
  - fulfil obligations under the Universal Declaration of Human Rights and the ICCPR. (para. 1078)

  Such a tort would be too vague. It would need to be worked out, case by case, as courts and administrative tribunals grappled with particular fact situations that came before them. In time, the limits of the tort might ultimately be fixed. But until then, it would not be clear how it would affect freedom of the press, of speech and of information. The Commission has concluded that a general tort of 'interference with privacy' would be undesirable at this stage. (para. 1079, 1081)
- *Tort Remedy where Specified Standards Breached.* It is not appropriate that all breaches of privacy standards should give rise to action in tort. The degree of authority of the standards will vary. So will the degree of their particularity. Some will be very general, while others will be extremely particular. The question of whether a breach of any particular standard should give rise to tort liability should be resolved in the context of framing that standard. The Commission recommends only that breach of the disclosure standard should give rise to tort liability, and in limited circumstances, (s. 25.50-4, below) related to liability for breach of confidence. (para. 1085)
- *Criminal Remedies.* The criminal law already plays a significant part in protecting personal privacy. This is more so in the area of intrusive conduct than in information privacy. But even in the area of information privacy, significant privacy protection is available through the criminal law, especially so far as the unauthorised disclosure of information by government agencies and officers is concerned. There is undoubtedly a place in any privacy regime for the criminal law. But care must be taken. For the same reasons that a general right to privacy, enforceable by civil action, is not recommended, breach of privacy standards should not, in general, be a criminal offence. Where the criminal law presently protects privacy, that protection should be continued.

If necessary, it should be reinforced. But criminal liability should only be extended by legislation where the privacy-invasive activity can be clearly identified in the legislation creating the offence. Clarity is one of the essential ingredients in criminal law. (para. 1086) There are serious problems in rejecting completely any form of legislative response. The need can best be met by a judicious mixture of judicial and administrative mechanisms, provided within a legislative framework. (para. 1087)

17. Uniformity Considerations

Information Standards

17.1 In formulating the standards recommended in this report, the Commission has paid close regard to the international instruments sponsored or approved by these bodies. Australian information protection and privacy laws should not be significantly different from those applied overseas. Australia's trade links with OECD and other countries will inevitably lead to increased information flows. It may well be that countries which have strong information protection mechanisms will be reluctant to allow at least some information flows to countries with inadequate protections for information privacy. Indeed, it was this consideration which led the OECD to formulate its guidelines. (para. 1089)

Intrusions Standards

17.2 It is desirable that a person's privacy should not be more at risk in one part of Australia than in another. Some kinds of intrusive conduct that interfere with privacy can be dealt with on a national basis. Telecommunications and postal services are matters within the Commonwealth Parliament's constitutional competence. But in other respects (for example, the use of listening devices) the States have accepted legislative responsibility. (para. 1090)

Administrative Uniformity

17.3 The particular mechanism that the Commission recommends for the Commonwealth public sector and private sector activities in the Territories may or may not be appropriate in other jurisdictions. It has been designed having regard to the existing structure of law and practice affecting Commonwealth administration. The standards which the Commission recommends for privacy protection in the context of information handling and intrusive conduct are based on principles identified at the highest international level and therefore appropriate for application in Australia beyond the Commonwealth's sphere. They do not, however, define appropriate administrative mechanisms for domestic application. The effects of intrusive behaviour on a person's privacy do not vary from jurisdiction to jurisdiction. The consequences of mishandling personal information are the same, in whatever jurisdiction it might occur. A person's civil rights should not vary significantly as he moves within Australia. The standards can, in their present form, be applied in any Australian jurisdiction, but, outside the Commonwealth and Territory area, the administrative setting might well be different. Because of its intended coordinating functions in respect of the States, this is an additional advantage of using the HRC as the administrative body to oversee privacy protection. (para. 1091)

18. General Response to Intrusions

18.1 The background law that presently applies to protect privacy threatened by intrusive conduct, together with the recommendations that a Privacy Commissioner within the HRC should have the function of conciliating and reporting on complaints of interferences with privacy in areas of Commonwealth responsibility, will provide an adequate and appropriate general response to the problems caused by intrusive conduct. It can be expected that the Privacy Commissioner's efforts at conciliation, and his power to make recommendations, both to the HRC and to the people whose

conduct is privacy invasive, will be effective in helping to alter intrusive practices in areas such as health, employment, journalism and commerce. (para. 1095-6)

19. Powers of Arrest, Search and Entry onto Property

General Principles

19.1 To assess these powers from the standpoint of personal privacy, and in developing new powers, the Commission recommends the following set of principles:

PRINCIPLES GOVERNING THE GRANTING OF POWERS OF INTRUSION

1. A power of intrusion (i.e., a power to arrest a person, to search a person or a place or to enter private premises) should not be granted as a matter of course. There should be a clear weighing up of the need to interfere with privacy against the social value of the policy to be achieved by conferring the power.

2. A power of intrusion should be conferred expressly, not by implication.

3. A power of intrusion should be conferred by an Act, not by subordinate legislation.

4. The grounds on which a power of intrusion may be exercised should be stated expressly and in objective terms.

5. Authority to exercise a power should normally be dependant on special judicial authorisation (a warrant). Exceptions may be made to this, where necessary, for 'barrier' powers (for example, customs) and cases of emergency.

PRINCIPLES GOVERNING THE EXERCISE OF POWERS OF INTRUSION

Powers of arrest

6. The purposes for which an arrest of a person may be made with respect to an offence are:
   (a) to ensure the appearance of the person before a court in respect of the offence;
   (b) to prevent a continuance or repetition of the offence;
   (c) to prevent the loss, concealment or destruction of evidence relating to the offence;
   (d) to preserve the safety or welfare of a person.

7. A person should not exercise a power of arrest unless he believes on reasonable grounds that:
   (a) the person he is arresting is committing, or has committed, an offence; and
   (b) proceedings by way of summons would not be likely to achieve one or more of the purposes for which an arrest may be made.

8. Where a person arrests another person, he should not use more force than is necessary.

9. A person arrested should be told the reason for his arrest as soon as practicable after his arrest.

10. An arrested person should be taken, as soon as practicable after his arrest, before a judicial officer to be dealt with according to law.

Powers of search of the person

11. A person should not exercise a power to search another person except with that latter person's consent or in accordance with law.

12. A person should not exercise a power to search another person except for the purpose of preventing the loss, concealment or destruction of evidence relating to an offence or, where the person to be searched has been arrested, for the purpose of removing any dangerous weapon that the arrested person may be carrying.

13. Where a person exercises a power to search another person, he should do so with respect for the dignity of the person searched.

14. Only a medical practitioner should be allowed to search a body cavity of another person.

Powers of entry and search of premises (including vehicles)

15. A person should not exercise a power to search premises (including vehicles and other property) except:

(a) with the consent of the owner or occupier of the premises or property;

(b) to prevent the loss, concealment or destruction of evidence relating to an offence; or

(c) in accordance with law.

16. Reasonable notice should be given of intention to exercise a power of entry, unless to do so would defeat the purpose of the exercise of the power.

17. A power of entry onto premises should only be exercised at a reasonable time.

18. A person should not use any more force than is necessary in effecting an entry onto premises under a power of entry.

19. Where a person has taken possession of any goods, papers or documents, he should permit, so far as is practicable, the person otherwise entitled to possession of them to use them.

Implementing the Principles

19.2 The HRC should undertake a review of all existing Commonwealth and Territorial legislation conferring intrusive powers to ensure that the principles identified above are appropriately embodied in the enabling legislation. Particular attention should be given, as an early priority, to:

- the powers granted to officers of the Department of Immigration and Ethnic Affairs, including:
  - the power to board and search any vessel in which the officer has reason to suspect that there may be found a stowaway or a person seeking to enter Australia in circumstances in which he would become a prohibited immigrant; and
  - the power to enter and search any building, premises, vehicle or place in which he has reasonable cause to believe there may be found specified persons or documents.

  None of these powers are subject to prior judicial warrant, although some can only be exercised by 'authorised officers' (i.e., with the so-called 'administrative' warrant).
- the very wide powers of officers of the Customs administration, including under 'general warrants', to enter and search premises and to seize goods, especially where these can be exercised apart from 'barrier' situations.
- the powers of intrusion conferred by the National Health Act 1953 and the Health Insurance Act 1973, only some of which are subject to prior judicial authorisation. (para. 1104)

The HRC should be consulted in respect of proposals to confer an intrusive power on an official, or to widen existing intrusive powers already conferred on officials or on the AFP before the proposal reaches Cabinet stage. (para. 1105) In addition to the HRC's role, the Privacy Commissioner will play a significant part in monitoring and regulating the exercise of intrusive powers by Commonwealth officials. He will share this role with the Commonwealth Ombudsman: each should be able to refer complaints to the other. The activities of the Privacy Commissioner and the Commonwealth Ombudsman should complement each other. The Privacy Commissioner should be required to have regard to the basic principles whenever a complaint that personal privacy has been interfered with is being considered. This will help him deal with complaints consistently, and in accordance with the international human rights instruments on privacy. The Commonwealth Ombudsman should also be required to have regard to them in dealing with complaints that privacy has been interfered with. Parliamentary approval should be given to these principles as the basis for the consideration of the privacy implications of administrative acts and practices within the Commonwealth and Territorial administrations. (para. 1106)

