Parliament of the Commonwealth of Australia

In Confidence

A report of the inquiry into the protection of confidential personal and commercial information held by the Commonwealth

House of Representatives
Standing Committee on Legal and Constitutional Affairs

June 1995

Canberra

ISBN 0 642 22977 5

This document was printed by the Australian Government Printing Service from camera-ready copy prepared by the House of Representatives Standing Committee on Legal and Constitutional Affairs.

Foreword

One of the distinguishing features of the latter part of the twentieth century is that the technological advances that improve our quality of life are only too often accompanied by adverse consequences. These raise questions about the nature of so-called 'progress'. Better access to information and improved communication has benefited us all but has also raised the spectre of 'Big Brother'. The fact that the vast bulk of information is now held in electronic form creates possibilities for unauthorised access and distribution that could not be comprehended even a decade ago.

There is no doubt that the Commonwealth Government's ability to collect and analyse information has public utility advantages. For example, there is greater fairness to the taxpayer as it becomes more difficult for people to evade tax or falsely claim social welfare benefits. However, the vast increase in the amount of personal and commercial information collected by the Commonwealth increases the potential for the accidental or deliberate misuse of that information. Further, it creates the possibility of a silent, invisible but nonetheless insidious erosion of individual rights to privacy. This intrusion into personal privacy is not the consequence of deliberate policy measures. It results from an accumulation of small changes to legislation and administrative practice affecting the amount of information held and the procedures and attitudes of the guardians of that information. Of particular concern is the increasing practice of collecting information for one purpose and using it for additional purposes.

The object of this inquiry has been to consider the Commonwealth's handling of confidential personal and commercial information. Not surprisingly, the handling is exercised with varying degrees of efficiency across different agencies. Those agencies which hold the most sensitive confidential third party information tend to have better developed systems for its protection although this is by no means universal. In general, the Committee found that the protections afforded to such information are neither comprehensive nor reliable.

Protection has not kept pace with the potential for abuse of the trust placed in the Commonwealth. The Committee considers that there is a need to enhance the 'privacy culture' of the public sector. This should be accompanied by improved capacity for information technology security systems to detect breaches of the conditions in which confidential information is held. The penalties for abuse of the Commonwealth's privileged position in relation to holding confidential third party information need to be consistent. The current position in which penalties are spread across a range of individual acts should be revised in favour of consolidation of offence provisions and penalties in the Crimes Act. This would ensure consistent treatment of similar types of offences. It would also emphasise the serious nature of breaches of trust by Commonwealth officers. The report also considers the desirability of extending the protections offered by the privacy principles to the private sector and the Committee recommends the establishment of a national privacy code.

Over the course of the inquiry we have been assisted by many people. I would like to thank all those individuals and organisations who provided evidence and support throughout the inquiry. I would also like to thank the members of the current and

previous Legal and Constitutional Affairs committees and the staff in both parliaments who have worked on the inquiry and report.

The Committee hopes that its report will be useful to the many Commonwealth agencies who are responsible for the protection of confidential third party information. Above all we hope the report will safeguard the people and organisations of this country who, for sound public policy reasons, must provide government with details of their personal and commercial affairs. They have a right to expect that their privacy will be respected and protected.

Daryl Melham, MP
Chair

Contents

Terms of reference

The Committee shall inquire into and report on the adequacy of the existing protections for confidential personal and commercial information (third party information) held by the Commonwealth Government and its agencies and, in particular:

(a) the adequacy of existing administrative measures for safeguarding third party information held by Government agencies, and the need to ensure that senior managers of such agencies are responsible for these matters;

(b) the effect which the existing legal safeguards for third party information may have in inhibiting the legitimate transfer of information between Government agencies;

(c) the adequacy of the penalties and administrative sanctions which can be applied to officers who wrongly disclose third party information;

(d) the adequacy of the existing penalties which can be applied in relation to persons who procure the wrongful disclosure of such information;

(e) the application which the criminal law should have in relation to such matters;

(f) the effectiveness of existing civil and statutory remedies for third parties in circumstances where information relating to them has been wrongly disclosed, and the need for compensation in such circumstances; and

(g) the appropriateness of the legislative and administrative provisions which govern access to third party information - particularly in relation to the length of time such information is treated as confidential and the circumstances under which it may be released.

The Committee shall also examine the findings of the New South Wales Independent Commission Against Corruption investigation into the unauthorised release of government information, and report on the implications of these findings for information handling practices in Commonwealth administration.

Standing Committee on Legal and Constitutional Affairs

Members **37th Parliament**

Chair	Mr Daryl Melham MP
Deputy Chairman	Mr Alan Cadman MP
	Hon Michael Duffy MP
	Hon Wendy Fatin MP
	Hon Clyde Holding MP
	Mr Mark Latham MP (from 9 February 1994)
	Mr Christopher Pyne MP (from 10 May 1994)
	Rt Hon Ian Sinclair MP
	Mr Peter Slipper MP
	Hon Peter Staples MP (from 9 February 1994)
	Mr Lindsay Tanner MP
	Mr Daryl Williams AM QC MP
	Ms Mary Crawford MP (until 9 February 1994)
	Hon John Kerin MP (until 22 December 1993)
	Mr Alexander Somlyay MP (until 10 May 1994)

Committee Secretary	Ms Judy Middlebrook (from November 1993) Mr Grant Harrison (to November 1993)
Inquiry Secretary	Ms Claressa Surtees (from January 1995) Ms Lorraine Ball (to August 1994)
Research staff	Ms Kelly Williams (from March 1995) Mr Michael Wright (from September 1994)
Administrative support	Mrs Di Singleton Ms Gemma Searles

Members **36th Parliament**

Chair	Mr Michael Lavarch MP
Deputy Chairman	Mr Alan Cadman MP
	Mr Kevin Andrews MP
	Mr Peter Costello MP (to 14 September 1992)
	Hon Janice Crosio MP
	Hon Clyde Holding MP
	Mr Duncan Kerr MP
	Mr Daryl Melham MP
	Mr Chris Miles MP (from 14 September 1992)
	Mr Michael Ronaldson MP
	Hon Gordon Scholes MP
	Rt Hon Ian Sinclair MP
	Mr Keith Wright MP

Committee Secretary	Mr Grant Harrison
Inquiry Secretary	Ms Lorraine Ball
Administrative support	Ms Louise Carney

Glossary and abbreviations

AAT	Administrative Appeals Tribunal
ACS	Australian Customs Service
AHEC	Australian Health Ethics Committee
AIHW	Australian Institute of Health and Welfare
ANAO	Australian National Audit Office
APS	Australian Public Service
ASC	Australian Securities Commission
ATO	Australian Taxation Office
AUSTEL	Australian Telecommunications Authority
AUSTRAC	Australian Transactions Reports and Analysis Centre
DIEA	Department of Immigration and Ethnic Affairs
DILGEA	Department of Immigration, Local Government and Ethnic Affairs
DOD	Department of Defence
DPP	Director of Public Prosecutions
DSD	Defence Signals Directorate
DSS	Department of Social Security
FOI	freedom of information
Gibbs Committee	Review of Commonwealth Criminal Law, chaired by Sir Harry Gibbs
HIC	Health Insurance Commission
ICAC	Independent Commission Against Corruption (NSW)
IPPs	Information Privacy Principles
IEC	Institutional Ethics Committees
MOU	memorandum of understanding
NHMRC	National Health and Medical Research Council
PC	Privacy Commissioner
PSC	Public Service Commission
PSM	Protective Security Manual
third party information	information supplied to the government by third parties, individuals, groups, business etc – about personal and commercial affairs
VCCL	Victorian Council for Civil Liberties

Summary and recommendations

Introduction (Chapter 1)

1. The first chapter of the report covers the background to the inquiry and the scope and structure of the report. An inquiry into the adequacy of the existing protections for confidential personal and commercial information held by the Commonwealth Government and its agencies is an important means of reviewing the two aspects of protection – security and privacy. Concerns in 1992 about well publicised releases of confidential personal information held by Commonwealth agencies, and evidence to the investigation into the unauthorised release of government information by the New South Wales Independent Commission Against Corruption, led to the inquiry.

2. The report has a wide scope, reflecting the terms of reference. It begins with an introduction which describes the inquiry process, surveys the structure of the report and introduces some of the issues of dealing with confidential third party information. This is followed by a description of the administrative and legal measures for safeguarding such confidential information. The report then considers each of the terms of reference in turn.

3. The responsibility of senior managers for privacy and security matters is addressed. The report then examines the adequacy of administrative safeguards for third party information followed by a consideration of concerns that the existing legal safeguards for third party information inhibit the legitimate transfer of information between Government agencies.

4. The adequacy of penalties and sanctions which apply to officers who wrongly disclose information is then discussed. The next chapter of the report discusses the adequacy of penalties which can apply to persons who procure the wrongful disclosure of information. This is followed by an examination of the application of the criminal law in its protection of confidential third party information.

5. The matter of remedies for third parties and the need for compensation in circumstances where information relating to them has been wrongly disclosed is then considered. The final term of reference is then addressed in the report's discussion of the appropriateness of provisions governing access to third party information.

6. The report then examines suggestions for a national privacy code to apply to public and private sector organisations alike. It concludes with a brief review of matters raised recently that illustrate some of the problems identified elsewhere in the report.

Description of administrative and legal measures (Chapter 2)

7. A range of administrative and legal measures provide access to and protection of third party information held by the Commonwealth Government and its agencies. Some measures are common to agencies throughout the Australian Public Service (APS), while

other measures apply to a specific agency or activity. The result is that each agency has a unique combination of administrative and legal measures which protect the confidential information with which it deals.

8. Administrative measures which apply generally include, guidelines and training programs provided by the Public Service Commission, voluntary guidelines issued by the Privacy Commissioner and the Attorney-General's Department's *Protective Security Manual*. These measures may be adopted by individual agencies although they are not compulsory measures. In addition, local guidelines, instructions and training programs may be provided within agencies. The actual measures which apply in an agency vary because the responsibility for managing staff in the APS rests largely with individual agencies through the agency head who adopt administrative measures according to the individual requirements of each agency.

9. The framework for the APS is provided by the *Public Service Act 1922* and the *Public Service Regulations* made under that Act. The main rule covering the disclosure of information is regulation 35 which prohibits the disclosure of information except in the course of official duty. Under regulation 8A, officers have a duty to comply with official guidelines, directions and recommendations. The combined effect of these regulations is that an unauthorised disclosure of confidential information by an officer will attract the disciplinary measures set out in sections 55 to 66 of the Public Service Act.

10. The *Protective Security Manual* was issued by the Attorney-General's Department following consultation with the Privacy Commissioner and Commonwealth agencies. It is not binding on agencies and will apply only if expressly adopted by the agency head. It contains administrative policies, standards of practice, principles and common procedures for the protection of official information, including information technology aspects of protection.

11. The Acts which provide for the protection of confidential third party information under administrative law apply broadly. These include, the *Freedom of Information Act 1982* (FOI Act), the *Archives Act 1983* and the *Privacy Act 1988*. The focus of the FOI Act and the Archives Act is on access to information held by the Commonwealth Government. Each of these two Acts contains exemptions which balance the objective of providing access to government information against legitimate claims for the protection of sensitive material. The exemption categories differ because of the reduced sensitivity of the older documents being accessed under the Archive Act.

12. The Privacy Act establishes a scheme to govern the handling of personal information and imposes rules called Information Privacy Principles (IPPs). Disclosure is generally prevented unless one of the prescribed exceptions applies. A Privacy Commissioner appointed under the Privacy Act, provides advice to agencies concerning their responsibilities in applying the IPPs, and has powers to conduct audits and investigations, and to make determinations about the behaviour of agencies.

13. There is no special regulation of data-matching in the Privacy Act. The *Data-matching Program (Assistance and Tax) Act 1990* provides authority for a computer matching program and requires agencies to comply with guidelines issued by the Privacy Commissioner and set out in a schedule to the Act. As well, the Privacy Commissioner is to monitor and report on agencies' compliance with the Act or guidelines, investigate breaches of the Act or guidelines and advise agencies of their obligations under the Act.

14. The general law of confidence is also applicable to the protection of confidential third party information. So too are general secrecy provisions in the *Crimes Act 1914*. Section 70 and subsection 79(3) deal with the disclosure of information by Commonwealth officers; section 73 deals with the corruption and bribery of Commonwealth officers; and sections 76B and 76D prohibit unlawful access to data in Commonwealth and other computers. There are also some 150 specific secrecy provisions in Commonwealth legislation, many of which are located in subordinate legislation, such as regulations.

Administrative safeguards and the accountability of senior managers (Chapter 3)

15. Within the legislative framework there are many administrative measures for safeguarding third party information held by Commonwealth Government agencies. Responsibility for those measures rests with individual agencies and agency heads. The agency head and the Senior Executive Service (SES) officers of an agency are the senior managers who are the focus of attention in trying to set effective standards of behaviour.

16. The role of the Public Service Commission (PSC) in providing guidance to the SES on standards of conduct and ethics in the public sector is important in this regard.

17. While it is not necessary to develop legislation that would impose personal liabilities on agency heads in relation to the protection of third party information, it is desirable for agency heads to have express responsibility for the protection of confidential third party information held by the Commonwealth Government.