Official Powers: Particular Problems

19.3 *Body Cavity Searches*. The dangers and indignities associated with body cavity searches are sufficiently great to warrant special controls. A general authority conferred by a Commonwealth law to 'search the person of' another person should not be interpreted as authorising the official or police

officer to conduct a body cavity search. This should include, not only Commonwealth officers, but other persons who have authority under Commonwealth and Territory laws to search persons. A body cavity search should be conducted only by a medical practitioner, and then only under strict controls. Consistent with the Commission's views expressed in the *Criminal Investigation* report, judicial authority should be required to search a body cavity, which should be granted only if there is reasonable cause to suspect that evidence of the commission of an offence, or the likely commission of an offence, is secreted in that cavity. To ensure that inappropriate applications are not made, only a Commonwealth officer who would have a power to search the person concerned should be able to seek an authority to have a body cavity search conducted. (para. 1110) In view of the nature of a body cavity search, there should be a restriction on the offences for which such a search is to be available. It should not be available for trivial offences. A person should not be at risk of a body cavity search except in relation to an offence that carries a penalty of imprisonment for seven years or more. (para. 1111)

19.4 A Commonwealth officer, including a member of the AFP, who is authorised to search a person, should, if he considers that a search of a specified body cavity is necessary, specifically ask the person to be searched whether he consents to be so searched. Any consent should be properly evidenced. If there are other adequate and feasible means of determining whether there is something secreted in a body cavity, these should be used in preference to a body cavity search. The officer should not carry out the search. This should only be done by a medical practitioner. In the event that no consent is forthcoming, the officer should be able to approach a magistrate, as is contemplated by the Customs Amendment Act 1979, for a statement that sufficient grounds exist to warrant the search. Even if the magistrate does this, the search should not be carried out unless the suspect co-operates. If consent is not forthcoming, the officer should be able to approach the magistrate again, but this time for an order authorising the detention of the suspect for a specified period of time, not longer than 48 hours. If, at the end of the detention period, the suspect has not consented to the search, the Commonwealth officer should be required to have the authority of a Judge of the Federal Court or of a State Supreme Court before making arrangements for the search. In all cases, the person to be searched should be given the opportunity to obtain legal advice and representation, and to be heard by the magistrate or judge. Where it is not practicable for the Commonwealth officer to make an application in person, he should be able to make it by telephone. (para. 1112)

19.5 *Seizure of Records*. The principles that the Commission has formulated to deal with seizure of goods generally will apply in the case of mass seizure of records. They include principles analogous to those enacted in the Companies Act that require, for example, investigators who have seized records to allow reasonable access to them by the person from whom they were seized. In addition, the record-subject (in the medical fraud case, the doctor's patients) will, under the Commission's recommended access right, be able to approach the investigating agency and make a request to see the record. If the record is irrelevant to the purpose for which it was collected — the investigation of a particular offence — the patient may exercise his rights of amendment. The HRC should confer with the AFP and other Commonwealth and Territory agencies whose powers authorise them to seize records to develop appropriate guidelines for these cases. The powers themselves will also be reviewed by the HRC as part of the recommended overall review of intrusive powers. In individual cases, complaints about the exercise of these powers might be made to the Privacy Commissioner. This will have a continuing educative effect on the agencies that have and exercise these powers. Beyond these measures, no legislative action is needed. (para. 1116)

20. Non-Official Intrusions

Present Problems: Extent and Protections

20.1 The general remedies for intrusive conduct are an adequate legal response to most of the

problems of non-official intrusions. What is needed is a greater appreciation of the need to protect privacy from unwanted intrusions and of the protections that the law already affords the individual. The HRC has a specific public education role for human rights matters generally. The Privacy Commissioner's powers of conciliation, resolving particular complaints of intrusive non-official conduct, will also have an educative effect. (para. 1117)

Intrusions by Private Police and Private Agents

20.2 Some difficulties with licensing schemes are examined in the context of licensing personal record-systems. (s. 25.6) Licensing schemes are aimed at protecting the public from unscrupulous operators, or ensuring that only competent operators are permitted in the particular area of activity. It is not possible to justify licensing of private agents' and private police activities in the A.C.T. solely on the ground of protecting privacy. The costs of such a scheme could be greater than the specific benefit to privacy involved. But there may be a case for licensing private police operating in the A.C.T. for other reasons. Private police, by being uniformed and armed, intentionally project the same image of authority as official police. But they are not bound by the rules and disciplines that have been devised to prevent and redress abuse by official police. Consideration should be given by the Department of Territories and Local Government, in conjunction with the HRC, to the question whether private police in the A.C.T. should be licensed. (para. 1120)

20.3 Misleading conduct and conduct amounting to harassment, by agents in the A.C.T., including by debt collectors, process servers, persons executing legal process and investigation agents (for example, loss assessors and private inquiry agents), should be prohibited. This conduct should include:

- failing to disclose that the agent is acting as such;
- causing undue annoyance (without actually committing an assault or trespass);
- communicating with a debtor about a debt in a way that indicates to another person that the first person is a debtor;
- making unjustified threats;
- employing harassing tactics.

These practices are equally privacy invasive when carried on, not by an agent, but by a principal, for example, the creditor himself. The prohibition of these practices should therefore extend to principals. (para. 1121)

21. Interference with Communications

Listening Devices: Non-consensual Surveillance

21.1 The need for personal autonomy, the basis of the claim for privacy, implies the individual's ability to exclude others from his communications. It is inconsistent with personal privacy that listening devices be used to overhear or record conversations that are intended by their participants to be private. A statement of society's standards will benefit the law abiding, inhibit at least some potential breaches, and provide redress where surveillance is discovered. For these reasons, Commonwealth legislation should prohibit the use of listening devices for non-consensual or secret surveillance. (para. 1122-6)

Listening Devices: Participant Monitoring

21.2 Participant monitoring occurs in two circumstances. The most obvious is the case of a party to a private conversation using a listening device to record it without the consent of the other party. But it may also be that a party to a private conversation is using a listening device to transmit the conversation to someone who is not a party. (para. 1127) The Commission's tentative view on participant monitoring was that participant monitoring ought not to be permissible. On that view, only police would have been able to engage in participant monitoring, and then, only on judicial warrant.

Businessmen, journalists, public servants and others who may now lawfully monitor and record their own conversations — principally, to protect themselves from misrepresentation as to their position — would not. Nor would a person being interviewed by the police, who wished to make an accurate record of what was said, or an elderly person, or one with a defective memory, who wished to have an accurate record of instructions from, for example, their doctor. The Commission no longer holds this view. It now considers that to prohibit or otherwise regulate participant monitoring would be unnecessary and undesirable. To prohibit participant monitoring would lead to the result that a participant could take accurate and complete shorthand notes of a conversation and reproduce those notes with impunity, but would not be able to use a pocket recorder to perform exactly the same function. This similarity of function is an important reason for not prohibiting participant monitoring. The prohibition of non-consensual or secret surveillance by Commonwealth officials, and in the Territories, by means of listening devices should not extend to participant monitoring. The Commission is encouraged in this view by the fact that international standards and overseas laws generally permit participant monitoring, and the virtual acceptance of the practice by the State laws that regulate the use of listening devices. (para. 1133)

Telecommunications

21.3 *Secret Surveillance of Telecommunications.* The previous recommendation that non-consensual or secret surveillance be prohibited related to the use of listening devices to overhear or record private conversations not involving telecommunications. For the same reasons as the use of listening devices to overhear conversations should be an offence, their use to intercept telecommunications passing over a telecommunications system, without the knowledge of any of the parties to the communication, should continue to be an offence. (para. 1141)

21.4 *Extension of Scope of Telecommunications (Interception) Act.* The restriction of the Telecommunications (Interception) Act 1979 to communications that are passing over the telecommunications system might have been a defect or gap in the privacy protection provided by the Act if the Act were the only way in which communications intended for the telecommunications system were to be protected. But the Act must be seen in the context of existing laws prohibiting non-consensual or secret surveillance generally and the Commission's recommendation that similar laws should be enacted for the Territories. The Telecommunications (Interception) Act 1979 is concerned to ensure the security of the telecommunications system and of communications passing over it. It was not intended to regulate or protect communications that have not yet been or are no longer committed to the system. The privacy of communications outside the system is properly controlled by general listening devices law. While the Act might be amended so as to regulate the use of listening devices to overhear words spoken into or heard from a telephone, constitutional uncertainties may arise from the fact that s. 51(v) of the Constitution is expressed to relate only to 'services'. Further, there are serious practical difficulties with such an approach. For example, in particular fact situations, it would be difficult to determine whether the Telecommunications (Interception) Act applied or State and Territory listening devices law applied. For these reasons, the Telecommunications (Interception) Act 1979 should not be extended to cover the interception of communications before or after they pass over a telecommunications system. Communications outside the system are within the ambit of ordinary listening devices legislation, and are properly regulated in that context. (para. 1142)

21.5 *Participant Monitoring.* Under the Commission's proposals for a general listening devices law for the Territories, participant monitoring would not be prohibited. As there is no distinction in principle between the use of listening devices to monitor conversations generally, and their use to monitor or record telecommunications, participant monitoring of telecommunications should not be an offence. However, interference with a telecommunications system itself should continue to be an offence, whether the interference occurs in the course of participant monitoring or not. The technical integrity of the system must be maintained. It is adequately protected by Telecommunications