Recommendation 1
The Committee recommends that there be a description of responsibilities of heads of agencies in the *Public Service Act 1922*. The description should include responsibility for the protection of confidential third party information held by the Commonwealth Government. (p. 27)

18. Guidelines, operating manuals and training have a significant effect on shaping the environment in which people work and in shaping attitudes within the work place. The agency head should also be responsible for the provision of guidelines, operating manuals and training to officers within an agency.

Recommendation 2
The Committee further recommends that the head of an agency be responsible for providing all agency staff with comprehensive guidelines and operating manuals relating to the protection of confidential third party information that it holds. In addition, the head of an agency should be responsible for ensuring that all staff of the agency receive training in the protection of confidential information and compliance with relevant guidelines and operating manuals. (p. 27)

19. The rationale for collecting confidential information from individuals is that it is needed for the proper functioning of government. Information Privacy Principle 1 relies on this rationale. A real commitment to privacy and protection of confidential third party information requires a demonstration that only necessary information is collected. Each agency which collects such information should expressly consider this issue and report on the outcome.

Recommendation 3
The Committee recommends that for each agency that collects third party information, the agency head be responsible for monitoring the on-going need for that information. Each agency should report annually to the Privacy Commissioner on the outcome of that monitoring with regard to personal information. Each agency should state in its annual report the outcome of that monitoring with regard to commercial information.(p. 28)

20. Extreme caution should be exercised in the delegation of certain functions relating to the protection of third party information. As a matter of policy, discretion to release information should be held only by a limited number of senior officers and should not be able to be delegated to junior officers. Such a policy would indicate that the disclosure of third party information is not routine, and that a mere claim of convenience is not sufficient to justify broader delegation. The limited number of senior managers empowered with a discretion of release information should operate to reinforce the important status of the power to release information.

Recommendation 4
The Committee recommends that the power to disclose confidential third party information held by a Commonwealth Government agency be given only to a limited number of clearly identified senior executive officers who are, where practicable, at a level no lower than SES Band 2. (p. 30)

21. The fact of disclosure should be a matter of record and reporting that will assist in the auditing and monitoring of the exercise of this important power.

Recommendation 5
The Committee recommends that agencies be required to provide, within 14 days of the disclosure, reasons to the Privacy Commissioner for an authorised disclosure of personal information being made. (p. 30)

Recommendation 6
The Committee recommends that each Commonwealth Government agency keep a record of authorised disclosures of confidential third party information for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is disclosed, the names of individuals and organisations to whom that disclosure is made, and the date of disclosure. (p. 30)

Implications of ICAC findings for Commonwealth agencies

22. The New South Wales Independent Commission Against Corruption investigation into the unauthorised release of government information found that Commonwealth officers had made unauthorised disclosures of confidential third party information. They had done so for money or for supply to an informal information exchange club. While the ICAC investigation revealed problems in certain Commonwealth agencies there is no reason to believe that other officers were not engaging in those or similar practices, and that similar practices were not occurring elsewhere.

23. A recurring theme in the responses of agencies the Committee questioned in relation to the ICAC report was that the activities revealed were to some degree due to employees misunderstanding their responsibilities and releasing information in the belief that it was part of their duties. Such lapses raise questions about the privacy culture or ethos in the public service.

24. Unfortunately, the evidence does not support the claims of many to this inquiry that an effective privacy ethos exists. It is important for an agency to have an ethos that fosters and nurtures the protection of confidential information. This can overcome the perceptions within agencies that privacy requirements either get in the way of officers performing their duties, or do not matter if information is just accessed and not passed on. Senior managers have a very important role to play in promoting a privacy culture within an agency and it is unfortunate that many senior managers do not appear to be actively involved in privacy matters.

Recommendation 7
The Committee recommends that each agency have a senior manager who is responsible for implementing and promoting privacy standards and the protection of information within an agency. The chosen senior manager should be a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2. (p. 35)

25. The Committee considers that the development and enhancement of a culture that is sensitive to the responsibility of handling third party information is a matter of great importance and urgency. It is necessary that such a culture be created and fostered within the public sector generally but particularly important for those agencies holding large quantities of confidential information.

26. Agencies would benefit by establishing focus groups or 'information privacy committees' to review both administrative procedures and compliance with legal requirements. Such committees would assist agency heads to fulfil their responsibilities and their very existence would enhance the privacy ethos.

Recommendation 8
The Committee recommends that each agency head establish an Information Protection Committee with the objective of monitoring the protection of third party information within the agency and disseminating information which would foster the protection of that information. (p. 35)

27. As well as indicating that confidential information held by the Commonwealth has been bought and sold for illegal purposes, the evidence to ICAC provides an insight into the nature of the demand for that confidential information and of the persons who create that demand. As part of the active role that senior managers must take in promoting privacy within an agency, they should seek to inform themselves about the possible unsatisfied demand for confidential third party information held by that agency.

Recommendation 9
The Committee recommends that the senior executive service officers of agencies inform themselves of the demand for confidential third party information held by their respective agencies. (p. 36)

28. Auditing and investigation programs under both the *Audit Act 1901* and the *Privacy Act 1988* contribute to the assessment of the adequacy of public service wide and agency specific measures for the protection of confidential third party information.

29. Inter-agency agreements on transfers of confidential third party information encourage a disciplined approach to such transfers. There should be a clear commitment to regularised access to confidential third party information, and agencies should enter into inter-agency arrangements wherever possible in accordance with guidance from the Privacy Commissioner.

Recommendation 10
The Committee recommends that agencies be required to enter into inter-agency agreements on the disclosure of confidential personal information to be approved by the Privacy Commissioner. (p. 47)

30. While the physical security of information stored in paper form is still a vital issue for most agencies computer storage is a significant security issue. It is critical that agencies keep under continuous review their computer security policies. There is a strong need for a comprehensive approach to security within an agency.

Recommendation 11
The Committee recommends that all agencies adopt a comprehensive security system such as that provided by the *Protective Security Manual*. Agencies should adapt the general standards to their particular circumstances. (p. 51)

31. Computer storage of information, including the large volume of information that can be stored on computers and the ease with which data can be accessed and used, poses a significant risk to the privacy of individuals. Agencies should adopt adequate standards and guidelines for computer security.

Recommendation 12
The Committee recommends that all agencies adopt adequate standards for computer security. Guidelines should be developed after incorporating advice from existing government agencies with expertise in computer security. (p. 51)

32. Computer security should be the subject of express audit to assess its effectiveness. To this end computer security should be integrated into the ANAO program.

Recommendation 13
The Committee recommends that the Australian National Audit Office conduct security efficiency audits of computer systems. (p. 52)

Recommendation 14
The Committee recommends that sufficient resources be allocated to the Australian National Audit Office to support this role. (p. 52)

33. In the public sector working environment, where the opportunity for home based work is likely to increase, security for portable computers is an important issue. Consequently, the installation and activation of security features for portable computers is an important computer security matter, as are guidelines for officer behaviour. Computer security policies should expressly cover portable computers.

Recommendation 15
The Committee recommends that security manuals specifically address the process required to authorise work taken out of the fixed office site and the security features of portable computers. (p. 53)

34. As contracting out of work by Commonwealth agencies has become more common, it has been argued that this has weakened the protections of the *Privacy Act 1988*. This is so because individuals can not assert their rights under the Privacy Act in relation to activities undertaken by a contractor on behalf of a Commonwealth agency.

35. In the short term, the Committee favours the legislative approach of amending the Privacy Act to make the contractor liable for observance of the Information Privacy Principles as if the contractor were the agency. A long term solution would include the development and implementation of a national privacy code.

> *Recommendation 16*
> The Committee recommends that the *Privacy Act 1988* be amended to make a contractor to a Commonwealth agency primarily liable for observance of the Information Privacy Principles as if the contractor were the agency. (p. 55)

36. Generally agencies have adopted adequate security policies. However, there is evidence that the practical systems put in place to give effect to these policies have not always been satisfactory.

Legal safeguards and the legitimate transfer of information (Chapter 4)

37. Legal safeguards for third party information are to be found in both the common law and statute law. The critical legal measures are contained in the *Privacy Act 1988*, various specific Commonwealth Acts containing secrecy provisions, the *Freedom of Information Act 1982* and the *Data-matching Program (Assistance and Tax) Act 1990*.

38. The balancing of competing interests is an underlying difficulty in determining legitimate transfers of information. Traditionally some agencies have had wide access to confidential third party information. They regard this position as desirable because transfers are made morally if not legally for legitimate reasons. The competing interests are *individual privacy, free flow of information and fraud detection and prevention.*

39. Significantly, the Privacy Commissioner and most agencies seeking transfers of information agree that the philosophy underpinning the *Privacy Act 1988* is correct, even if the interpretation of the provisions is not agreed. The Privacy Act should be the primary means by which to regulate the flow of information between government agencies.

40. Secrecy provisions have failed to meet the need for flexible regulation of the transfer of information between government agencies. It is also difficult to incorporate adequate privacy protection safeguards in secrecy provisions.

Recommendation 17
The Committee recommends that transfers of confidential personal information between Commonwealth Government agencies should be regulated by the *Privacy Act 1988*, rather than by the by the secrecy provisions in specific statutes. The Privacy Act should be reviewed and amended to ensure that the necessary degree of protection for transferred information is maintained. (p. 63)

Recommendation 18
The Committee further recommends that each Commonwealth Government agency keep a record of authorised transfers of confidential personal information between agencies for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is transferred, the names of individuals and organisations to whom that transfer is made, and the date of the transfer. (p. 63)

41. A high priority should be given to clarifying the Information Privacy Principles. The interpretation of the IPPs is a vexed matter. Where other Acts specifically address disclosure or protection of information, the current approach of the Privacy Commissioner should be followed, and the IPPs should not be used to create extra exceptions. To do so would undermine the protections expressly provided by the secrecy provisions and would provide a distortion of the protective purpose of the Privacy Act. The relationships between these other Acts and the Privacy Act should be addressed in the Privacy Act.

Recommendation 19
The Committee recommends that the *Privacy Act 1988* be amended to provide that where an Act other than the Privacy Act deals expressly with a matter of permissible use and disclosure, IPPs 10 and 11 do not operate to provide additional grounds for disclosure. (p. 64)

42. The exceptions under IPPs 10.1(c) and 11.1(d) for disclosures authorised by law are capable of broad interpretation. A broad interpretation would make the IPPs meaningless. To overcome this difficulty, the exceptions in IPPs 10 and 11 should be more specific.

Recommendation 20
The Committee recommends that as part of the review of the scope of the *Privacy Act 1988*, that the exceptions in Information Privacy Principles 10 and 11 be more specific. (p. 67)

43. The exception in the IPPs for protection of the public revenue should be clarified by amendment to the Privacy Act to put the meaning of the expression beyond doubt.

Recommendation 21
The Committee recommends that the *Privacy Act 1988* be amended to clarify the meaning of the term 'protection of the public revenue'. (p. 68)

44. Permitted transfers of confidential information between agencies should be accommodated by clarification of the Information Privacy Principles through legislative exceptions.

Recommendation 22
The Committee recommends that permitted transfers of confidential third party information between Commonwealth Government agencies be accommodated by way of exceptions to the Information Privacy Principles. (p. 68)

45. Responses to the Privacy Commissioner's guidelines for data-matching under the *Data-matching Program Assistance and Tax) Act 1990* have been prompt and rigorous. In contrast, in relation to voluntary data-matching guidelines, while some agencies have agreed to comply, only two agencies have prepared appropriate documentation for the data-matching programs they are conducting.

46. The nature of data-matching means that the scope for accessing information is extensive and uniform high standards need to apply to such activities.

Recommendation 23
The Committee recommends that uniform controls for data-matching carried out by Commonwealth Government agencies be made a legal obligation and incorporated into the *Privacy Act 1988*. (p. 70)

47. Major data-matching programs should proceed only after receiving the express approval of an SES officer.

Recommendation 24
The Committee further recommends that major data-matching programs proceed with the authority of a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2. (p. 71)

48. There should be a discretion for agency heads to authorise the disclosure of information in certain circumstances, where the use of information for its original

purpose involves disclosure but where the disclosure is not covered by the IPPs. An exercise of this discretion should be subject to the scrutiny of the Privacy Commissioner.

Recommendation 25
The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information held by the agency where notification of or consent for disclosure is not a reasonable possibility. This discretion is to be subject to:

- the necessity of the disclosure;
- the disclosure being an integral part of the use for which the information was obtained; and
- notification or consent procedures being demonstrably inappropriate. (p. 72)

Recommendation 26
The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner. (p. 72)

49. There should be a discretion for agency heads to authorise the disclosure of information in certain circumstances where consent could not be obtained. An exercise of this discretion should be subject to the scrutiny of the Privacy Commissioner.

Recommendation 27
The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information where a disclosure is clearly in the individual's interest and consent could not be obtained. (p. 73)

Recommendation 28
The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner. (p. 73)

Adequacy of sanctions and penalties relevant to wrongful disclosure of third party information (Chapter 5)

50. The Committee examined the adequacy of the administrative sanctions in the Public Service Act. These sanctions would apply to the wrongful disclosure of third party information. They include dismissal, a maximum fine of $500, demotion, reduction of salary to a lower point in the same salary range, transfer, admonition or a combination of these measures.

51. The Committee considered the range of sanctions, consistency and delay in the application of sanctions and the persons to whom the sanctions apply. The Committee concluded that the range of administrative sanctions is adequate and any increase in monetary penalty would make the fine more like a criminal penalty and not in accordance with the philosophy of a disciplinary code.