(General) By-law 19, which should not be altered. However, the Telecommunications (Interception) Act 1979 will need to be altered to remove the restrictions that presently exist on participant monitoring. (para. 1144)

21.6 *International Telecommunications.* Protection for the privacy of communications passing over the telecommunications system controlled by OTC is incomplete. It is as important that the law should, so far as is compatible with constitutional power and practical realities, provide protection against interception of private conversations or messages which pass beyond Australia, as it is to protect the privacy of messages within the territorial limits of Australia. The Commonwealth Parliament has legislative power to control the interception of such communications. The Telecommunications (Interception) Act 1979 should be amended so as to regulate interception of communications passing over the telecommunications system controlled by OTC. (para. 1145)

21.7 *Wireless Telegraphy Act.* The use of scanners should be closely considered by the HRC in conjunction with the Department of Communications, Telecom Australia and representatives of those groups the security of whose communications are at risk from these devices, with a view to bringing forward recommendations either to license the use or to regulate the import of scanners that can monitor radio-telephone frequencies and other frequencies that carry sensitive messages. (para. 1146)

Mail

21.8 The power (para. 1149) to open mail as to which there is a reasonable belief that it was posted or contains a thing in contravention of a Commonwealth Act extends to offences against the Customs Act 1901. But the Postal Services Regulations also authorise mail to be opened at the request of Customs officers. Mail entering the country is subject to the control of Customs as is any other import, and Customs officers are therefore entitled to require mail that is entering the country be opened without necessarily being of the opinion that contraband is actually present. (para. 1150) Protecting the privacy of the mail is fundamental to the protection of privacy. The setting of proper limits to the power to interfere with mail, and the provision of proper safeguards for the rights of individuals, should not be left to subordinate legislation. The Postal Services Regulations, Part VI, should be repealed. They should be replaced by provisions to be included in the Postal Services Act 1975. (para. 1151)

21.9 The procedural requirements that apply when mail is to be opened are adequate. There is, however, one area in which reform in the interests of privacy is warranted. The Postal Services Regulations, reg. 45, confers a wide power on Australia Post officials. It would, for example, authorise them to open and examine mail that consisted of advertising matter that was misleading or deceptive, or likely to mislead or deceive. On the other hand, it does not permit them to open mail that merely contains evidence of the commission of an offence (for example, a confession). While it might be necessary to empower Australia Post officials to open mail to ensure that the Postal Services legislation is complied with, there is no compelling reason to empower them to open mail for general law enforcement purposes. General law enforcement should be left to the AFP. In the interests of privacy, regulation 45 should be repealed. (para. 1152) Section 93 of the Postal Services Act 1975 should be amended to make it clear that it does not authorise Australia Post to permit opening the mail. (para. 1153)

21.10 There is no requirement that, before a Customs officer examines mail or individual postal articles, he have a reasonable suspicion that contraband or dutiable goods are present inside. Under the Postal Services Regulations, a similar situation applies. The power of a Customs officer to request the opening of postal articles consisting of, or containing, dutiable goods or prohibited imports or exports does not depend on his belief that reasonable grounds exist to justify opening. The Commission has not made specific recommendations about the form in which such 'barrier powers' should be cast. It has recommended that the HRC review these powers. This review should be conducted by testing the powers against the principles recommended by the Commisson for the grant

of new instrusive powers. The power of Customs to require the opening of mail for Customs purposes should also be reviewed in this examination. (para. 1154)

22. Law Enforcement Issues

Customs Act Regime a Desirable Standard

22.1 The Customs Act 1901 imposes a basic prohibition on the use of listening devices, but allows exceptions in the case of participant monitoring and surveillance in accordance with a warrant. The procedure for the grant of these warrants is also prescribed. The important aspects of the procedure are:

- the warrant is a judicial warrant;
- the judge must be satisfied, by information on oath that either:
  - there are reasonable grounds for suspecting that a particular person has committed, or is likely to commit, a narcotics offence and the use of a listening device will, or is likely to, assist in or in connection with inquiries into the commission of that offence; or
  - there are reasonable grounds for suspecting that premises have been, or are likely to be, used in connection with the commission of a narcotics offence, and the use of a listening device will, or is likely to, assist in or in connection with inquiries made in relation to the use of the premises in connection with the commission of a narcotics offence;
- the warrant is to be subject to such conditions as the Judge thinks fit;
- the time limit for the warrant cannot exceed six months;
- the warrant may be renewed;
- the Commissioner of Police must keep detailed records of all warrants;
- the Commissioner of Police must supply the Minister with copies of these records and with reports on the use of information gained and diclosures made;
- the Commissioner of Police, if satisfied that the grounds for the warrant no longer exist, shall revoke it;
- information gained from secret surveillance is not to be disclosed, except for the purposes of:
  - the narcotics inquiry concerned;
  - inquiries into another offence punishable by a jail sentence of more than 3 years duration;
  - security within the meaning of the Australian Security Intelligence Organization Act;
  - certain other offences and legal proceedings.

This legislative regime represents a generally fair balance between the claim of the individual to privacy and the need for effective and efficient policing. It should form the basis for the regime to be applied generally for all law enforcement use of listening devices, and mail interception, by Commonwealth officials. (para. 1156)

Who May Use Listening Devices for Law Enforcement Purposes?

22.2 Only AFP officers, who are subject to the traditional restraints on police, should be entitled to use listening devices for secret surveillance and then, only on a properly based suspicion that an offence against Commonwealth or Territory law (other than Northern Territory or Norfolk Island law) has occurred. The Commission does not agree with proposals that use of listening devices should be permitted merely as an intelligence gathering mechanism. To permit their use for such a purpose would clearly allow 'fishing expeditions', and would not provide proper recognition of the privacy of communications. It would also be inconsistent with Art. 17 of the ICCPR, insofar as it involves an arbitrary interference with communications and correspondence. (para. 1157)

Elements of the Regime

22.3 *Need for Judicial Warrant.* The authority for the use of listening devices by AFP should be judicial authority. This accords with the Commission's view, expressed in the *Criminal Investigation* report. Participant monitoring by members of the AFP should not require a warrant. (para. 1158)

22.4 *Gravity of Offence.* A warrant to use a listening device should only be available for the investigation of an offence that carries a penalty of seven years or more imprisonment. The implementation of this recommendation will make Division 1A of Part XII of the Customs Act 1901 unnecessary, and it should, in consequence, be repealed. (para. 1159)

22.5 *Telecommunications and the Mail.* So far as telecommunications are concerned, there are, at the present time, greater protections. In particular, the classes of offence for which interception for law enforcement purposes may be authorised is limited to narcotics offences. The same is true of police powers to open mail (as distinct from the power purportedly conferred by the Postal Services Regulations, reg. 45 on Australia Post officials to open mail for general law enforcement purposes). It would be anomalous if the classes of offence in respect of which a listening device to overhear private conversations may be used were different to the classes of offence in respect of which a listening device may be used to overhear communications passing over a telecommunications system or for which mail may be intercepted. The reason for extending the protection against secret surveillance in these areas to telecommunications and the mail is that what is protected is, essentially, the privacy of correspondence and communications, however they are transmitted. To avoid inconsistency, the recommendation that a warrant to use a listening device should only be available in respect of the investigation of an offence that carries a penalty of seven years or more imprisonment should extend to the use of listening devices in respect of telecommunications and to the opening of mail. (para. 1160)

22.6 *Written Application.* In the *Criminal Investigation* report, the Commission concluded that a written application for a warrant, whether authorising arrest or search, was desirable. A written statement, on oath, of the grounds for the application was also required. Under the Criminal Investigation Bill 1981, formal, written application would have been required for a search warrant or an arrest warrant. Similar requirements apply under the Crimes Act. A warrant to authorise the exercise of monitoring or interception powers should have at least the same requirements. A written application, supported by a statutory declaration as to the grounds on which the warrant is sought, should be required as part of the application for a warrant for the use of a listening device. (para. 1162)

22.7 *Use of Other Investigative Techniques?* The particularly intrusive nature of these techniques should be adverted to by the judge considering an application for a warrant. Their use should not be regarded as a routine investigative tool. They are particularly intrusive investigative techniques, that will, under the Commission's recommendations, be denied to private investigators, businesses and the general public. The appropriateness of, and the need for, the particular technique for which the warrant is sought should be matters for consideration every time a warrant is sought. In all cases, in addition to the other matters properly to be considered, the availability and suitability of other methods of obtaining the evidence should be taken into account when applications for the grant or renewal of warrants for secret surveillance are considered. (para. 1163)

22.8 *Seriousness of the Offence.* A judge should, when deciding whether to authorise the use of a listening device, be required to take into account the gravity of the particular offence being investigated and the extent to which the privacy of any individual is likely to be interfered with through the use of a listening device. (para. 1164)

22.9 *Time Limits.* A warrant authorising the use of secret surveillance devices to overhear conversations or intercept telecommunications, or the interception of mail, should remain in force for a maximum period of 30 days. A warrant should be renewable, if necessary, more than once. (para. 1165)

22.10 *Reports.* The Attorney-General has a special and overriding responsibility in respect of matters relating to the administration of law and justice at the Commonwealth level. He also has responsibility for human rights matters in general. Reports under the Telecommunications (Interception) Act and the

general listening devices legislation recommended in this report should be furnished to the Attorney-General. (para. 1166)

22.11 *Reporting to the Parliament.* The Attorney-General should report annually to Parliament on the number of surveillance warrants issued for law enforcement purposes. The report should also cover, in appropriately general terms, the use made by the AFP of listening devices and telecommunications and mail interception, under these warrants.