52. This conclusion was in keeping with the recommendation of the Public Service Act Review Group (the McLeod Report) that the language of the misconduct provisions should be decriminalised because the relevant offences concern administrative misdemeanours.

53. The relevant criminal penalties are contained in general and specific secrecy provisions. The provisions of the *Crimes Act 1914* which are relevant to the disclosure of third party information ('general secrecy provisions') include section 70, subsection 79(3), section 73 and sections 76B and 76D. Section 70 prohibits the disclosure of information by Commonwealth officers, subsection 79(3) prohibits the communication of prescribed information, section 73 deals with the corruption and bribery of Commonwealth officers and sections 76B and 76D create offences relating to computers. A maximum penalty of two years imprisonment is, in most cases, standard for the general secrecy provisions relevant to the protection of third party information.

54. The evidence did not generally focus on the adequacy of the penalties of the general secrecy provisions as departments tended to concentrate on their own specific legislation in assessing the adequacy of penalties for the unauthorised disclosure of third party information.

55. There have been few prosecutions under the general secrecy provisions in the Crimes Act. This may not be indicative of the adequacy of the penalty in deterring potential offenders, but rather of the small number of people actually apprehended for those particular crimes. The Committee also focussed on the adequacy of the general secrecy provisions themselves.

56. There are a number of problems with the general secrecy provisions. This includes problems with the specification of the duty, problems arising from the breadth of the information protected, difficulties in relation to the prosecutions and the limited application of sections 73, 76B and 76D to the wrongful disclosure of third party information.

57. There are more than 150 secrecy provisions in Commonwealth laws and more than 100 different statutes which contain one such provision or more. Some departments commented favourably on the adequacy of the penalties in the secrecy offences in their respective legislation (for example, the Australian Customs Service and the Australian Taxation Office).

58. The penalties relevant to the secrecy provisions in statutes other than the Crimes Act ('specific secrecy provisions') vary greatly. For example, a breach of subsection 130(1) of the *Health Insurance Act 1973* attracts a penalty of $500 while an offence under section 16 of the *Income Tax Assessment Act 1916* carries a $10 000 fine or two years imprisonment or both.

59. The Committee noted an example of inconsistency in penalties between two statutes where the information protected did not appear to be more sensitive in one situation than the other (compare subsections 130(1) and 130(9) of the *Health Insurance Act 1973* and subsections 135A(1) and 135A(9) of the *National Health Act 1953*).

60. The adequacy of the specific secrecy provisions was also considered. The provisions have been introduced in a piecemeal fashion and influenced by a variety of philosophies. The provisions protect information to varying extents. There are different qualifications on the prohibitions and the provisions impose varying penalties. The coverage of the specific provisions is uncertain and information held by Commonwealth organisations is not always protected by specific provisions.

61. There appears to be a need for a more organised approach to protecting third party information held by the Commonwealth Government and its agencies. The problems with the general and specific secrecy provisions reveal a need for rationalisation and the Committee canvasses proposals for reform in chapter 7.

Penalties relevant to procuring the wrongful disclosure of third party information (Chapter 6)

62. In recent years there has been increasing recognition of the number of occasions where the wrongful disclosure of confidential third party information is procured from Commonwealth agencies. Procuring information involves convincing officers to leak information to individuals for unlawful purposes. An example of the use which individuals may then make of that information is to sell it to financial institutions which may use the information to locate debtors.

63. There is no general provision in the Crimes Act which makes it an offence to procure the wrongful disclosure of third party information from a Commonwealth officer. Section 70 of the Crimes Act does not directly apply to secondary disclosures. However subsection 5(1) of the Crimes Act, which provides that any person who aids or abets a Commonwealth offence is deemed to have committed that offence, is relevant in this context. This provision may facilitate the prosecution of a person who came to an arrangement with a Commonwealth officer for that officer to unlawfully disclose information to the person. However a second or later recipient of unlawfully disclosed information, who had no direct or indirect involvement in the commission of the original offence by the Commonwealth officer would not have committed an offence, as the aiding and abetting provisions would not apply. A specific offence would need to be created to cover that type of offence.

64. Some departments have specific provisions dealing with procuring/soliciting third party information. The Australian Taxation Office submitted that the penalties which attach to the procurement offences in the *Income Tax Assessment Act 1936* and the *Taxation Administration Act 1953* were adequate. On the other hand, the Australian

Customs Service informed the Committee that there was little that could be done to penalise persons who procure the wrongful disclosure of information under Customs legislation as the relevant provision does not generally prohibit that conduct.

65. The Committee noted that in some circumstances it may be difficult to establish that information was actually disclosed to the procurer in breach of a secrecy provision. Section 8XB(2) of the Taxation Administration Act was cited as a method of dealing with that potential problem. The subsection provides that it is unlawful to obtain taxation information if the information relates to the affairs of another and the circumstances in which the information was obtained would have led a reasonable person to believe the information came from the Commissioner of Taxation, the Deputy Commissioner or the records of other ATO officers and the information was obtained in circumstances that gave no reasonable cause to believe that the communication was authorised by law.

66. Although some statutes contain regimes which prohibit the procurement of confidential third party information, procuring that information is not expressly prohibited by all statutes. This, combined with the limited application of the Crimes Act in this area, suggests that some of the existing provisions and penalties in this area are inadequate and in need of reform.

Application and rationalisation of the criminal law (chapter 7)

67. The application of the criminal law is an appropriate response to the unauthorised disclosure and procurement of confidential third party information in some circumstances. Criminal sanctions are particularly appropriate where information is deliberately released for profit, or with malicious intent. However, the criminal law should not operate more widely than is needed as the imposition of criminal sanctions can have serious repercussions and may involve deprivation of an individual's liberty.

68. The Review of Commonwealth Criminal Law (the Gibbs Committee) recommended that section 70 and subsection 79(3) of the Crimes Act be repealed and that the criminal law should only apply to the unauthorised disclosure of a limited number of categories of official information where disclosure could harm the public interest. The Gibbs Committee thought that the unauthorised disclosure of confidential third party information should be prohibited by criminal sanctions in specific statutes and thus it would not be the subject of a general criminal law.

69. This Committee's view is that confidential third party information is most adequately protected by general laws located in one statute. General provisions would have a number of advantages. They would provide a central focus. They would also avoid the situation where officers who disclose information obtained under one enactment may face prosecution while officers who disclose information obtained under a different enactment may not be subject to criminal sanctions. Similarly, general provisions would avoid the situation where a party soliciting information from officers in some agencies may be liable to prosecution while a party soliciting equally sensitive information held by another agency is not liable to prosecution. General provisions would also enable the application of a consistent set of penalties, according to the sensitivity of the information disclosed. Finally, general provisions may raise the consciousness of public servants and would mean that officers only need to be familiar with one set of obligations.

70. The Committee considers that the most appropriate location for the general provisions is in the Crimes Act. This location indicates the seriousness with which the offences are viewed; it contributes to the community perception of the gravity of the offence and may act as a greater deterrent than if the provisions were located in another statute.

Recommendation 29
The Committee recommends that the protection of confidential personal and commercial information should be the subject of general offence provisions located in the *Crimes Act 1914*. (p. 118)

71. The Committee identified two options for rationalisation of the existing secrecy provisions, namely consolidation and partial consolidation in the Crimes Act. Consolidation involves locating all the law relevant to the protection of confidential third party information in the Crimes Act. These provisions would include a description of the information protected, the prohibited conduct and the penalties.

72. However, there may be doubt as to whether a description of the information currently protected by all statutes could be consolidated. Another problem associated with consolidation is that departments may wish to address, and maintain control of, matters that are of particular concern to them in departmental legislation rather than vest that function in the Crimes Act. Thus there may be difficulties in obtaining broad inter-departmental agreement and approval for totally consolidated provisions in the Crimes Act.

73. With the partial consolidation option, the Crimes Act would contain provisions prohibiting the relevant conduct and the penalties for such conduct. The description of the information protected would be defined by reference to enactments contained in a schedule to the Crimes Act. The various departments would thereby retain the responsibility for determining the information to be protected. Descriptions of the lawful transfers of third party information between government agencies would be located in the Privacy Act (refer to recommendations 17 and 22).

74. The Committee favours partial consolidation in the Crimes Act. It recognises that some departments have regimes dedicated to ensuring third party information is protected (for example, the Department of Social Security and the Australian Taxation Office). However, the Committee views this proposal as the most favourable option for rationalising the existing provisions and ensuring that confidential information held by the Commonwealth Government is adequately and consistently protected in all circumstances.

Recommendation 30
The Committee recommends that general offence provisions, protecting confidential third party information held by the Commonwealth Government and its agencies, be included in the *Crimes Act 1914*. The Committee further recommends that the information protected by these general provisions be defined by reference to other enactments. (p. 122)

75. The Report of the Independent Commission Against Corruption commented that unauthorised disclosure of confidential information should be prohibited at every point on the distribution chain. The report recommended that 'unauthorised dealing in

protected government information be made a criminal offence' in New South Wales. The Committee endorses the view that all unauthorised dealings with government-held third party information should be prohibited and recommends similarly in the Commonwealth sphere.

76. In the Committee's view, unauthorised dealing in confidential third party information includes at least the following conduct: unauthorised access, unauthorised use (including disclosing and recording confidential information), procuring, soliciting, soliciting by making untrue representations, offering to supply, holding oneself out as being able to supply confidential information and publishing such information. The Committee does not favour a public interest defence to publishing confidential third party information.

Recommendation 31
The Committee recommends that unauthorised dealing in confidential third party information held by the Commonwealth Government and its agencies, should be prohibited at every point on the distribution chain by general offence provisions in the *Crimes Act 1914.* (p. 127)

Remedies and the need for compensation (Chapter 8)

77. Remedies are available to individuals in some circumstances where information about them has been wrongly disclosed under the *Privacy Act 1988.* Remedies are also available under the general law of confidence, although such actions may be both protracted and expensive.

78. If the Privacy Commissioner finds a complaint to be substantiated, he may make a determination to provide a remedy to the individual who complained.

79. A remaining deficiency of the scope of remedies in such cases is that the Privacy Act does not provide redress where information has been unlawfully disclosed by an employee acting for her or his own purposes, and the Commonwealth agency can show that it has not breached privacy standards required under the Privacy Act. It is appropriate for third parties to have more comprehensive access to compensation from Commonwealth agencies where information is wrongly disclosed. The Commonwealth should be regarded as holding third party material 'in trust' for the persons and organisation which are the subject of such records. Accordingly, a 'strict liability' scheme for compensation administered by the Privacy Commissioner should be introduced.

Recommendation 32
The Committee recommends that the *Privacy Act 1988* be amended so that, if there is an unauthorised disclosure of personal information held by a Commonwealth agency, a person's right to compensation from the Commonwealth agency would be established by the unauthorised disclosure, regardless of whether there has been a breach of an Information Privacy Principle by the agency. (p.136)

Access to third party information (Chapter 9)

80. The provisions which govern access to third party information are generally contained in the *Archives Act 1983* and the *Freedom of Information Act 1982* (the FOI Act). The Archives Act creates a statutory right of public access to Commonwealth records that are more than thirty years old. Records which fall within the categories of exempt records are not released after the thirty year period. Exempt records include information where disclosure would involve the unreasonable disclosure of information relating to the personal affairs of any person, information relating to trade secrets and information where disclosure would constitute a breach of confidence.

81. In relation to personal affairs, the sole criterion for deciding whether access should be given to such information is whether disclosure would constitute an unreasonable disclosure of an individual's affairs. The *Australian Archives Access Manual Part 1* considers the meaning of this term. It notes that the issue is a matter of individual perception and rarely subject to a consensus of views.

82. Australian Archives informed the Committee that it had only received a small number of internal reconsideration applications relating to personal privacy exemptions and none of those applications had proceeded to the Administrative Appeals Tribunal. Archives also noted that it had not received any complaints from members of the public about personal information released under the Archives Act. The Committee concludes that, on the evidence presented, the provisions in the Archives Act which govern access to third party information, including the provision for public access to records after thirty years, are appropriate.

83. The Privacy Commissioner commented on the use of the expression 'information relating to personal affairs' in the Archives Act. Prior to 1991 this expression was also used in the FOI Act. It was given a restricted interpretation by the Administrative Appeals Tribunal and was subsequently replaced with 'personal information about any person' which was viewed as a broader term. This amendment brought the terminology of the FOI Act in line with that in the Privacy Act in this respect. The Privacy Commissioner suggested the expression in the Archives Act could be amended in this way. The Committee considers that, in the interests of consistency, it may be useful if the relevant expression in the Archives Act were amended in this manner.

Recommendation 33
The Committee recommends that consideration be given to amending the *Archives Act 1983* by replacing references to 'information relating to the personal affairs of any person' with 'personal information about any person' and inserting the definition of 'personal information' found in the *Freedom of Information Act 1982* and the *Privacy Act 1988*. (p. 144)

84. The FOI Act establishes a general right of access to government information. This right is, however, subject to certain exemptions. The exemptions include documents which affect personal privacy, relate to business affairs and contain material obtained in confidence. The Act is currently being reviewed by the Australian Law Reform Commission and the Administrative Review Council.

85. The Attorney-General's Department commented, and others agreed, that it is not appropriate to set an arbitrary deadline at which information will lose its confidentiality. But rather, in determining whether information should be kept secret, it is preferable to examine the interests which will be affected by disclosure.