22.12 *Discretions to Exclude Evidence.* In any criminal proceedings, evidence otherwise admissible can be excluded on the basis that it was unlawfully or unfairly obtained. It is a matter of judicial discretion. One possible approach is a 'reverse onus' exclusionary rule. Under such a rule, unlawfully obtained evidence would *not* be admitted unless the court was satisfied the balance of competing requirements of public policy fell in favour of admitting the evidence. The competing requirements are:

- convicting the wrongdoer; and
- discouragement of unlawful conduct by law enforcers.

The public policy consideration involved here should be not merely the desirability of convicting offenders, but the desirability of conviction only after a fair trial. It is the fairness of the trial that is of critical importance to the administration of criminal justice. A fair trial, from both the accused's and the prosecution's point of view, requires that a decision be made in the light of as much relevant factual material as can be properly put before the court. Against the need to discourage contraventions of laws controlling police investigation should be weighed the desirability of having as much relevant evidence as possible before the court. That is how the rule should be formulated. Accordingly, the reverse onus exclusionary rule should be expressed as follows:

> Where, in proceedings in a court in respect of an offence, it is proved on the balance of probabilities that evidence was obtained in contravention of, or in consequence of a contravention of, the relevant laws, the court shall not admit the evidence unless it is satisfied that, in the circumstances of the case, the desirability of having evidence relating to the offence before the court substantially outweighs the undesirability of admitting evidence that has been obtained in the manner in which the evidence was obtained. (para. 1170)

22.13 *Telephone Warrants.* It is possible that there would be fewer telephone applications for warrants to intercept telecommunications, or to use listening devices for secret surveillance, than there would be for the issue of search warrants. But the ability to obtain these warrants by telephone should exist, for the same reasons as apply to search warrants. (para. 1171)

22.14 *Disclosure of Information.* Information which is not relevant to the investigation at hand may fall into one of three categories:

- it may disclose evidence of the commission, or likely commission, of another Commonwealth offence;
- it may disclose evidence of the commission or likely commission of an offence against the law of a State or a Territory;
- it may be totally irrelevant to any offence.

Information in the last category should be protected from disclosure to any person. If the information relates to the commission of an offence for which a warrant to use a listening device for secret surveillance of private conversations or to intercept telecommunications could have been obtained, there should be no prohibition on disclosing it for the purposes of the investigation of that offence. (para. 1172) However, more difficult issues arise if the information falls into either of the first two categories, and relates to an offence for the investigation of which a warrant could not have been obtained (i.e., an offence punishable by less than seven years imprisonment or a State offence). Where information obtained in pursuance of such a warrant relates to an offence other than the offence specified in the warrant, it should not be disclosed for the purposes of investigating that offence unless the offence carries a penalty of seven years or more imprisonment. Where the offence is an offence

against a State or Territory law, the same provisions should apply. This would preclude the disclosure of information for intelligence purposes only. (para. 1173)

23. Unsolicited Communications

Options For Reform: Mail

23.1 Direct mail organisations are usually willing, if asked, to remove an objector's name from mailing lists. This is re-inforced by the code of practice that the Australian Direct Marketing Association (ADMA) has published for its members. But certain problems remain. Not all direct marketers are members of ADMA. Even for members, the sanctions available may not be very effective to ensure that names are in fact removed. Even direct mail organisations that are willing to remove names may be inefficient in doing so. Further, lists circulate widely to various organisations, and the objector may have to approach many different organizations to ensure that he receives no more unsolicited mail. (para. 1175) Possible broad approaches include:

- *Master List.* A list could be maintained by a suitable central body, such as ADMA or Australia Post. An obligation would be imposed on direct marketers to check with that list before sending material out through the post, and it would be a criminal offence to send, through the post, unsolicited advertising material to a person whose name appeared on the list. (para. 1176) This would be impractical and costly and should not be adopted. (para. 1176)
- *Information as to Source Included.* A second alternative is to ensure that direct mail organisations inform recipients of the source of the unsolicited communication, so that they can notify the organisation of their desire to have their names removed. It would also be possible to have the organisation include the source from which the names and addresses were obtained. Again, this would be impractical and costly and should not be adopted. (para. 1177)
- *Statement of a Right.* Under the third alternative, direct mailing material would have to include a statement of the legislative right to obtain, on request, information concerning the source of the name and address. But notification of a right to information concerning the source of one's name and address used by direct mail organisations can never provide a guarantee that the name and address of a person who wishes it will be removed from a mailing list. This alternative should not be legislatively required. (para. 1178)

Recommendation

23.2 The Commission proposes a right of access to personal information. (para. 1179) List brokers and organisations that make lists available for direct marketing purposes will be 'record-keepers' for the purposes of the Commission's recommendation about a general access right. Any person who is concerned that a record-keeper (such as a retailer or a list broker) is maintaining a record about him for the purposes of direct marketing, even if only a record of his name and address on a list, will enjoy a new right of access to the record. He will be able to see whether his name is included on lists compiled and rented out by a list broking organisation. There would be, in fact, no need for further legislation to implement this alternative. It is already implicit in the general right of access to personal information recommended by the Commission. (para. 1179)

Telephone Calls

23.3 For many people, direct marketing and telephone canvassing are not privacy problems. Under the Commission's general recommendations, the HRC will engage in discussions with direct marketing organisations operating in the Territories to develop appropriate, publicly acceptable and balanced guidelines. However, the HRC's powers in relation to these kinds of activities, so far as privacy is concerned, should not be limited merely to the Territories. It should extend Australia-wide, since the mail and telecommunications are clearly within Commonwealth legislative power. The direct mail industry has expressed considerable enthusiasm for the notification requirement of the

third alternative discussed earlier. Notification might therefore usefully be included as part of the guidelines. In the area of telephone marketing, a relatively new development in Australia, the majority of telephone 'canvassers' are aware of the problems and of the need to deal with them, and are prepared to do so as those problems arise, in consultation with the relevant branches of government. This is an area where guidelines, developed by the HRC in conjunction with industry representatives and consumer groups, and monitored by the Privacy Commissioner through his complaints and conciliation function, would work adequately. They will be overseen by the HRC, which will report regularly to the Parliament on their effectiveness. In the long term, the aim should be to provide a uniform industry approach to the privacy problems involved. (para. 1182)

24. Optical Surveillance

Principles

24.1 *Technological Prying Objectionable.* Law enforcement authorities generally take the view that the use of optical devices ought not be subject to legislative control. But if unlimited use of such devices were to be permitted, the right of people to seclusion, free from prying inspection, could be seriously diminished. (para. 1185)

24.2 *Reasonable Expectation.* It is not desirable to regulate the use of surveillance or recording by means of optical devices in streets, parks and other such entirely public places. A person who is in a public place cannot complain if he is seen or photographed. But when he moves outside the public place, the situation changes. Outside a public place, there is a range of possible situations to be considered, including activities taking place in banks, hospitals and large private buildings, for example, a department store or an office or factory in which there may be surveillance by optical devices. The surveillance may be overt — the cameras easily seen — or covert, with the cameras carefully concealed. Again, he may be in a private home. Even here, different situations can occur:

- He may be inside, with the curtains drawn.
- He may be in his backyard, which can easily be overlooked by those in the next door flat. On the other hand, his backyard may be well screened.
- He may be in his front yard, visible from the street.

Where a person may reasonably expect that his activities will be private, that expectation should be respected. (para. 1186)

Recommendations

24.3 *Public Places.* Complaints of prying and intrusive optical surveillance in the Territories or by Commonwealth or Territory officers will, under the Commission's proposals, be able to be made to the Privacy Commissioner. Valuable though the conciliation and complaints procedure will be, it is not adequate, by itself, to ensure that privacy is protected from other optical surveillance, including unwelcome and unwarranted optical surveillance outside public places. So far as public places are concerned, the current situation should continue, i.e., there should be no regulation of optical surveillance. For the purposes of legislation, a 'public place' should be defined in the same terms as it is defined in police offences, summary offences and like legislation. (para. 1187)

24.4 *Outside Public Places.* Outside public places, the use of optical surveillance devices to observe people who could otherwise reasonably expect to be safe from observation should be prohibited. This prohibition should apply to all Commonwealth officers. It should also apply in relation to the Territories, by prohibiting optical surveillance by Territory residents, or of Territory residents. But this prohibition should not be drawn in such a way as to protect wrongdoers who take steps to ensure that they are out of sight. Accordingly, where the surveillance device is used by a person for the purpose of observing what he had reasonable grounds to believe was the commission of an offence, the use of the device should be excused. Further, if the person using the device had reasonable grounds to believe that the use of the device was known to those whose activities were being recorded

or observed, the use of the device should be excused. Finally, there should be the overriding requirement that the particular use of the surveillance device was, in all the circumstances, reasonable. This should apply even if those observed or recorded knew about the surveillance device. The onus of proving these matters should be cast on the person using the surveillance device in order to discourage their indiscriminate use. (para. 1188)