86. Examining the interests which will be affected by disclosure rather than setting a deadline does not necessarily conflict with the 30 year general rule in the Archives Act. Under the Archives Act, the exemptions to public access are dependent on whether the disclosure would be unreasonable and under the FOI Act, the exemptions are dependent on potential damage to third parties. Examining the interests which will be affected by disclosure is also relevant in any action for breach of confidence.

Public register information

87. The Privacy Act regulates the handling of personal information held by Commonwealth agencies with some exceptions. Public register information is one such exception because the information is publicly available. Public registers which contain personal information include the records of the Australian Securities Commission, the electoral roll and court records.

88. Advances in information technology allow public register information to be searched, analysed and modified. This information may then be used for purposes in addition to those for which it was created.

89. In light of these technological advances, the Privacy Commissioner suggested that:

- the reasons for allowing access to existing public registers may need to be reviewed, particularly where information technology advances allow the information to be used for purposes in addition to that for which it was collected;
- where public register information is used for other purposes, consideration should be given to limiting access to the registers or limiting the purposes for which information obtained from the registers may be used; and
- databases created from public register information should be subject to the tests which apply to records of information containing information not otherwise available to the public.

Recommendation 34
The Committee recommends that the Privacy Commissioner coordinate a review of the reasons for allowing access to public registers, particularly where technology permits the information contained on public registers to be used for purposes in addition to that for which it was collected. The review should also consider whether any limits need to be imposed on access to public register information or on the purposes for which such information can be used. (p. 149)

90. The Electoral Roll was considered as an example of public register information. The public has access to the electoral roll in hard copy or microfiche form. The Australian Electoral Commission (AEC) informed the Committee that this information can now be scanned electronically and the newly created data bases may be sold to commercial interests.

91. End use restrictions on the use of electoral roll information currently exist in relation to information obtained on tape or disk by Senators, members of the House of Representatives, political parties and other persons or organisations that the AEC determines can receive the information on tape or disk.

92. The Commission submitted that the problem of business interests using electoral information for commercial purposes may be partly alleviated by imposing end use restrictions (which currently exist in relation to tape or disk) on all data obtained from the Roll regardless of its source (that is, microfiche, tape or disk). The Committee agrees with this proposal although it notes the difficulties in policing such restrictions.

Recommendation 35
The Committee recommends that the *Commonwealth Electoral Act 1918* be amended so that the end use restrictions which currently apply to electoral roll data contained on tape or disk also apply to the same data contained on microfiche or in hard copy. (p. 152)

Access to medical records for statistical and research purposes

93. Medical records can be disclosed for epidemiological purposes without the consent of the person involved. Epidemiological research is based on information about the health status of individuals and their exposure to factors that may affect their health.

94. The *Australian Institute of Health and Welfare Act 1987* allows the Australian Institute of Health and Welfare (AIHW) to release identifiable data to external researchers with the agreement of its ethics committee. The National Health and Medical Research Council (NHMRC) may, with the approval of the Privacy Commissioner, issue guidelines for the protection of privacy in the conduct of medical research. The Privacy Commissioner has advised, and the Institute has accepted, that all relevant NHRMC guidelines be adhered to in respect of research using identifiable data.

95. The NHMRC Statement on Human Experimentation includes a supplementary note on Ethics in Epidemiological Research which provides that consent of subjects should generally be obtained for the use of their records in medical research. The Committee considers that, as a general rule, the consent of a data subject should be obtained before the subject's records are used in medical research.

96. The AIHW maintains a range of statistical collections for the purpose of health research. It maintains two registries, namely the Cancer Registry and the National Death Index.

97. Registration of cancer is mandatory in all States and Territories. The AIHW informed the Committee that data release provisions permit cancer registries to release identified data to individual researchers or institutions where the use of this data for medical research is perceived to be of public benefit and there will be no compromise of information integrity. Individuals are advised that details of their medical condition may be collected pursuant to State legislation. However, individuals are not advised that details of their medical condition may be provided to AIHW and that identifiable data may be released to external researchers.

98. There are a number of options concerning how patients could be most effectively informed about the use that may be made of medical records concerning them. The written or verbal consent of the patient could be obtained before the specimen is sent for cancer registration. However, it was suggested that a consent requirement may produce biases, distort incidence data and make data unreliable for public health monitoring and cancer control purposes. Other options include notifying cancer patients of the possible use of medical records for cancer registration and research purposes or removing the name of the patient from the specimen before it is forwarded to the cancer registry.

99. The Committee weighed these options. It considers that individuals should be made aware that details of their condition may be made available to cancer registries and that identifiable data may be passed on to external researchers. The Committee favours the primary collector (that is, the general practitioner or the hospital admissions department) informing the patient verbally that details may be forwarded to a cancer registry and to the Institute and may ultimately be used for research purposes.

100. The Committee further considers that cancer patients should be informed in writing that details will be forwarded to a registry and the Institute and may be used for research. This written notification should be forwarded within a week of the verbal notification. The reason for forwarding written notification to the patient (after the initial verbal notification) is to detach notification from the time of treatment (or diagnosis) when the patient may be distressed and therefore less likely to fully comprehend the information.

101. There are obviously many details involved in implementing such an initiative. The Committee recommends that options for ensuring patients are notified that identifiable data may be disclosed to cancer registries, the Institute and external researchers should be pursued by the Australian Health Ministers Advisory Committee and the Australian Association of Cancer Registries. The Committee also considers that public education programs should be conducted which will alert the general public to the practice of forwarding certain information to state registries, the AIHW and external researchers.

Recommendation 36
The Committee recommends that the Australian Health Ministers Advisory Committee and the Australian Association of Cancer Registries jointly explore options and implement measures which will ensure patients are notified, verbally and in writing, that identifiable data concerning their condition may be forwarded to cancer registries, the Australian Institute of Health and Welfare and may be released to external researchers. (p. 159)

Recommendation 37
The Committee further recommends that public education programs be conducted to inform the public that certain confidential personal information may be forwarded to registries and the Australian Institute of Health and Welfare, and released to external researchers. (p. 160)

102. The Committee's recommendations focus on notifying individuals in relation to the possible use of personal information for cancer research and statistics as this was the focus of the evidence received by the Committee. The Committee also considers that where personal medical information, relating to medical conditions other than cancer, is used for purposes other than that for which it was collected, measures for notifying individuals of these practices should also be explored. Public education campaigns may also be useful in this respect.

The need for a national privacy code (Chapter 10)

103. Evidence given to the Committee during the inquiry raised the problem of the protection of confidential third party information which is not subject to the Privacy Act. While the terms of reference did not require the Committee to consider this issue, it was difficult to avoid in an environment in which confidential third party information collected by the Commonwealth may not be subject to the Privacy Act or any other Commonwealth protection. This situation can arise in several ways. The Privacy Act itself has limited jurisdictional scope. It does not apply to the private sector, other than to credit reporting organisations. Nor does it apply to state and territory governments. It does not apply to some Commonwealth business enterprises.

104. Further, information collected by the Commonwealth is not necessarily held only by the Commonwealth. Technological advances permit information collected by the Commonwealth to be accessed and manipulated by the non-government sector in increasingly sophisticated ways. Contracting out by agencies has a weakening effect on the Privacy Act. Privatisation is another factor which weakens the Privacy Act. Dealings between Commonwealth and territory and state agencies means that confidential information collected under the safety of the Commonwealth Privacy Act is no longer subject to the same protections when it is in the hands non-Commonwealth government agencies. In addition many functions which involve large amounts of sensitive third party information which were once the exclusive preserve of government are now performed by commercial enterprises.

105. Telecom is an example of a Government Business Enterprise which hold large quantities of third party information which does not have the protection of the Privacy Act. The circumstances of the 'bugging' of some of the Casualties of Telecom (COT) cases demonstrate the problem of protecting information held by utilities which were once Commonwealth departments. In the Committee's view the protections provided by the Information Privacy Principles should be extended to all confidential third party information by way of a national privacy code.

Recommendation 38
The Committee recommends that the protections provided by the Information Privacy Principles should be extended to all confidential third party information by way of a national privacy code. (p. 173)

106. As this proposal would have wide coverage in the Australian community, including application in state and territory government operations, it is desirable to have the proposal considered in the forum of the Council of Australian Governments.

Recommendation 39
The Committee recommends that the proposal for a national privacy code be placed on the agenda, for the earliest possible meeting of the Council of Australian Governments. (p. 173)

Afterword (Chapter 11)

107. Since the conclusion of formal evidence taking for this inquiry, several matters have arisen which relate to the issues covered in the report. It is useful to consider them and to comment on them because they are illustrative of the problems identified in the report.

108. These recent matters support the Committee's findings of a weak privacy ethos in Commonwealth agencies. Some of them involve the unauthorised disclosure of computer held information on a large scale. This underlines the Committee's comments about the need for care because computer held information creates the opportunity for disclosure and manipulation of a large volume of information.

109. The recent matters lend weight to the Committee's argument that administrative and criminal sanctions are needed as a deterrent to others considering engaging in such behaviour. Finally, the increase in computer matching activity by the private sector through the growing use of affinity purchasing programs, exposes individuals to a higher likelihood of having their personal information used by public and private sector organisations for profiling and direct marketing. This highlights the need for a uniform approach to privacy standards and for a national privacy code.

Chapter 1

Introduction

The inquiry commenced in the last Parliament (having been referred in August 1992) and was re-referred in the present Parliament in 1993. The impetus for the inquiry was concern about the effectiveness of the protection of confidential information held by the Commonwealth - concerns raised by the Privacy Commissioner and others. The application of the criminal law to illegal disclosure of information is considered.

The inquiry focuses on the need to find a balance between competing legitimate interests. Open government, public utility and efficient administration and the protection of privacy must all be accommodated. While most evidence related to personal information, the principles of information protection are the same and the recommendations in the report apply to both personal and commercial information.

The report covers Commonwealth government departments and their agencies, government business enterprises and other agencies which hold information originally collected by the Commonwealth, even though they are not Commonwealth agencies. The report also considers the protection of information collected by the private sector.

The report follows the order of the terms of reference except that references to the ICAC inquiry appear where relevant, rather than in a separate section.

1.1 The inquiry process

1.1.1 The House of Representatives Standing Committee on Legal and Constitutional Affairs in the last parliament[1] commenced its inquiry into the adequacy of the existing protections for confidential personal and commercial information held by the Commonwealth Government and its agencies, on 1 August 1992 at the request of the then Attorney-General, the Hon Michael Duffy, MP. Two days after the inquiry was advertised, the New South Wales Independent Commission Against Corruption (ICAC) published the *Report on unauthorised release of government information*.[2] On 21 August 1992 Mr Duffy asked the Committee, as part of its inquiry, to also examine the findings of the ICAC investigation and to report on the implications of these findings for information handling practices in Commonwealth administration.

1 The last parliament was the 36th parliament from March 1990 to February 1993.

2 Independent Commission Against Corruption, *Report on unauthorised release of government information*, August 1992, Sydney.

1.1.2 The terms of reference for the inquiry were advertised in August 1992 in the national press. Invitations to provide submissions were sent to civil liberties organisations, state privacy committees, community and consumer organisations, business associations, state law societies, state premiers and territory chief ministers, state and territory law reform agencies, Commonwealth departments and agencies, financial institutions and other interested persons. Submissions were received, and oral evidence was taken during public hearings.

1.1.3 The Committee made available to interested parties the submissions authorised for publication and the transcripts of evidence from the public hearings. Some evidence was taken in camera about the illegal disclosure of confidential information by employees in the Department of Social Security, Australia Post and the Health Insurance Commission.

1.1.4 Although the Committee received evidence in the 36th Parliament, it was not able to complete its inquiry during that term. On 28 May 1993, following the establishment of the Committee in the 37th Parliament[3] the Attorney-General, the Hon Michael Lavarch, MP referred the inquiry again to the Committee. By then the membership of the Committee had changed considerably, and by the end of the inquiry only three members remained from the original group who made up the Committee at the commencement of the inquiry.

1.1.5 The Committee reviewed the evidence that had been received in the previous parliament, and again invited interested persons and organisations to make submissions to the inquiry. The Committee also held further public hearings. In total one hundred and nine submissions and forty exhibits[4] were received from individuals and organisations including civil liberties and consumer organisations, law societies, academics, financial institutions and Commonwealth departments and agencies. Oral evidence was taken from more than 70 persons during public hearings in Canberra, Sydney and Melbourne.[5]

1.1.6 During the 37th Parliament, the Committee undertook a new course of inquiry into Bills before the Parliament – as well as inquiries into other matters referred by Ministers. The contracted timeframe for Bills inquiries meant the Committee had at times to redirect its resources and energies away from this inquiry into confidential third party information to meet the more immediate demands of Bills inquiries. The result has been

---

3 The present parliament commenced on March 1993.

4 A list of individuals and organisations who made submissions is at Appendix A, and a list of exhibits is at Appendix B.

5 A list of witnesses who appeared at public hearings is at Appendix C.

that the Committee completed four substantive reports on Bills in 10 months, and work on this inquiry was delayed accordingly to support the passage of important legislation.

1.1.7 Nevertheless, the Committee has been at pains to complete this inquiry because of the importance of the issues it raises in the proper functioning of government. Over the course of the inquiry, members of the Committee have spoken in public forums on the subject of the inquiry. The Committee notes there was also some discussion about and reference to the inquiry on television and radio programs throughout this time and formed the impression that there was widespread knowledge within the community of the Committee's inquiry into confidential information.