Definition: Surveillance Devices

24.5 For the purpose of implementing these recommendations, analogies can be drawn with present listening devices legislation. Thus, the sorts of devices whose use should be proscribed should be defined in a manner similar to the definitions of 'listening device' in that legislation. A typical definition of 'listening device' is 'any instrument, apparatus, equipment or device capable of being used to hear, record or listen to a private conversation simultaneously with its taking place'. Similarly, the definition of surveillance device should be based on the capability of the device to observe or record the activities of a person. It should not include torches or other devices that simply provide illumination. It should not include spectacles and other devices used by a person whose sight is impaired to enable him to overcome the impairment. (para. 1189)

Definition: Private Activities

24.6 Again, for the purpose of defining the activities that should be safe from surveillance, analogies with listening devices legislation can be drawn. That legislation prohibits the use of listening devices to hear or record conversations taking place in such circumstances as may reasonably indicate that the participants expect the conversation to be private. It will be sufficient to prohibit optical surveillance of a person who is in circumstances that indicate that he would reasonably expect not to be seen by the person who is using the surveillance device. This is an objective test, focussing on a reasonable assessment of the circumstances in which the activity concerned occurs. (para. 1190)

Law Enforcement

24.7 It is necessary to consider the extent to which exceptions to the general rule prohibiting optical surveillance of private activities should be permitted. Consistent with the Commission's recommendations on aural surveillance, optical surveillance should be permitted if carried out by the AFP under the authority of a judicial warrant. The regime adopted in relation to the use of listening devices should be adapted to cover the use of optical devices. (para. 1191)

Other Protections

24.8 In dealing with complaints about optical surveillance, as with complaints about interception of communications, the Privacy Commissioner should have regard to the approach taken by the Commission in this report. The persuasive effect of the Privacy Commissioner's activities in conciliating and arbitrating disputes will be a significant protection for this aspect of privacy. As well as the Privacy Commissioner's conciliation role, the HRC will itself have, under the Commission's proposals, a 'public education' function. This will be a particularly significant long term protection for privacy. The HRC would, through liaison with the police and industry groups whose members might use optical surveillance in their day to day activities, try to inculcate an appreciation of the importance of ensuring that optical surveillance is only used legitimately. (para. 1192)

25. Privacy and Personal Information

Basic Principles of Information Privacy

25.1 The Commission, drawing primarily on the OECD guidelines, has formulated the following general principles for privacy protection in the information-processing context:

INFORMATION PRIVACY PRINCIPLES

Collection of Personal Information

1. Personal information should not be collected by unlawful or unfair means, nor should it be collected unnecessarily.

2. A person who collects personal information should take reasonable steps to ensure that, before he collects it or, if that is not practicable, as soon as practicable after he collects it, the person to whom the information relates (the 'record-subject') is told:

(a) the purpose for which the information is being collected (the 'purpose of collection'), unless that purpose is obvious;

(b) if the collection of the information is authorised or required by or under law — that the collection of the information is so authorised or required; and

(c) in general terms, of his usual practices with respect to disclosure of personal information of the kind collected.

3. A person should not collect personal information that is inaccurate or, having regard to the purpose of collection, is irrelevant, out-of-date, incomplete or excessively personal.

Storage of Personal Information

4. A person should take such steps as are, in the circumstances, reasonable to ensure that personal information in his possession or under his control is securely stored and is not misused.

Access to Records of Personal Information

5. Where a person has in his possession or under his control records of personal information, the record-subject should be entitled to have access to those records.

Correction of Personal Information

6. A person who has in his possession or under his control records of personal information about another person should correct it so far as it is inaccurate or, having regard to the purpose of collection or to a purpose that is incidental to or connected with that purpose, misleading, out-of-date, incomplete or irrelevant.

Use of Personal Information

7. Personal information should not be used except for a purpose to which it is relevant.

8. Personal information should not be used for a purpose that is not the purpose of collection or a purpose incidental to or connected with that purpose unless:

(a) the record-subject has consented to the use;

(b) the person using the information believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to the life or health of the record-subject or of some other person; or

(c) the use is required by or under law.

9. A person who uses personal information should take reasonable steps to ensure that, having regard to the purpose for which the information is being used, the information is accurate, complete and up to date.

Disclosure of Personal Information

10. A person should not disclose personal information about some other person to a third person unless:

(a) the record-subject has consented to the disclosure;

(b) the person disclosing the information 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 record-subject or of some other person; or

(c) the disclosure is required by or under law. (para. 1195)

Implementing the Principles

25.2 *Personal Information.* To limit the definition of 'personal information' to information relating to the 'personal affairs' of a person is too restrictive. Any information about a natural person should be regarded as being personal information. But the link between the person and the information need not be explicit. Information should be regarded as being 'personal information' if it is information about a natural person from which, or by use of which, the person can be identified. Finally, the general recommendations should not be restricted to personal information kept in a systematic fashion: in a record-system. (para. 1198).

25.3 *Record-keeper.* Where personal information is collected or held by a body corporate, the body corporate should be regarded as the record-keeper, with the primary responsibility for observing the proposed information privacy principles. This will not relieve individuals, such as computer programmers and data managers, employed within a corporate structure from responsibilities that may be imposed on them through codes of practice or statements of ethics devised or adopted by their particular professional organisations. The recommended legislative statement of information privacy principles will help those personnel in resolving such dilemmas. (para. 1199)

25.4 *Adoption by the Parliament.* Of necessity, the principles are widely expressed and in general terms. They are not intended to be statements of inflexible law. The principles should be endorsed by the Parliament and expressed in legislation as a guide to proper information-handling practices. This would provide 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. (para. 1200)

25.5 *Legislation or Guidelines?* The NSWPC has relied heavily on 'voluntary guidelines'. These guidelines have generally been based upon principles similar to those recommended in this report. They are purely informal 'agreements' with only some of the participants in a limited number of areas of activity. Their impact has therefore been circumscribed. The principles for information privacy stated by the Commission have been distilled from the various international instruments and laws on information privacy. Without such a basis in principle, there is the clear risk that inconsistent policies will be developed. A legislative statement of the principles for privacy protection is clearly desirable. Wherever practicable, mechanisms to give legal force to the principles should be provided. The appropriate mechanism for each of the principles should be considered separately. (para. 1201)

25.6 *Licensing.* Under a licensing scheme, record-systems that contain records of personal information would have to be licensed by a central authority. Alternatively, the requirement for licensing could be restricted to particular sorts of record-systems, for example, those that have been computerised. The sanction for operating without a licence would be a criminal one. The licensing authority would have the power to revoke a license, and to impose conditions on the grant of a licence. (para. 1202) A number of European laws require licensing (or what amounts to licensing) for some record-systems, (para. 1203) The following arguments may be advanced in favour of licensing record-systems:

- *Control of Standards.* Licensing provides a simple framework for privacy policies to be implemented.
- *Benefits to Licences.*
- *Controlled Development.* A licensing system would allow the future development of record-systems to be controlled. (para. 1204)

But there are strong arguments against licensing record-systems, including cost and ineffectiveness. Licensing schemes confer exclusive economic advantages and tend to be anti-competitive, by inhibiting new entrants into the areas of activity licensed, and tending to discourage new developments. (para. 1205) The Commission's Reference is limited to the Commonwealth public sector and the Territories. To introduce an administrative structure to grant licences to record-keepers,

effectively only in the A.C.T., could not be justified on economic grounds alone. Further, the difficulty of deciding which record-keepers should have to be licensed is a significant one. The Commission is not persuaded by the fact that a significant number of European laws have adopted systems of licensing to implement information privacy principles. (para. 1206) There is no evidence to suggest that privacy problems have reached such a stage as to warrant licensing. Finally, the primary object of the Commission's recommendations on information privacy is not to punish those who breach the privacy principles. It is to encourage record-keepers themselves to adopt proper and responsible practices, giving due weight to privacy interests. There are better ways of doing this than to require that all or some record-systems be licensed. (para. 1206)

25.7 *Publicity*. So far as the Commonwealth public sector is concerned, efforts should be made to publicise the existence and nature of record-systems containing personal records. To some extent, the publication requirements of the Freedom of Information Act 1982 will help to publicise the existence and operation of public sector record-systems that include personal information. The HRC, as part of its general research and public education functions, should collate this information so that it can be published together for ease of reference. The HRC should encourage major private sector record-keepers (such as credit bureaus, insurance companies, large employers and the like) whose personal record-systems affect residents of the Territories to include similar details in the compendium. (para. 1208)

Collection Principles and Storage Standards

25.8 *Licensing*. Licensing is an inappropriate way to ensure that the information privacy principles are observed. Other legal means available to ensure compliance are either the creation of a civil right to claim damages for breach of the principles or the imposition of criminal liability for such a breach. Neither is appropriate for principles formulated in the way in which Principles 1 to 4 (see s. 25.1) are drawn. Criminal liability, for example, should only be imposed in respect of clearly and precisely defined activities. But the principles do not specify with sufficient clarity the acts they prohibit. This is not their purpose. In addition, the nature of a breach of the principles is generally such that criminal penalties are inappropriate. Failure to inform the record-subject that the collection of some personal information was authorised by law, for example, while undesirable, should not give rise to criminal liability in the collector. Likewise, the fact that a person can never be sure that information being collected is accurate until after he has collected enough information to verify it, and the fact that he can never be sure that he has collected all the personal information relevant to his purpose, make criminal sanctions for these contraventions of the principles inappropriate. Nor should they, without more, be a special ground of civil liability. Extreme departures from the standards set by the principles will, in most cases, be contrary to existing laws or legal standards, such as laws against unjustified discrimination or deception in marketing products. (para. 1225)