1.2 Background to the inquiry

1.2.1 The inquiry arose from concerns about the protection from disclosure of confidential third party information. These concerns included the effectiveness of the administrative measures and system security practices implemented by Commonwealth Government agencies. Related to this is the need to establish effective deterrents against individuals attempting to procure confidential information through improper disclosure by government employees, and to ensure there are appropriate penalties to be used against government employees who unlawfully disclose such information.

1.2.2 A number of these issues had been raised by the Privacy Commissioner shortly after the introduction of the *Privacy Act 1988*. The Privacy Commissioner's concerns were subsequently supported by the findings of the New South Wales ICAC that Commonwealth employees had released, exchanged and, in some instances, sold confidential information.[6]

1.2.3 In his first annual report on the operation of the Privacy Act, the Privacy Commissioner highlighted shortcomings in the protection of information. He raised the matter of the unauthorised disclosure of confidential information by Commonwealth employees.[7] The Privacy Commissioner considered that more effective deterrents were needed against those who procured the illegal release of confidential information, as well as those employees who released such data. The Privacy Act sets out some Information

---

6 Independent Commission against Corruption. *Report on Unauthorised Release of Government Information*, August 1992, p. 96.

7 Privacy Commissioner. *First Annual Report on the Operation of the Privacy Act. For the period 1 January 1989 to 30 June 1989*, pp. 27–29.

Privacy Principles for data protection, however, breaches of these principles are not subject to criminal sanctions.

1.2.4 In his first annual report, the Privacy Commissioner recommended that the criminal law be amended to enable the prosecution of parties involved in illegal disclosure.

1.2.5 The Privacy Commissioner was also concerned that a Commonwealth employee could improperly disclose confidential information held by a Commonwealth department and, provided the relevant department could demonstrate that all reasonable measures consistent with the security standards set down in Information Privacy Principles 4 and 11 had been taken to avoid improper disclosure by employees, little could be done by way of remedy for an injured party under the Privacy Act.

1.2.6 These matters were again taken up by the Privacy Commissioner in his second annual report, together with comments on the inadequacy of the existing range of disciplinary provisions in the *Public Service Act 1922* relating to improper disclosure of confidential information.[8]

1.2.7 The Senate Standing Committee on Legal and Constitutional Affairs considered the matters raised by the Privacy Commissioner. In June 1991 that Committee reported to the Senate its conclusion that the procurement and illegal disclosure of confidential information was potentially an increasing problem in the absence of effective legal and administrative deterrents.[9]

1.2.8 The criminal law as to the disclosure or use of Commonwealth government information is located in a wide range of Commonwealth legislation. These include several provisions in the *Crimes Act 1914*, for example, section 70 and subsection 79(3) which refer to the disclosure of information by Commonwealth officers. There are also many other secrecy provisions in other Commonwealth legislation.

1.2.9 The final report of the *Review of Commonwealth Criminal Law*, chaired by Sir Harry Gibbs, considered the criminal law in respect of disclosure of official information. The Gibbs Committee considered that it was undesirable to apply generally criminal law

---

8 Privacy Commissioner: Human Rights Australia, *Second Annual Report on the Operation of the Privacy Act*, For the period 1 July 1989 to 30 June 1990, pp. 14–16.

9 Senate Standing Committee on Legal and Constitutional Affairs. *Unauthorised Procurement and Disclosure of Information*, June 1991, p. 9.

sanctions to all unauthorised disclosures of confidential information.[10] If adopted, the outcome of this recommendation would be to remove the existing protection provided to confidential personal information under section 70 of the Crimes Act.

1.2.10 The Gibbs Committee considered that the protection of confidential personal and commercial information should be dealt with instead by specialised legislation such as the Privacy Act[11] and, if necessary, by extending the secrecy provisions of specific statutes such as the *Income Tax Assessment Act 1936* and the *Social Security Act 1991.*[12]

1.3 Scope of the inquiry

1.3.1 The main aspect of the inquiry is to determine what is an appropriate balance between competing interests in dealing with confidential personal and commercial information held by the Commonwealth. In considering and answering this question, the Committee has sought to recognise and to acknowledge the legitimacy of each of the competing interests. The inquiry process has led to the identification of the competing interests of open government, public utility and efficient administration and the protection of privacy.

1.3.2 The evidence to the Committee focussed on confidential personal information to a far greater extent than confidential commercial information. So while the illustrative examples the Committee draws on throughout the report will necessarily reflect this focus on confidential personal information, the Committee considers that the same principles should apply to confidential third party information held by the Commonwealth regardless of its character as personal or commercial. Consequently, the recommendations of the Committee apply equally to all confidential third party information held by the Commonwealth Government and its agencies.

1.3.3 The Committee observes, without drawing any inference from, the fact that the inquiry did not draw out significant evidence comparable to that given to the New South Wales ICAC inquiry by 'whistleblowers' regarding cases in which information had been wilfully provided in breach of confidentiality.

1.3.4 The Committee found it was not useful to provide an exhaustive definition of the expression 'Commonwealth Government and its agencies'. While the expression obviously

---

10 Review of Commonwealth Criminal Law. *Final Report December 1991*, p. 233.

11 ibid., p. 321.

12 ibid., p. 319.

includes federal public service departments, it would also seem appropriate to include organisations like Australia Post and Telecom, about whom the New South Wales ICAC made comments. It should be noted that during the course of the inquiry the status of Telecom changed and it is no longer subject to the *Privacy Act 1988*, although certain of its operations are subject to the *Freedom of Information Act 1982*. It would not have been appropriate for the Committee to overlook Telecom in conducting the inquiry because of this change of circumstance. Consequently the Committee did not limit the scope of the inquiry by expressly excluding agencies on the basis of the directness of their links with the Commonwealth, where evidence was provided about their activities. The Committee has made conclusions and recommendations which will impact on both Commonwealth government departments and agencies holding information collected by government, even where the agency itself is not a Commonwealth agency. The issue of protection of privacy in relation to information held by the private sector is also considered.

1.3.5 While the individual terms of reference are interrelated they focus on specific aspects of dealing with confidential information and have been addressed in the report in the order suggested by the terms of reference. The findings of the New South Wales ICAC investigation into the unauthorised release of government information are not treated in the report as a separate topic for discussion, but are referred to throughout the report where they may illuminate the main focus of the inquiry.

1.3.6 The report commences with a brief introduction to some of the issues that arise in relation to the Commonwealth having confidential third party information (chapter 1) and then outlines the existing measures for providing protection to such confidential information (chapter 2). A more detailed examination of the protections follows.

1.3.7 First, there is an assessment of the adequacy of existing administrative measures for safeguarding third party information held by government agencies, and the need to ensure the responsibility of senior managers for these matters (chapter 3). Next, there is an examination of the effect which the existing legal safeguards for third party information may have in inhibiting the legitimate transfer of information between government agencies (chapter 4).

1.3.8 The report then provides a review of the adequacy of the penalties and administrative sanctions applicable to officials who wrongly disclose third party information (chapter 5), and of the adequacy of the existing penalties applicable to persons who procure the wrongful disclosure of information (chapter 6). This leads to a discussion of the application of the criminal law (chapter 7).

1.3.9 The report also considers the effectiveness of existing civil and statutory remedies and the need for compensation for third parties where information about them has been wrongly disclosed (chapter 8). Then the report examines the appropriateness of the legislative and administrative provisions which govern access to third party information (chapter 9). Finally, the report discusses the need for a national privacy code (chapter 10), and briefly reflects on several matters which have arisen since the Committee concluded its evidence taking (chapter 11).

1.4 Some issues that arise when dealing with confidential third party information

1.4.1 There is a need for third party information to be collected, used and held by a government in order for it to be able to make informed decisions and to perform its functions effectively and efficiently. The government holds a large and seemingly increasing amount of confidential personal and commercial information. In a practical sense, this information is obtained so that voters can be enrolled, benefit recipients can be paid, grants can be allocated, taxes can be collected, persons can travel overseas, the law can be enforced and the defence forces can operate.

1.4.2 The government has competing statutory rights and responsibilities to use, protect and disclose such information. Persons obliged to provide the information and to whom the information relates, may have expectations that the information will be used only for the purpose for which it was provided and seen only by those with an official need to know. The government has a responsibility to deal with the information provided in a way that also respects the interest of the individuals. Individuals have a direct interest in its use and disclosure. There is an apparent tension between the interests of the government in accessing information for a certain official purpose, and in safeguarding information from unauthorised access.

1.4.3 Modern technology has made access to and collection of large volumes of information relatively simple. It has become increasingly apparent since the New South Wales ICAC investigation that there is a market for confidential third party information held by the Commonwealth Government. It is also apparent that some unauthorised release of confidential information has occurred and that such third party information held by the government has been sold, otherwise deliberately released, or carelessly released.

1.4.4 ICAC found that some Commonwealth officers have improperly provided information and received illicit payments. Other well intentioned officers were members

of an 'information exchange club' and they improperly provided information, without payment, to Commonwealth and state agencies. ICAC found that some of this information nevertheless also found its way to the illicit market.

1.4.5 Furthermore, it has come to public attention that some officials have accessed confidential personal and commercial information because of what appears to be idle curiosity, or at least without an official need to know. No matter what the purpose, these unauthorised accesses are cause for concern because, among other things, they are indicative of a lack of regard for the privacy and economic interests of individuals and businesses.

1.4.6 In the first instance it is necessary to review the existing legal and administrative measures that provide access and protection to confidential third party information held by Commonwealth agencies, to determine where improvements can best be made to those measures.

Chapter 2

Description of administrative and legal measures

Legal measures that provide access and protection to third parties are found in common law and statute law. Some apply to agencies generally including the administrative law mechanisms laid down in the Freedom of Information Act 1982 (FOI Act), the Archives Act 1983 and the Privacy Act 1988 – including legally binding guidelines issued by the Privacy Commissioner. Other measures with general application include the general law of confidence – including its extension by the Privacy Act and the Public Service Act 1922 and Public Service Regulations in force under the Public Service Act.

Other legal measures apply only to specific agencies such as legally binding guidelines issued by the Privacy Commissioner which apply only to those parties taking part in specific programs of activity. Numerous secrecy provisions in specific Commonwealth legislation which apply only to the agencies provided for under those Acts.

Administrative measures include guidelines and training programs issued by the Public Service Commission.

2.1 Introduction

2.1.1 The Attorney-General's Department advised the Committee that there was a range of administrative and legal measures that provide access to and protection of confidential third party information.[13] Administrative measures include:

- guidelines and training programs provided by the Public Service Commission;
- voluntary guidelines issued by the Privacy Commissioner;
- information handling practices in the Attorney-General's Department's *Protective Security Manual* (PSM); and
- local guidelines, instructions and training programs provided by individual agencies.

2.1.2 Legal measures are found in both the common law and statute law. Some legal measures apply to agencies generally:

- the administrative law mechanisms laid down in the *Freedom of Information Act 1982* (FOI Act), the *Archives Act 1983* and the *Privacy Act 1988*;
- the general law of confidence – including as extended by the Privacy Act;
- general secrecy provisions in the *Crimes Act 1914*; and

13 Attorney-General's Department, *Submissions*, p. S353.

- the *Public Service Act 1922* and *Public Service Regulations* in force under the Public Service Act.

2.1.3 Other legal measures which apply only to specific agencies include:

- legally binding guidelines issued by the Privacy Commissioner apply only to those parties taking part in specific programs of activity; and
- numerous secrecy provisions in specific Commonwealth legislation apply only to the agencies provided for under those Acts.

2.1.4 The brief survey of administrative and legal measures that follows highlights the competing nature of the interests of the Commonwealth Government in holding and dealing with confidential personal and commercial information. Clearly, the primary purpose of an individual Act may sometimes be at odds with the primary purpose of another Act. For example, the FOI Act generally encourages the disclosure of government held information, but provides for exceptions to protect certain information from disclosure. On the other hand, the Privacy Act generally protects information from disclosure, but provides for exemptions to permit the disclosure of certain information in certain circumstances.

2.2 *Public Service Act 1922*

2.2.1 The *Public Service Act 1922* is administered by the Prime Minister.[14] It provides the legal framework for the public sector which may deal with confidential personal and commercial information. The Public Service Act and the Public Service Regulations, made under that Act, contain the primary duties of public servants. Most officials who handle third party information are subject to the Public Service Act. The Federal Government recently responded to the *Report of the Public Service Act Review Group* which was tabled in December 1994.[15] The Government agreed with most of the recommendations of the review including the recommendation that the existing Act should be replaced with a more modern Act which was more suited to the realities of the public service.[16]

---

14 The Public Service Act is currently the responsibility of the Hon Gary Johns, the Minister Assisting the Prime Minister on Public Service Matters.

15 *Report of the Public Service Act Review Group*, December 1994, AGPS Canberra.

16 Hon Gary Johns MP, Minister Assisting the Prime Minister for Public Service Matters, *Media Release*, 'Review of the Public Service Act', 4 May 1995.

2.2.2 The head of a department plays a pivotal role in relation to the protection of sensitive information. Although there is no specific legislative provision in relation to the protection of sensitive information, the head of an agency is accountable under section 25(2) of the Public Service Act:

> 25.(2) The Secretary of a Department shall, under the Minister, be responsible for its general working, and for all business thereof, and shall advise the Minister in all matters relating to the Department.

Responsibility for developing an agency's practices is therefore in the hands of its most senior manager.