25.9 *Difficulties with Further Legislation*. Further, there would be difficulties with a coercive scheme that required information collection principles to be followed under threat of civil or criminal penalties. The freedom to collect information about others is an integral part of the right to freedom of expression. Enforcing limits, beyond those that already exist, on the information that can be collected would constitute an interference with this right that could have undesirable ramifications. Additionally, if the collection principles were to be legally enforceable, it would be necessary for all collectors to define precisely their purposes in advance. (para. 1226)

25.10 *Role of Human Rights Commission and of Privacy Commissioner*. The legislative statement of principles proposed in relation to collection and storage of personal information, and the complaints, conciliation and public education functions of the Privacy Commissioner and the HRC, are sufficient to ensure that the principles will be properly implemented in the Commonwealth and Territory administrations and in the private sector in the Territories. (para. 1228)

25.11 In relation to record storage and security practices, the role of the HRC in formulating detailed

principles — taking into account all the difficulties which have been outlined earlier — will be most important. The HRC, in conjunction with industry groups, existing government agencies such as the Commonwealth Ombudsman and the Auditor-General, and other experts, will be able to give advice as occasion warrants. (para. 1229) It may also propose formal guidelines of a more detailed kind. Most record-keepers will be receptive to approaches from the HRC (and the Privacy Commissioner), because, amongst other things, improvement in security and storage standards in records-systems will, in most circumstances, be in their interest. (para. 1229)

Access to Personal Information

25.12 *Enforceable Right of Access to Personal Records.* The internationally accepted principles for information handling practices include a statement of the right to access. (para. 1235) Unlike the collection and storage principles, the access principle can be stated with sufficient precision to be enforceable. It is already implemented in the Commonwealth administration, through the Freedom of Information Act 1982, and has also been implemented at the State level. To that extent, it is already a legally enforceable right. There should be a right, enforceable under Commonwealth law, for an individual to have access to records of personal information held about him by record-keepers. (para. 1236) The records to which the right of access should apply are records of personal information as defined. (see s. 25.2)

25.13 *Extent of the Right.* The Commission's Reference extends to the Commonwealth public sector, as does the Freedom of Information Act 1982, although certain Commonwealth instrumentalities are excluded from the operation of that Act. The right to obtain access to personal records under a privacy law, however, should not be subject to this limitation. It should apply to all Commonwealth instrumentalities, whether or not they are bound by the Freedom of Information Act 1982. The access right should apply to records held by any Commonwealth Department or statutory authority, including trading authorities. It should be available to anyone in Australia. (para. 1238)

25.14 In the interests of privacy, the record-subject should be able to secure access in relation to records of his personal life and history kept in both public and private sectors. There can be no valid basis for differentiating between public sector and private sector record-keepers. The risks which their activities, particularly if computerised, pose to privacy are identical. Nor is there any valid basis for distinguishing between them in terms of the remedies available for refusal of access. (para. 1239)

25.15 Just as there can be no valid basis for differentiating between public sector and private sector record-keepers, there can be no basis for limiting the right of access to personal records created after the implementation of the Commission's recommendations. The risks for privacy involved in misuse of a record of personal information, collected or recorded before a particular date, are no different to the risks involved in misuse of records of personal information collected after that date. (para. 1241)

25.16 *Intermediary Access.* There are cases where the record-subject may not be able properly to appreciate the significance or the full purport of the contents of the record. It may also be that access to some records, for example, health records, would be injurious to the record-subject. Intermediary access, i.e., giving access not directly to the person concerned but to another, who might explain and interpret it to him, is a useful device to overcome these difficulties. Because the right of access is primarily the right of the record-subject, the record-keeper should only be able to require intermediary access where there are reasonable grounds to believe that the record-subject will be harmed by seeing the record. Where the record-keeper believes that the record-subject will have difficulty, unaided, in understanding the record, he might suggest intermediary access. But the record-subject should be able, if he wishes, to insist on direct access to the record. The record-keeper should not be able to insist upon intermediary access. The choice of intermediary should be agreed between the record-keeper and the record-subject. Failing agreement, the Privacy Commissioner would be able to conciliate and resolve the dispute. (para. 1242)

25.17 *Records about Incompetent Persons.* The granting of a right of access to records of personal

information includes the granting of a right to access to personal information concerning those who are, for legal purposes, 'incompetent'. (para. 1243) The general reasons for conferring a right of access to records of personal information apply with equal force where the record-subject is an incompetent person. Mentally retarded persons, for example, are entitled to exercise, so far as is feasible, the same rights as others in the community. Access to a record of personal information concerning a child should not be denied the child simply because he is a child. If the record-keeper is concerned that the record-subject will not be able adequately to comprehend the record (by reason of immaturity or intellectual incapacity), the facility of intermediary access (s. 25.16), is the appropriate means of ensuring that the object of the right of access is not lost. (para. 1244)

25.18 A basic reason for access by the record-subject to records of personal information kept about him is to ensure that, when decisions are made on the basis of that information, it is as accurate and complete as possible. The more significant the decision, the greater the effect it would have on the life of the person concerned, the more important it is that this right of access be available. (para. 1247)

25.19 There is a need to make special provision for children because of their immaturity, and for mentally retarded persons in appropriate cases, because of their vulnerability. These needs are recognised by the Declaration on the Rights of the Child and the Declaration of the Rights of the Mentally Retarded. A legal right of access to personal records concerning the child or incompetent person, conferred on his guardian, is a special provision of this kind. In the case of children, the legal guardian will most commonly be the parent who has the custody of the child. In other cases, *viz.*, where the record-subject is an adult but of unsound mind, his legal guardian, appointed under the relevant State or Territory law, should be able to exercise the right of access. The legal guardian of a person should have a right of access to records of personal information concerning the person on the same basis as if he were seeking access to records about himself. Subject to exceptions (s. 25.20), the same exemptions and procedural requirements should apply. This right of the guardian should be in addition to the right of the record-subject himself. (para. 1248)

25.20 There must come a time when a child should be treated as an adult, even if some of those who are labelled 'adults' are still immature, and some of those who have not attained the specified age display adult attitudes and behaviour. But an age must be selected beyond which the parent will no longer be entitled to access to records of personal information about their children. (para. 1249) The age of 18, the usual age of majority, should be the age at which the access right of the parents, like other rights in respect of their children, ceases. (para. 1249)

25.21 *Exemptions to Accommodate Competing Interests.* Privacy is not an absolute right. The right of access to records of personal information should therefore not be absolute. (para. 1250) The regime governing access to records of personal information should be the same, so far as is possible, as the Freedom of Information Act 1982. It would be undesirable to have two different regimes for access to records held by Commonwealth agencies. In most cases, records of personal information are not held apart from other working files by Commonwealth agencies, and the same personnel will administer them. Unnecessary differences between privacy and freedom of information legislation would be confusing and therefore undesirable. (para. 1253)

25.22 *Categories of Exemption in the Private Sector.* The decision as to which classes of information should be the subject of an exemption under the Freedom of Information Act was taken on the basis of the character of the information contained in the record, not the identity of the record-keeper. It is appropriate that they also apply in relation to access to personal records in the private sector. A record-keeper forced to disclose information may run the risk of breaching a confidence or interfering with criminal investigations whether he is in the public sector or the private sector. The interests to be taken into account are essentially the same. Some categories of exemption are less likely to be relevant to records kept in the private sector than those kept by government agencies. However, in view of the growing inter-relationship between the public sector and private enterprise, and the increasing flows of information between the sectors, government information within an exempt class is increasingly likely to flow into the private sector and back again. (para. 1254)

25.23 *Nature of Exemptions*. There are two qualifications to the proposition that the Freedom of Information Act exemptions should also be applied under the privacy regime. First, the general interest of the individual, as a citizen or resident of Australia, in having access to government documents is not the same as the interest of the individual in having access to records of personal information about himself. Secondly, as the privacy regime will extend to private sector record-keepers, the qualifications in some of the tests in the Freedom of Information Act 1982 may need slight adaptation to ensure that they are expressed in a way that adequately reflects competing interests involved. In particular, some of those tests in the Freedom of Information Act 1982 that balance the right of the general public to have access to government documents against 'the public interest' in non-disclosure should be altered. In some cases, even for private sector record-keepers, the 'public interest' test is appropriate. For example, in the case of the exemption on the ground of 'defence and national security', it is appropriate to balance the individual's interest in having access with the public interest in ensuring that defence and national security are not prejudiced. But the exemption in the Freedom of Information Act 1982 on the ground that the document concerned is an 'internal working document', disclosure of which would be contrary to the public interest, is not appropriate for a record-keeper in the private sector. (para. 1255)

25.24 *Defence and National Security*. This Commission is not able to make specific recommendations in relation to access to personal information which has a bearing on defence or national security. The relationship between access to information and national security and defence has been addressed by the Parliament in the Freedom of Information Act 1982. The Commission has assumed that, when privacy legislation is enacted by the Parliament, a similar approach will be taken. The draft legislation attached to this report reflects this assumption. (para. 1256)