2.2.3 The Act extends the provisions relating to secretaries, to office holders under other Acts where they have or exercise the powers of a secretary.[17] Subsection 25(4) of the Act provides the Auditor-General and the Commissioner of Taxation with all the powers of a secretary. Although the Act refers to 'Secretary' and 'Department', in practice, heads of agencies are usually given the same powers and responsibilities as a secretary under the agency's enabling legislation.[18]

2.2.4 Although the Public Service Act does not expressly require the development of guidelines or standards, guidelines are anticipated under the Public Service Regulations. The Public Service Regulations are legally binding on all officers. Two of the most important Regulations are 8A and 35. Regulation 8A requires public servants to meet set standards of performance and comply with official guidelines, directions and recommendations. They are also required to treat members of the public with sensitivity to their rights and to not take improper advantage of any official information or document to which they have access as a consequence of their employment:

> **8A.** An officer shall:
> (a) perform with skill, care, diligence and impartiality the duties of his or her office, or any other office whose duties he or she is directed to perform, to the best of his or her ability;
> (b) comply with any enactments, regulations, determinations, awards or departmental instructions applicable to the performance of his or her duties;
> (c) comply with any lawful and reasonable direction given by a person having authority to give the direction;
> (d) have regard to any official guidelines or recommendations applicable to the performance of his or her duties;
> (e) in the course of his or her duties treat members of the public and other officers with courtesy and sensitivity to their rights, duties and aspirations;

---

17 Public Service Act, section 25(4C).

18 For a comprehensive list of agencies staffed under the *Public Service Act 1922*, refer to *Report of the Public Service Act Review Group*, December 1994, Canberra, Australian Government Publishing Service, Appendix 3 at p. 147.

> (f) provide reasonable assistance to members of the public in their dealings with the Service and help them understand their entitlements and any requirements with which they are obliged to comply;
> (g) avoid waste, or extravagance in the use, of public resources;
> (h) not take, or seek to take, improper advantage, in the interests, pecuniary or otherwise, of the officer, any other person or any group, of any official information acquired, or any document to which he or she has access, as a consequence of his or her employment; and
> (i) at all times behave in a manner that maintains or enhances the reputation of the Service.[19]

2.2.5 Regulation 35 provides that an officer is obliged to fulfil duties[20] and is not to disclose information obtained in the course of official duties unless authorised to do so:

> 35. Except in the course of official duty, no information concerning public business or any matter of which an officer or employee has knowledge officially shall be given, directly or indirectly, nor shall the contents of official papers be disclosed, by an officer or employee without the express authority of the Secretary.[21]

Accordingly, official guidelines may be developed for the operations of an individual agency that will not apply to other agencies.

2.2.6 Should a breach of regulations occur the officer would be liable to action under the APS disciplinary provisions in the Public Service Act. An officer who fails to fulfil her or his official duties may be charged with misconduct. If misconduct is proven, the officer will be subject to disciplinary action including admonishing the officer, reducing salary, transfer, dismissal, or a combination of these sanctions.[22] It is possible to take disciplinary action under the Public Service Act together with criminal charges. For example an official's behaviour might be in breach of the Crimes Act or of provisions in the appropriate agency specific legislation.[23]

2.2.7 Mr Edmund Attridge, Acting Deputy Commissioner of the Public Service Commission (PSC), told the Committee that the PSC is a policy making body which has policy responsibilities in relation to setting the framework for staff in the Australian Public Service (APS).[24] It has developed general standards for the guidance of officers in carrying out their duties that were drafted in recognition of the Privacy Act and the Information Privacy Principles. These general standards include *Guidelines on Official*

---

19 *Public Service Regulation 8A.*
20 Section 56 of *Public Service Act 1922.*
21 *Public Service Regulation 35.*
22 Subsection 62(6).
23 PSC, *Submissions*, p. S541.
24 *Transcript*, p. 195.

Conduct of Public Servants[25] and *Guidelines on the Keeping of, and Access to, Personal Records.*[26] They set out principles relating to the collection and storage of personal information, rights of access by staff to their own records and disclosure of such records to third parties.

2.2.8 The guidelines are not binding on agencies and will apply if an agency expressly adopts them. The voluntary nature of the guidelines gives effect to the principle that the responsibility for managing APS staff and their conduct, including their conduct in relation to the protection of confidential third party information, rests largely with individual agencies through the role of the agency head.

2.3 The *Protective Security Manual*

2.3.1 The *Protective Security Manual* (PSM) is not binding on agencies. It was issued by the Attorney-General's Department following consultation with the Privacy Commissioner and a number of other Commonwealth agencies. The PSM contains administrative policies, standards of practice, principles and common procedures for the protection of official information. It was developed in full realisation of the need to balance competing interests in dealing with third party information:

> It is the firm view of the Government that people should have access to information held by or on behalf of the Government unless there are good reasons to the contrary. Such reasons for non-disclosure include the need to protect national security, the national interest and the private affairs of individuals and organisations.[27]

2.3.2 The voluntary nature of the PSM recognises the principle that responsibility for managing APS staff and their conduct rests largely with individual agencies and their heads. The PSM provides a basis from which agencies may develop protective security policies and practices in relation to information held by them. For example, paragraphs 3.64 and 3.65 state:

> Agencies should take all reasonable and appropriate precautions to see that only people with a 'need-to-know' and the appropriate security clearance gain access to classified material. A person has a genuine 'need to know' if, without access, s/he would be hindered in the proper or efficient performance of her/his duties. Officers are not entitled to access

---

25 *Transcript*, p. 195.

26 Public Service Commission, *Submissions*, p. S540.

27 Attorney-General's Foreword to the PSM, p. iii, as extracted in Attorney-General's Department, *Submissions*, p. S367.

> merely because it would be convenient for them to know or by virtue of their status, rank, office or level of authorised access.
>
> Where classified material covers a number of subjects, agencies should consider the possibility of producing it in sections so that all the material need not be distributed to those concerned with only part of it.

2.3.3 The PSM suggests two broad categories for classified material: national security material and sensitive material. Sensitive material includes material which the unauthorised disclosure, loss, compromise, misuse of, or damage to, would reasonably be expected to:

- cause serious harm to any person, or organisation which provided information to the Commonwealth under an assurance or expectation of confidentiality, or about which the Commonwealth holds information;
- breach a statutory requirement to protect that material; or
- give unfair advantage to any entity.[28]

The PSM also provides for three main classifications to be applied to material according to its level of sensitivity: 'in confidence', 'protected' and 'highly protected'. Privacy information which requires some degree of protection is usually classified as 'in confidence' material.

2.3.4 The PSM sets out standards for: the physical protection of all types of classified material; assessing the suitability of staff to have access to classified or sensitive information; and procedures for protecting and handling such material when it is stored on, manipulated by and transmitted via computers, and when passed over other telecommunications systems such as facsimiles and telephones.

2.3.5 Although the PSM is not binding, the Attorney-General's Department considers it to be 'a guide for best practice in protecting the security of information held by the Government.'[29] The Attorney-General's Department provides training to support the information set out in the PSM.

2.3.6 The principles of ethical conduct and privacy are also provided for in the administrative law regime that is found primarily in Commonwealth statutes.

---

28 Paragraph 3.4 of the PSM as extracted in Attorney-General's Department, *Submissions*, p. S426.

29 Attorney-General's Department, *Submissions*, p. S367–S369.

2.4 *Freedom of Information Act 1982*

2.4.1 The *Freedom of Information Act 1982* (FOI Act) is administered by the Attorney-General. It regulates the authorised disclosure of information held by the Commonwealth Government and provides a general right of access to documents held by the government, subject to several specified exemptions. It is a means to paragraph 3(1)(b) of the FOI Act states that the general right of access to government information should be:

> limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom [the] information is collected and held . . . .

2.4.2 The purpose of the exemptions is to balance the objective of providing access to government information against legitimate claims for the protection of sensitive material.[30] There are 19 exemptions in Part IV of the FOI Act.[31] Importantly for the purposes of this inquiry, exemptions apply to:

- documents protected by secrecy provisions[32];
- documents affecting personal privacy[33];
- documents relating to business affairs[34]; and
- documents containing material obtained in confidence[35].

2.4.3 The FOI Act requires that a request for access must be in writing and must contain information that will enable the identification of the document.[36] An agency is obliged to take reasonable steps to assist an applicant to make the request in a manner that complies with the Act. The FOI Act also contains consultative mechanisms designed to ensure that documents containing third party information will usually not be released unless the third party has been consulted about its release[37], and has been provided with an opportunity to seek a review of a decision to release information.[38]

---

30 ALRC & ARC, *Freedom of information*, Issues Paper 12, ALRC IP 12, September 1994, p. 31.

31 ALRC IP 12, p. 32.

32 FOI Act, section 38 and Schedule 3.

33 FOI Act, section 41.

34 FOI Act, section 43.

35 FOI Act, subsection 45(1).

36 FOI Act, subsection 15(2).

37 FOI Act, sections 27 and 27A.

38 FOI Act, sections 59 and 59A.

2.5 *Archives Act 1983*

2.5.1 The *Archives Act 1983* is administered by the Minister for Communications and the Arts, and was developed in conjunction with the FOI Act. It regulates public access to non-current Commonwealth government records and the management of current Commonwealth government records. It established the Australian Archives to conserve and preserve Commonwealth archival records, which must be available for public access under established procedures, consultations and safeguards.

2.5.2 The Archives Act provides for all records over 30 years old – and thereby 'in the open access period'[39] – and which are not exempt [40], to be made available for public access. Australian Archives may grant partial access to an exempt record where such access could be given without disclosing the information or matter which rendered the record exempt.[41]

2.5.3 The Archives Act contains a number of exemptions that are relevant to the protection of third party information:

- information or matter the disclosure of which would constitute a breach of confidence;
- information or matter the disclosure of which would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person);
- information or matter relating to trade secrets, or any other information or matter having a commercial value that may be destroyed or diminished if the information or matter were disclosed; and
- information or matter concerning a person in respect of her/his business or professional affairs or concerning the business, commercial or financial affairs of an organisation or undertaking, being information or matter the disclosure of which may unreasonably affect that person or organisation adversely.[42]

2.5.4 The exemptions and appeal provisions in the FOI Act and the Privacy Act are similar. The exemption categories differ because of the reduced sensitivity of the older documents being accessed under the Archives Act.[43]

---

39 Archives Act, section 3.

40 Archives Act, section 31.

41 Archives Act, section 38.

42 Archives Act, section 33.

43 ALRC IP 12, p. 9.

2.6 *Privacy Act 1988*

2.6.1 The Privacy Act is administered by the Attorney-General. It establishes a scheme to govern the collection, storage, security, access, use and disclosure of personal information by Commonwealth agencies including the transfer of information between government agencies. The Privacy Act is not restricted to confidential information, however it applies only to a natural person and not to a corporation:

> 'personal information' means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[44]

2.6.2 The Privacy Act imposes rules for the handling of personal information called Information Privacy Principles (IPPs)[45] and requires agencies not to breach the IPPs[46]. The Privacy Act does not prevent the disclosure of information if disclosure is required in certain circumstances, including under the FOI Act.

2.6.3 The IPPs are based on the guidelines adopted by the Council of the Organisation for Economic Co-operation and Development in 1980.[47] The 11 IPPs govern:

- collection of information (1–3);
- storage of information and access to it (4–7);
- accuracy and use of information (8–9); and
- limits on use and disclosure (10–11).[48]

2.6.4 The Privacy Commissioner has stated that for the purposes of this inquiry, the most important IPPs are numbers 4, 10 and 11[49]:

- IPP 4 requires an agency to maintain reasonable security safeguards in relation to the storage and dissemination of personal information. This means not only devising and stating standards but also encouraging officers of an agency to behave in appropriate ways.[50]

---

44 Privacy Act, section 6(1).

45 Privacy Act, section 14.

46 Privacy Act, section 16.

47 *First Annual Report on the Operation of the Privacy Act*, For the period 1 January 1989 to 30 June 1989, Sydney, p. 14.

48 Section 14 of the Privacy Act, which sets out the Information Privacy Principles, is extracted at Appendix D.

49 Privacy Commissioner, *Submissions*, p. S555.

50 Attorney-General's Department, *Submissions*, pp. S377–S378.

- IPP 10 limits an agency's use of personal information with prescribed exceptions; and
- IPP 11 limits an agency's disclosure of personal information, with prescribed exceptions.

2.6.5 The Privacy Act also contains provisions relating to the protection of tax file number information[51] and to regulate the credit reporting industry[52]. These rules apply to both private and public sector organisations, including commercially competitive enterprises.

2.6.6 A Privacy Commissioner is appointed under the Privacy Act.[53] The Privacy Commissioner provides advice to agencies concerning their responsibilities under the Act, and has powers to conduct privacy based audits of agencies[54] and to investigate individual complaints[55]. The Privacy Commissioner may then make a determination declaring that an agency should alter its practices, an amount of compensation or reimbursement should be paid or that no further action is necessary.[56]

2.6.7 The Privacy Commissioner has the power to issue guidelines which are legally binding and guidelines for voluntary compliance. He has issued legally binding guidelines on the use of personal information for medical research conducted by third party researchers, matching agencies involved in data-matching, the use of tax file numbers for data-matching between government assistance agencies and the Australian Taxation Office, and the handling of personal information by credit reporting agencies and credit providers. The Privacy Commissioner has also issued voluntary guidelines which apply to handling information on spent convictions, HIV information, data-matching – which apply to a wider range of agencies and programs than the legally binding guidelines, deciding whether to undertake covert optical surveillance of individuals, and assist members of parliament to obtain personal information from government departments on behalf of their constituents.