25.25 *Inter-Governmental and Diplomatic Relations*. Records that contain information about diplomatic and Commonwealth–State relations should be exempt from the right to access in the same way as they are exempt under the Freedom of Information Act 1982. (para. 1257)

25.26 *Companies and Securities Records*. Records of personal information that fall into this category should be exempt from access by the record-subject. (para. 1258)

25.27 *Executive Council and Cabinet Documents*. Records of personal information that relate to the deliberations of the Federal Executive Council or the Cabinet should be exempt from access by the record-subject to the same extent that they are exempt from access under the Freedom of Information Act. (para. 1259)

25.28 *Internal Working Documents*. Some records, including records of personal information, would, if disclosed outside the organization concerned, hamper its ability to ensure that its operations are carried out efficiently and that, where confidentiality is necessary for effective performance of its functions, that confidentiality is respected. This is not a need peculiar to government administration. It is a need recognised by all organizations where complete openness would impede the effectiveness and efficiency of its operations. To cover adequately both the public sector record-keeper and the private sector record-keeper, the test should be framed in terms of whether giving access to the record-subject would, in the circumstances, unreasonably disclose information of the kind specified in the exemption in the Freedom of Information Act 1982. A test so formulated includes within it the public interest considerations that are peculiar to government administration, but in a way that is appropriate in the context of a right of access by the record-subject to records of personal information about himself. To give further guidance to record-keepers and others who will have to apply the test, legislation should indicate some of the matters that should normally be taken into account in determining whether the disclosure of the information would be unreasonable. These matters would include the use that is likely to be made of the information by the person seeking access. (para. 1260)

25.29 *Law Enforcement*. Protection of privacy interests involves resolving the tension between personal interests and the competing legitimate interests of others in the society and the society itself. One such competing interest is the need to prevent sensitive police and other law enforcement

information from falling into the hands of those against whom it might be used. The Freedom of Information Act exemption relating the law enforcement information should apply in relation to the right of the individual to gain access to records relating to himself. (para. 1261)

25.30 *Legal Professional Privilege.* The privilege from production on the grounds of legal professional privilege, arising in proceedings between the record-keeper and the record-subject, should not be disturbed. But access to personal records about a person should not be denied to that person merely on the ground that, in proceedings between the record-keeper and some third person, the information contained in the record would be privileged. The exemption should be formulated bearing in mind that legal professional privilege is a corollary of the system of adversary litigation. The record-keeper's right to refuse access to personal records on the grounds of legal professional privilege should be limited. It should only arise if the person seeking access is himself in litigation, or it could reasonably be expected that giving the access would result in a party to litigation (whether actual or contemplated) being provided with the contents of a document which he would not be able to obtain in discovery and inspection in the litigation. (para. 1263)

25.31 *Financial, Property and Other Interests.* The Freedom of Information Act 1982 exempts from the requirement of access under the Act documents that contain information the disclosure of which would have a substantial adverse affect on financial and property interests; or that contain information relating to audit and other testing procedures. These exemptions should be available to record-keepers in respect of access by the record-subject. However, the test in the Freedom of Information Act 1982 is that the giving of access to all the world must be contrary to the public interest. This is not an appropriate formulation in the context of private sector record-keepers. They have analogous, although not precisely equivalent, legitimate interests that should be protected. As with the 'internal working documents' exemption, the test should be formulated in terms of disclosure of information of the kind identified in s. 39 and 40 of the Freedom of Information Act 1982 that is, in the circumstances, unreasonable. (para. 1264)

25.32 *National Economy.* The Freedom of Information Act 1982 exempts from the requirement of access under the Act documents that bear on sensitive economic policy, the disclosure of which would substantially affect the Commonwealth Government's ability to manage the Australian economy. The exemption should apply in the proposed privacy regime in the same way as it applies in the Freedom of Information Act 1982. (para. 1265)

25.33 *Contempt of Parliament and Courts.* An exemption similar to the exemption in the Freedom of Information Act 1982 for documents the disclosure of which would be in contempt of Parliament or of a court should be available to record-keepers under the proposed privacy regime. (para. 1266)

25.34 *Privacy of Others.* The privacy exemption in the Freedom of Information Act 1982 should also be available to record-keepers under the privacy regime. But, under the privacy regime, there should be a 'reverse-FOI' procedure similar to the procedure provided by the Freedom of Information Act 1982 for trade secrets, requiring a record-keeper to inform a record-subject that access to a record of personal information about him is being sought, and permitting the record-subject to object to the provision of access. This would assist the agency or officer dealing with the request for access to determine whether granting access to a particular person would be unreasonable. The result of a request under either should be the same. Personal information about a person should not be at greater risk under the Freedom of Information Act. The Freedom of Information Act 1982 should be amended to provide for 'reverse-FOI' where access is sought to records of personal information. (para. 1269)

25.35 *Breaches of Confidence.* At present, the exemption under the Freedom of Information Act 1982 is cast in absolute terms. Provided the disclosure of the document under the Act would constitute a breach of a legal duty of confidence, the document is exempt. To protect privacy interests to an appropriate extent, it is necessary that the exemption in the Privacy Act be a qualified one. But, as with the 'internal working documents' exemption, 'public interest' is not the appropriate qualification in the private sector. The exemption should be drawn on the basis that the giving of access to the

record sought would, in the circumstances, constitute an unreasonable disclosure of personal information the disclosure of which to the person seeking access would otherwise constitute a breach of a legal duty of confidence. As with the 'internal working documents' exemption, legislation should indicate some of the matters that are to be taken into account in determining whether access, in the particular case, would be unreasonable. (para. 1272)

25.36 *Business Affairs.* The Freedom of Information Act 1982 exempts from the requirement of access documents recording trade secrets, information having a commercial value and information about the business, commercial or financial affairs of a person or an organisation if its disclosure could reasonably be expected to unreasonably affect that person or that organization in respect of those affairs. The Freedom of Information Act exemption should be reflected in the privacy regime to preserve the commercial value of that information. As in the Freedom of Information Act 1982, the record-keeper should be required to follow the 'reverse-FOI' procedure. (para. 1273)

25.37 *Secrecy.* The Freedom of Information Act 1982 exempts from mandatory access documents to which 'secrecy provisions' in other Commonwealth laws apply, whether the secrecy provision is absolute or is subject to exceptions or qualifications. Were a provision similar to the Freedom of Information Act, s. 38, to be part of the privacy regime, personal records, to which the record-subject might justifiably seek access, could be withheld from him simply on the ground that the law prohibited their general disclosure. Secrecy provisions are an appropriate way of preventing disclosure of information where the individual is seeking access to general government information simply as a citizen. But when he is seeking access to the records that a record-keeper holds about him, the reasons for the secrecy provision, directed to the world at large, are no longer relevant. If access is to be denied, it should be on some ground other than the fact that it is not appropriate that this information be made generally available. No provision comparable to s. 38 of the Freedom of Information Act 1982 should be included as part of the privacy regime. (para. 1274)

25.38 *Welfare of the Incompetent Person.* One of the reasons that guardians should have a right of access to personal records about those in their care is that their maturity will help ensure the accuracy, timeliness, relevance and fairness of facts and assessments in them. Misleading or unfair records concerning a child, for example, can seriously affect him. Where there are reasonable grounds to believe that the giving of access to records sought by a guardian would be contrary to the interests of the welfare of the record-subject, the record-keeper should be able to refuse access. In order to provide some guidance to record-keepers, and those reviewing their decisions, legislation should specify the matters to be taken into account when this decision is made. Two of these matters are the special responsibility towards children that their parents have and the need that children have for special safeguards and care. The ability of the guardian to exercise a right of access to the records concerning the child is in fact such a special safeguard. (para. 1275)

25.39 *Privacy and Confidentiality: Qualified Exemptions.* In most cases, record-keepers will not owe a legal duty of confidence to children in respect of the personal information they hold. But where they do, it would be inappropriate to override that duty simply on the ground that the person seeking access is the child's parent or guardian. Both the exemptions, as recommended by the Commission, are qualified exemptions. The first, protecting the privacy of third parties (in these cases, the child, mentally incompetent person or person of unsound mind who is the record-subject), only applies if the disclosure of the personal information in the record to the person seeking access (the guardian) would, in the circumstances, be unreasonable. The same applies in the case of the confidential information exemption: it only applies if the giving of the information in the record to the guardian would breach a legal duty of confidence owed to the child or person of unsound mind to an unreasonable extent. Legislation should specifically require record-keepers, in determining whether to refuse access to a guardian on either of these grounds, to have regard to these considerations. Under the Commission's recommendations, the record-keeper will also have the benefit of the mature child's views on whether access should be granted. (para. 1277)

Amendment of Records

25.40 The right to amendment of records of personal information should not be limited or restricted by reference to whether the applicant is a citizen or permanent resident of Australia. (para. 1280)

Procedure and Review

25.41 The procedure for obtaining access to personal records should be the same as that prescribed by the Freedom of Information Act 1982. (para. 1281)

Resources Test

25.42 The resources test, as it appears in the Freedom of Information Act 1982, only permits an agency to refuse a request for access if the effect on the agency's operation is 'substantial and unreasonable'. In the context of the individual's right of access to personal records, the added interest of the individual in access is a matter to be taken into account by the record-keeper in determining whether complying with a particular request would substantially and unreasonably interfere with his operations. The 'resources test' should be part of the privacy regime in the same way as it is part of the Freedom of Information Act 1982. (para. 1283)

Charges

25.43 In keeping with the Commission's general approach of consistency between the Freedom of Information Act 1982 and privacy legislation allowing for access to personal records, record-keepers should be entitled to levy a charge for access to personal records. To permit record-keepers to levy charges is a recognition of the fact that some cost will be incurred in processing requests for access and granting them. The amount of that charge should not be a practical deterrent to record-subjects who wish to exercise the right of access. The maximum amount of the charge that may be levied by a record-keeper should therefore be fixed by regulation. However, where personal information in a record has been corrected or modified after access, the charges imposed for the access should be refunded or, if they have not yet been paid, waived. (para. 1284)

Protection for Those Who Give Access

25.44 Protections should be provided to record-keepers and their officers and employees on the same basis as is provided under sections 91 and 92 of the Freedom of Information Act 1982. (para. 1285)

Review

25.45 *Conciliation and Negotiation*. If a person considers that he has been wrongly refused access by a record-keeper, the Privacy Commissioner will be able to approach the record-keeper to try to persuade him to give access, perhaps through an intermediary. In most instances this will be sufficient. Most record-keepers will obey the law, and not claim unnecessary or dubious exemptions. Most disputes will be resolved quickly and simply by conciliation. (para. 1288)

25.46 *Power of Direction*. The Privacy Commissioner will be an independent official with particular expertise in privacy matters, including the circumstances in which record-keepers can validly claim exemptions from access. He should be able, where appropriate resolution of any aspect of a dispute in relation to access or amendment of a personal record is not otherwise possible, to direct the record-keeper to give access to, or to amend, the record concerned. This should include other matters such as whether intermediary access is appropriate and the form in which the access should be given and, in the public sector, whether a charge should be levied or waived. He should not be able to issue such a direction of his own motion. It should be specifically requested of him by the applicant for access. He should not be able to direct that access be given to records that are exempt. Matters that the Privacy Commissioner should be required to take into account in determining whether to give such a direction should include the ease with which the record-keeper can comply with the direction and the cost (if any) that will be incurred by the record-keeper or any other person if the direction is complied with. The exercise of this power of direction by the Privacy Commissioner should be subject to

review, on the application of either the record-keeper or the record-subject, by the Administrative Appeals Tribunal. A direction once finally made should create an obligation on the record-keeper to comply. It should not be a criminal obligation, but one capable of enforcement in the usual ways in which similar obligations may be enforced, for example, by mandatory injunction. (para. 1289) For the reasons given the Freedom of Information review mechanisms should apply in relation to access to and amendment of personal records under the Commission's proposals in addition to the Privacy Commissioner's powers of direction. (para. 1290)

Use of Personal Information

25.47 Principles 7, 8 and 9 (s. 25.1) are statements of aspiration, not intended to be enforced by the mechanisms of law. They are standards against which conduct can be assessed. They indicate what is desirable. In fact, this aspect of personal privacy is already well protected through the duty of confidence and other branches of the law imposing civil liability for damage to the record-subject and to others from negligent or malicious use of inaccurate personal information. The difficulties involved in requiring consent to all uses of personal information, with civil or criminal sanctions, are too great to warrant further interference, for privacy reasons alone, with the balance struck by present law between the interests of the record-subject and other important values such as freedom of speech. It is undesirable to impose legal sanctions, beyond those that already exist, where a record-keeper has failed to take reasonable steps to ensure that the personal information he is using is accurate, up to date and not misleading. The general mechanisms proposed by the Commission, such as the Privacy Commissioner's power to conciliate disputes, the HRC's public education function, and its function of developing and publishing guidelines and advice (consistent with the basic privacy principles that this report recommends), will be sufficient to ensure appropriate implementation of the use principles. Finally, the right of access to and amendment of personal records will protect the record-subject from use by the record-keeper of inaccurate, out-of-date or misleading personal information when the record-keeper makes decisions about the subject. Using that right, the record-subject will normally be able to ensure that the quality of the personal information that the record-keeper holds about him is consistent with the recommended standard. Accordingly, while the principle of record-subject consent should be adopted by the Parliament, and embodied in the legislative statement of privacy principles, there should be no further legal requirement of consent. (para. 1300)

Disclosure

25.48 To marry Principle 10 (see s. 25.1) into the existing framework of non-statutory law and administrative practice is no easy task. The present law maintains a careful balance between the legitimate interests of individuals in restricting the dissemination of personal information about them and the legitimate interests of others in the community in exercising rights such as freedom of expression. One option would be to recommend that disclosures of personal information without consent or specific lawful authority constitute a criminal offence. In view of the competing interests involved, this would be impracticable. Alternatively, a person who made such a disclosure could face civil action from the record-subject. In the absence of specific damage, this would also be impracticable, as well as introducing considerable uncertainty. Privacy interests are relatively well protected by the existing law, although the duty of confidence and laws relating to defamation and liability for nervous shock protect those interests only incidentally, and in the context of providing compensation for activities that cause other kinds of damage. No general legislative restriction on disclosures should be made for the purpose of privacy protection alone. Such a restriction would unduly disturb the balance that existing laws have achieved between the interests of the community in the unrestricted flow of information and respect for individual rights, including the interests of the individual in maintaining his privacy. (para. 1307)

Defamation

25.49 Further reform of the law of defamation is not warranted in the interests of privacy alone. (para. 1308)

Legal Duties of Confidence

25.50 *Restatement Not Needed.* There is little need for a legislative restatement of the circumstances in which a duty of confidence will arise, at least in relation to personal information. The law confers a cause of action in circumstances that balances appropriately the relevant interests. It is still developing, and its growth should be guided, not forced or stultified. But the HRC should take steps to bring the law to public attention, to ensure that those who may be under a duty of confidence are aware of it. The public education role recommended for the HRC will allow the HRC to publish guidelines and to develop, with record-keepers whose activities are affected by this law, criteria for proper and appropriate information practices. (para. 1377)

25.51 *Who May Enforce a Duty of Confidence?* Defects in the present law, affecting the extent to which it protects privacy interests, should be remedied. The protections of the duty of confidence are not necessarily available to the record-subject. A duty of confidence may only be enforced by the person who is in a relationship of confidence. This may be the subject of the information to which the duty relates. However, in some cases it will not. For example, where a confidential employment reference has been given, the referee may be in a confidential relationship with the employer, but the prospective employee will not. Where a person is under a duty to preserve confidentiality in respect of personal information, the right to enforce that duty should be extended to the record-subject. (para. 1312)

25.52 *Extension of Duties of Confidence.* It should be made clear that, as a general rule, personal information to which a duty of confidence applies should remain protected by that duty no matter into whose hands it might subsequently come. A person who acquires personal information to which a duty of confidence, however created, applies should be subject to that duty if he knows, or ought to know, that the duty exists. (para. 1313)

25.53 *Damages.* The ability of a person to enforce a duty of confidence depends, in part, on the way in which the duty arose. The remedies should be rationalised so that, however a duty arose, both injunctions and damages, on the same bases, will be available to the person seeking to enforce the duty. (para. 1314)

25.54 *Secrecy Provisions.* Legislation should make it clear that, unless the particular secrecy provision otherwise provides, approvals to disclose personal information, given under a secrecy provision in a Commonwealth of Territorial law (including the Crimes Act 1914, s. 70), should not authorise a breach of a duty of confidence that may be involved in the disclosure. (para. 1319)

25.55 *Reform of Secrecy and Disclosure Provisions.* The HRC is an interdisciplinary body with the task of making the judgments that are called for in determining whether a particular secrecy or disclosure provision is needed, and what its form should be. It should do so taking into account the principles for privacy protection contained in this report. But it will also be better placed to take into account other considerations which may be offered to support secrecy provisions and which may have nothing to do with the protection of individual privacy. (para. 1315, 1320)

Some Special Problems

25.56 *Matching.* The HRC should encourage record-keepers, especially those in the Commonwealth public sector, to consult with it before matching programs, including those authorised by general legislation such as the Social Security Act 1947 and the Income Tax Assessment Act 1936, are undertaken. In some cases, it may be appropriate that particular programs not be implemented until full public consultation has taken place through an inquiry under the Human Rights Commission Act. (para. 1321)

25.57 *Logging.* The HRC should encourage record-keepers to log transactions involving the personal information in their systems. They should explore, in specific areas (especially computerised record systems and those that contain information which may be regarded as unusually sensitive for the individuals concerned), the need for further requirements for record-keepers to keep logs of the use

and disclosure of the information in their systems. There should not, at this stage, be a general legal requirement to keep logs. (para. 1325)

26. Cost Considerations

26.1 The Commission's proposals have been developed with the need to balance costs against benefits fully in mind. Where possible, it has used existing institutions, procedures and practices, in some cases modifying or altering them. In summary, the resource implications of the recommendations in this report will not be as drastic as some might fear. The benefits to be achieved from their implementation outweigh the costs that they will occasion. (para. 1328)

27. Effect of Recommendations

27.1 The Commission has consulted extensively with experts, industry groups, professionals and others working in key areas in developing the recommendations in this report. Their ramifications were extensively and generally explored. The discussions identified the problems which some record-keepers might face in implementing changes necessary to accommodate the proposals, and reassured those record-keepers who might see them as holding more than minor, short-term difficulties. (para. 1338)