2.6.8 The Privacy Act provides for the Privacy Commissioner to transfer a complaint to the Human Rights and Equal Opportunity Commission, the Commonwealth Ombudsman

---

51 Privacy Act, sections 17 and 28.

52 Part IIIA.

53 Privacy Act, section 19.

54 Privacy Act, section 27.

55 Privacy Act, section 36.

56 Privacy Act, section 52.

or the Merit Protection Agency in certain circumstances.[57] Such a transfer shall be made where a complaint could have been made to one of those offices and could be more conveniently or effectively dealt with by that particular office. A complaint so transferred, shall be taken to be a complaint made under the appropriate Act.[58]

2.6.9 Apart from the statutes in the administrative law area, other Acts and the common law affect access to and protection of confidential third party information.

2.7 *Data-matching Program (Assistance and Tax) Act 1990*

2.7.1 The *Data-matching Program (Assistance and Tax) Act 1990* is administered by the Minister for Social Security. It provides legal authority for a computer matching program which would otherwise be illegal.[59] The Data-matching Program Act contains specific controls for data-matching and extends the use of the tax file number (TFN) system to the government's payments and assistance schemes. The participating government agencies include the Australian Taxation Office (ATO), DSS, DEET, Department of Health and Human Service, and the Department of Veterans' Affairs. The TFN is used as the individual identifier for taxable income data held by the ATO and for unemployment benefits, family allowance, family allowance supplement, AUSTUDY, age and disability pensions etc.

2.7.2 DSS, the 'matching agency', receives data from the participating agencies or 'source agencies'. The Data-matching Program Act regulates the use of data-matching and prescribes a process for a data-matching cycle. The purposes of the matching programs are to detect persons who: are wrongly obtaining benefits from different assistance agencies; have incorrectly stated their income; and who have incorrectly stated their eligibility for tax rebates or deductions. Source agencies must destroy such information within 90 days of receipt unless there is a decision to investigate the need to take action. Action based on such information must commence within 12 months of receipt of that information.

---

57 Privacy Act, section 50.

58 One of the *Human Rights and Equal Opportunity Commission Act 1986*, the *Ombudsman Act 1976* or the *Merit Protection (Australian Government Employees) Act 1984*.

59 G. Greenleaf, 'Can the data matching epidemic be controlled?' (1991) 65 ALJ 220 at 221.

2.7.3 There is no special regulation of data-matching in the Privacy Act however, the Privacy Commissioner has a monitoring role over some data-matching activities. The Data-matching Program Act requires agencies to comply with guidelines issued by the Privacy Commissioner and set out in a schedule to the Act. The guidelines address the preparation of a program protocol by the matching agency covering the nature and purposes of the data-matching program. The clients of source agencies are to be informed such a protocol is available from the Privacy Commissioner.

2.7.4 As well as issuing guidelines, the Privacy Commissioner is to investigate breaches of the Data-matching Program Act or guidelines, advise agencies of their obligations under the Act, monitor and report on agencies' compliance with the Act and guidelines, and make available the program protocol.

2.8 General law of confidence

2.8.1 Principles of common law and equity apply to rights which are affected when third party information is used or disclosed. The law does not recognise a tort of violation of privacy although the courts will enforce a right of confidentiality.

2.8.2 The FOI Act and the Privacy Act support a duty of confidence.[60] A duty to maintain the confidentiality of third party information may arise in three ways. First, a duty may arise where confidentiality is an essential feature of a relationship – such as the relationship that exists between a doctor and patient. Second, parties to a contract may agree that certain information is to be kept confidential. Most importantly in the context of this inquiry, an equitable obligation of confidence will be imposed on the recipient of information in some cases because of the nature of the information and the circumstances of its disclosure.[61]

2.8.3 The Attorney-General's Department considers that the general principles governing breach of confidence apply to confidential information provided by a person or business to a government for a particular purpose. The Department considers that Professor Paul Finn, of the Australian National University, provides an authoritative summary of the general principles that would apply:

> A person who receives or acquires information in confidence cannot use or disclose that information for any purpose other than that for which it was received or acquired without

60 FOI Act, s 45. Privacy Act, ss 89–94. Privacy Act s 92 extends the common law duty.

61 Attorney-General's Department, *Submissions*, pp. S357–S358.

> the consent of the person or body from whom or on whose behalf it was received or acquired, unless that use or disclosure (a) is authorised or required by law; or (b) is justified in the public interest.[62]

2.8.4 These principles are modified in their application to information generated within government such that the Attorney-General's Department has explained that the law of confidence gives relatively more protection to third party information held by government than it does to government generated information. The Attorney-General's Department places emphasis on three aspects. The first aspect is that the obligations of secrecy which attach to confidential information may be transferred to others who receive that information. The second is that there is a wide range of remedies available in a breach of confidence action – including injunctions, damages for breach of contract, compensation for breach of an equitable duty of confidence and an account of profits. The third aspect is that the practical application of the law of confidence in Commonwealth matters is limited, because the obligation of confidence does not apply where the use or disclosure of information is authorised or required by law.[63]

2.9 Secrecy provisions in Commonwealth legislation

2.9.1 Secrecy provisions contained in various Acts also prohibit or restrict the disclosure of certain information by government officers. Secrecy provisions were originally developed to prevent the disclosure of sensitive information to the public.[64] They prohibit or restrict the disclosure of information by Ministers, Departments, statutory authorities and Commonwealth officers.[65] They also provide a guarantee of confidentiality to persons who provide information to the government.

2.9.2 General secrecy provisions are contained in the *Crimes Act 1914* which is administered by the Attorney-General. These provisions apply to the Commonwealth Government generally. The relevant provisions in the *Crimes Act 1914* are section 70 and subsection 79(3) which deal with the disclosure of information by Commonwealth officers; section 73 which deals with the corruption and bribery of Commonwealth officers and sections 76B and 76D which prohibit unlawful access to data in Commonwealth and other computers. (These provisions are discussed in more detail in chapter 5). Provisions in section 5 of the Crimes Act are also relevant.

---

62 As extracted at Attorney-General's Department, *Submissions*, p. S358.

63 Attorney-General's Department, *Submissions*, pp. S358–S359.

64 *Submissions*, p. S381.

65 See J. McGuiness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 9 *Federal Law Review* 49 cited in Attorney-General's Department, *Submissions*, p. S359.

2.9.3 There are more than 150 specific secrecy provisions in Commonwealth statutes, many of which are located in subordinate legislation.[66] These provisions generally protect personal and commercial information. Some of these provisions protect all information acquired by an officer in the performance of her or his duties. Other provisions are narrower in their effect. The provisions also vary in the exceptions and penalties. The provisions are not uniform and there is no consistent approach.

66 Refer Attorney-General's Department, *Submissions*, pp. S418–S423.

Chapter 3

Administrative safeguards and the accountability of senior managers

This chapter covers the first term of reference which relates to the adequacy of existing administrative measures and the responsibility of senior managers for implementing the measures.
The chapter considers examples of administrative arrangements including physical security controls, computer security controls, staff training, joint agency agreements on access, specific access procedures. The Committee notes that while the procedures described by agencies vary, this is a positive point because it shows flexibility in dealing with the varying responsibilities of agencies.

The role of senior managers in regard to the protection of third party information is considered. Secretaries and other heads should be given specific responsibility for the protection of third party information and caution should be exercised in delegating this responsibility. In exercising her or his responsibilities, an agency head should ensure that only necessary third party information is collected.

The chapter considers lapses of protection for third party information uncovered by ICAC and case studies are reviewed. These NSW case studies cannot be considered as isolated lapses. Insofar as they resulted from misunderstanding they indicate problems in public sector procedures and culture.

The chapter concludes with a review of concerns about administrative measures. The Committee concludes that inadequacies in administrative measures protecting third party information are more in the implementation than in the relevant policies.

3.1 Introduction

3.1.1 While the legislative framework provides the parameters within which Commonwealth agencies and officers must operate, within that legislative structure there are large numbers of administrative measures for safeguarding third party information held by government agencies. A descriptive overview of existing administrative measures can be found at 2.1.4 above. Best practice models addressing all areas of operations including the changing information environment, are developed for the public sector to guide the administrative practices and procedures of individual agencies.

3.1.2 Those administrative procedures which are service wide provide help in determining the effectiveness of existing protections for third party information. In recent years responsibility for matters such as personnel management has devolved to agency level, replacing the centralising role of the former Public Service Board. The principle

of 'letting managers manage' has not necessarily resulted in a wider variety of administrative practices as many agency heads are keen to take advantage of best practice approaches sponsored by the Public Service Commission (PSC). The role of senior managers is central to the adoption of administrative practices within agencies and is therefore the first issue that will be addressed.

3.2 Targeting the senior managers

3.2.1 The senior managers of an agency include the agency head (the secretary in departments) and the members of the senior executive service (SES). They are responsible for the general functioning of an agency. This group provides policy advice, and undertakes managerial and professional responsibilities.[67] In some agencies officers other than senior executive service officers will have an important managerial role. For the purposes of this inquiry however, the senior managers are the agency head and officers in the senior executive service, or equivalent.

3.2.2 Mr Edmund Attridge, Acting Deputy Commissioner of the PSC confirmed that responsibility for managing Australian Public Service (APS) staff and their conduct, including their conduct in relation to protection of third party information rests largely with departments and line agencies.[68] Senior managers are responsible for, among other things, protective security arrangements within Commonwealth agencies. This includes the development of guidelines or standards anticipated under the Public Service Regulations and security safeguards anticipated under Information Privacy Principle 4.

3.2.3 The PSC has focussed its attention, in its promotion of proper conduct within the public sector, on the SES. The PSC seeks to ensure the SES are providing leadership in respect of the protection of confidential information.[69] The PSC has written to all SES officers, providing information on the standard of conduct expected of public service officers, and encouraging them to promote awareness amongst their staff of that standard of conduct.[70]

3.2.4 The PSC conducts an orientation program for all officers appointed to the SES based on the PSC guidelines on official conduct. This orientation program is supported

---

67 S26AA(2) of the Public Service Act.

68 Mr Attridge, *Transcript*, p. 195.

69 Mr Attridge, *Transcript*, p. 200.

70 Mr Harding, *Transcript*, p. 205.

by subsequent SES development programs provided by the PSC which include sessions on official conduct and ethics.[71]

3.2.5 The PSC advised the Committee that although the courses and programs they provide are not compulsory, they are taken up by most officers when they join the SES. The PSC monitors the effectiveness of its promotion of proper conduct and ethics in the orientation and development programs by follow up with course participants.[72]

3.2.6 The Committee considers that it is important to disseminate widely, up to date information about expected standards of conduct and ethics in the public sector. The Committee notes and supports the role of the PSC in providing guidance to the SES on these matters. The Committee considers that the performance of such a function by the PSC will be important in helping to promote desirable conduct that is consistent throughout the many Commonwealth agencies.

3.3 Proposed statement of the responsibilities of agency heads

3.3.1 The Attorney-General's Department argued that the accountability of senior managers is one means of assuring that adequate security arrangements are practiced.[73] The Department suggested that the responsibilities of Commonwealth officers with access to sensitive information should be explicitly established within a legislative framework. The principal officer of an agency should be given an express duty to ensure the protection of third party information and should bear primary legal responsibility for its protection. Failure to observe this duty should give rise to the existing disciplinary sanctions. Mr Norman Raeburn, Deputy Secretary of the Attorney-General's Department argued that this approach would give greater certainty to a secretary's actions and give her or him greater authority.[74] The Department of Industrial Relations supported the Attorney-General's Department's arguments about these issues.[75]

3.3.2 The PSC was against the Attorney-General's Department's proposal.[76] Mr Richard Harding, Assistant Commissioner of the PSC said the rationale for this stance was that there is a general provision in the Public Service Act imposing responsibility on

---

71 Mr Gleeson, *Transcript*, p. 200.

72 Mr Gleeson, *Transcript*, p. 202.

73 Attorney-General's Department, *Submissions*, p. S379.

74 Mr Reaburn, *Transcript*, p. 183.

75 Department of Industrial Relations, *Submissions*, p. S705.

76 PSC, *Submissions*, p. S540.

the secretary. A departmental secretary is responsible for a wide range of matters, and it would not be appropriate to single out the management of confidential information from the range of other matters for particular mention under the Public Service Act.[77] The PSC regards the Privacy Act as imposing sufficient obligations on senior managers and departmental secretaries in this regard.[78]

3.3.3 Mr Kevin O'Connor, the Privacy Commissioner, was not convinced that the proposal of the Attorney-General's Department would necessarily lead to a more strict adherence to privacy standards.[79] He pointed out that chief administrators tended to be very busy and to delegate functions. Further, he considered that it was not necessary to impose personal liability on persons to get them to take security of information seriously.

3.3.4 The *Report of the Public Service Act Review Group* is also relevant to this issue.[80] It identified the need for a replacement Act, which should be streamlined and principles-based, in the interests of a more flexible public service framework suitable for the 1990s and the future. The Review Group recommended that the new Act have as its object that it 'defines the powers and responsibilities of the secretary of a department, and of the heads of other APS employing bodies'. At R108 the Review Group recommends that the new Act include:

> The secretary of a department shall:
> . . .
> - manage the affairs of the department in a way that promotes economical efficient and effective use of the resources for which the secretary is responsible; . . .
> - adopt management practices that are responsive to changing government policies and priorities, and that enable decisions to be made and action to be taken promptly; . . .
> - promote continuing evaluation and improvement of the efficiency and effectiveness of the department; . . .
> - promote the maintenance of high standards of conduct (including high ethical standards) within the department; . . . and . . .
> - ensure that proper standards are maintained at all times in the creation, management, maintenance and retention of Commonwealth records and in accordance with any relevant legislation.

3.3.5 The Government decided to accept the recommendations for a principles-based Act, and to accept with qualifications the recommendations about the role of secretaries and their more detailed responsibilities.

---

77 *Transcript*, pp. 198–199.

78 PSC, *Submissions*, p. S540.

79 *Transcript*, p. 478.

80 *Report of the Public Service Act Review Group*, December 1994, AGPS, Canberra.

> Under this model, secretaries would, for the first time, have a clear, published description of what the Government requires of them. This will reinforce the appropriate lines of accountability between the government of the day and the top echelons of the APS.[81]

3.3.6 The Committee considers that it is not necessary to develop legislation that would impose personal liabilities on agency heads in relation to the protection of third party information. However, the Committee considers that it would be desirable for agency heads to have express responsibility for the protection of confidential third party information held by the Commonwealth Government.

Recommendation 1
The Committee recommends that there be a description of responsibilities of heads of agencies in the *Public Service Act 1922*. The description should include responsibility for the protection of confidential third party information held by the Commonwealth Government.

3.3.7 The Committee notes and supports the recommendation by the Review Group that a secretary promote high standards of conduct. The Committee believes that guidelines, operating manuals and training have a significant effect on shaping the environment in which people work and in shaping attitudes within the work place. The Committee considers that the responsibility of the agency head should include responsibility for the provision of guidelines and operating manuals and training.

Recommendation 2
The Committee further recommends that the head of an agency be responsible for providing all agency staff with comprehensive guidelines and operating manuals relating to the protection of confidential third party information that it holds. In addition, the head of an agency should be responsible for ensuring that all staff of the agency receive training in the protection of confidential third party information and compliance with relevant guidelines and operating manuals.

---

81 Gary Johns MP, Assistant Minister for Industrial Relations and Minister Assisting the Prime Minister for Public Service Matters, *Media Release* 'Review of the Public Service Act', 4 May 1995, *Attachment* p. 2.

3.4 Rationale for collecting information

3.4.1 Some evidence suggested that the issue of whether to collect information should be the first point considered. Professor Gregory Tucker, an academic lawyer with expertise in privacy and data protection, told the Committee, "[p]rivacy begins at the collection of information itself: should you collect it or should you not collect it, and how do you collect it?"[82] He argued that the government should only collect and analyse information which is necessary for a specific purpose.[83] Dr June Factor, Committee Member of the Victorian Council for Civil Liberties, commented that there seemed to be a ". . . very powerful tradition that governments operate better the more information they have . . .", although she had never seen any analysis of this.[84]

3.4.2 The collection of information is necessary for the proper functioning of government. There is a need however to continuously and actively consider just what information is necessary. The agency head should be responsible for monitoring the on-going need for collecting confidential third party information.

3.4.3 The Committee notes that IPP 1 is directly relevant to this issue. In all the evidence presented however, surprisingly little expressly addressed this issue. Most evidence was impliedly based on the presumption that all information collected was necessary. The Committee considers that a real commitment to privacy and protection of confidential information requires firstly a demonstration that only necessary information is collected. Each agency which collects third party information should expressly consider this issue and report on the outcome.

> *Recommendation 3*
> The Committee recommends that for each agency that collects third party information, the agency head be responsible for monitoring the on-going need for that information. Each agency should report annually to the Privacy Commissioner on the outcome of that monitoring with regard to personal information. Each agency should state in its annual report the outcome of that monitoring with regard to commercial information.

3.4.4 Once information is collected, there are often many claims for the release of that information. The responsibility for the release of information is an important one.

---

82 *Transcript*, p. 451.

83 G. Tucker, *Submissions*, p. S761.

84 *Transcript*, p. 152.

3.5 Senior managers – discretion to release information

3.5.1 Former ICAC Assistant Commissioner, Hon Adrian Roden QC considers that the power to release information provides a large grey area where discretion is exercised. He suggested that such discretion should be exercised at the highest possible level and not by junior officers. As reinforcement, this discretion should be subject to independent audit.[85]

3.5.2 The Privacy Commissioner seemed to support Mr Roden's suggestion. Mr Kevin O'Connor, told the Committee that there is value in making a mid-SES level officer of an agency responsible for privacy and data protection matters with no right of delegation to another officer, because it is important that the protection of third party information be seen as an important issue within agencies.[86]

3.5.3 An example from the evidence indicates that such an approach to responsibility for the release of information is practical. In the DSS which is a large Commonwealth information holder, the release of information in the public interest, including release for law enforcement purposes, is provided for under paragraph 1314(1)(a) of the Social Security Act in accordance with Ministerial Guidelines as required by section 1315. The delegation to decide whether information will be released in the public interest is currently held by six senior officers in the DSS national office.[87]

3.5.4 The Committee considers that as a matter of policy, a discretion to release information should be held only by a limited number of senior managers and should not be able to be delegated to junior officers. Further, extreme caution should be exercised in the delegation of certain functions relating to the protection of third party information. Such a policy would indicate that the disclosure of third party information is not routine, and that a mere claim of convenience is not sufficient to justify broader delegation. The limited number of senior managers empowered with a discretion to release information should operate to reinforce the important status of the power to release information.

---

85 *Transcript*, p. 19.

86 *Transcript*, pp. 486–487.

87 DSS, *Submissions*, p. S456.

Recommendation 4
The Committee recommends that the power to disclose confidential third party information held by a Commonwealth Government agency be given only to a limited number of clearly identified senior executive service officers who are, where practicable, at a level no lower than SES Band 2.

3.5.5 The Committee considers that the fact of disclosure should be a matter of record and reporting that will assist in the auditing and monitoring of the exercise of this important power.

Recommendation 5
The Committee recommends that agencies be required to provide, within 14 days of the disclosure, reasons to the Privacy Commissioner for an authorised disclosure of personal information being made.

Recommendation 6
The Committee recommends that each Commonwealth Government agency keep a record of authorised disclosures of confidential third party information for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is disclosed, the names of individuals and organisations to whom that disclosure is made, and the date of the disclosure.

3.5.6 The Committee notes that the leaders of an organisation also direct its essential character. The fact of unacceptable behaviour which is common to several agencies suggests that there might be a deficiency in the broader culture. The New South Wales ICAC investigation provides strong indicators of such a deficiency.

3.6 Implications of ICAC findings for Commonwealth agencies

3.6.1 The Independent Commission Against Corruption investigated the unauthorised release of government information in New South Wales. During the investigation evidence revealed that there were also unauthorised disclosures of information held by

the Commonwealth Government information. Assistant Commissioner, the Hon Adrian Roden QC, noted that while only a small proportion of private investigators in New South Wales were investigated 'there is no reason to believe that the position in New South Wales was unique'.[88]

3.6.2 The New South Wales ICAC found that over 30 Commonwealth officers had been involved in the sale, supply or purchase of confidential information. Despite this, senior managers giving evidence before this Committee spoke of their sensitivity to privacy principles. The officers mentioned by the ICAC were employed by the Australian Customs Service, the Department of Defence, the Health Insurance Commission, the Department of Social Security and Telecom. Furthermore, ICAC found that records from the Department of Social Security, the Health Insurance Commission, Telecom, Australia Post, the Department of Immigration, Local Government and Ethnic Affairs, and the Australian Customs Service were included in the trade of confidential information.

3.6.3 The ICAC Assistant Commissioner reported

> It is clear that information held by Commonwealth departments and agencies has been the subject of unauthorised release, both by illicit sale and by improper exchange . . .
>
> Information from the records of the Department of Social Security in particular, and also from other Commonwealth departments and agencies mentioned in the Report, has been sold on the illicit market for many years...
>
> Department of Social Security information was particularly valued . . . The sanctions provided by the Social Security Act have provided little deterrent to those minded to participate in the unauthorised release of the information or subsequent dealings in it. Commencement of the Privacy Act in 1989 had some effect, but the illicit trade in information from the department's records continued until and after the commencement of the Commission's investigation. Some indication of the scope of the trade may be gained from the fact that 50 private investigators in New South Wales were identified as dealers in social security information. Most of it was passed to finance companies, banks and insurance companies. Some went to lawyers and real estate agents.[89]

3.6.4 The ICAC evidence is indicative of behaviour by officers who lack sensitivity to and understanding of privacy principles. The spread of such behaviour across these disparate agencies is indicative of a general failure of officers in the public service to respond appropriately to privacy and security issues in dealing with confidential third party information.

---

88 The Hon Adrian Roden QC, *Submissions*, p. S38.

89 *Submissions*, pp. S37–S38.

3.6.5 The Committee did not attempt to mirror the activities of ICAC, and notes that the ICAC investigation provided valuable evidence which was collected by a source which the Committee considers to be competent. The Committee notes that the ICAC report revealed that there were significant problems in the executive of the New South Wales Government, and considers that there are likely to be similar problems in the executives of the Commonwealth and the New South Wales Governments. Finally, the Committee relies on the fact that ICAC uncovered problems in the agencies of the Commonwealth Government.

3.6.6 The Committee followed up with Commonwealth agencies the Commonwealth matters raised by the ICAC investigation.[90] It would have been extremely fortuitous for Assistant Commissioner Roden to have come across the only officers in each organisation who were releasing confidential information. The Committee considers that other Commonwealth agencies should not necessarily take comfort because no evidence was heard by the ICAC regarding their employees. The ICAC had not set out to investigate the activities of Commonwealth employees generally and there had been no systematic examination of all Commonwealth agencies. The findings of the ICAC that involved the Commonwealth were incidental only to the main focus of the inquiry. There is no reason to believe that other officers were not also engaging in similar information disclosure practices, and that similar practices were not occurring elsewhere.

3.6.7 The Committee believes it is reasonable to expect that the relevant agencies' reactions to the ICAC findings should have included an investigation into whether similar activities were occurring in other States and Territories. Only the Australian Customs Service recognised the problem as systemic with the possibility of it occurring outside New South Wales.

3.6.8 A common element in the responses of agencies to ICAC was that the activities revealed were to some degree due to employees misunderstanding their responsibilities and releasing information in the belief that it was part of their duties. Mr Hawksworth's observation about these practices in the ACS is significant:

> It is those people who were particularly trusted, who were in charge of the particularly sensitive information, who were in fact engaged in the information exchange. So I cannot find a solution that says more locks, more passwords, more security clearances, to that sort of situation. As we have said before, you are really looking at a re-education campaign to explain that this is not an appropriate way.[91]

---

90 Refer Appendix E.

91 *Transcript*, p. 247.

3.6.9 A great deal more needs to be done before privacy could be considered to be entrenched in public sector practices and culture. The Committee agrees that it is important for an agency to have an ethos that nurtures the protection of confidential information within an organisation.

3.7 Fostering and nurturing a privacy culture

3.7.1 Some agencies, including the DPP, claimed that their 'corporate culture' strongly discourages the improper release of confidential information.[92] Others, such as the Department of Defence regard the Privacy Act as reinforcing pre-existing attitudes of protecting confidential information and approaching access from a need to know basis.[93]

3.7.2 Mr Harding of the Public Service Commission stated that he would expect all public servants to know that it was wrong to disclose confidential information, although he also stated that he believed there may be some variability in officers' perceptions about just how wrong they thought it was.[94] Mr Edmund Attridge Acting Deputy Commissioner of the Public Service Commission, stated that the PSC had been devoting its recent efforts to this issue, and that:

> the real issue at the moment is one of awareness in the public sector of the requirements in respect of protection of information and of behaving ethically generally.[95]

3.7.3 The Privacy Commissioner considers that senior managers have a very important role to play in promoting a privacy culture within an agency and notes that in many agencies senior managers do not appear to be actively involved in privacy matters.[96] He found that '[i]n most cases the privacy function is a task allocated to an officer in addition to other functions'.

3.7.4 The Privacy Commissioner commented that some agencies, including the DSS and the ATO had high level and ongoing privacy training and promotion programs. He concludes that in order to improve the protections for confidential information, the

---

92 DPP, *Submissions*, p. S27.

93 Department of Defence, *Submissions*, p. S644.

94 *Transcript*, p. 213.

95 *Transcript*, p. 199.

96 Privacy Commissioner, *Submissions*, p. S566.

organisational status of and resources for privacy should be treated as an important factor.[97]

3.7.5 Comments from Dr June Factor, a member of the Privacy Advisory Committee and also Committee Member of the Victorian Council for Civil Liberties, lend support to the finding by ICAC that there was no consistent policy amongst departments for handling privacy matters. Although that finding was made in relation to the New South Wales public sector, Dr Factor made the following pertinent comments about attitudes to privacy in Commonwealth agencies:

> There is no consistent policy; I think in some departments there is a genuinely negative sense that this is an intrusion on their proper work, that privacy is an issue which may be relevant to somebody else but is not relevant to them because they have been set up in order to do this, this and this and privacy gets in the way.[98]

3.7.6 The Committee agrees with the Privacy Commissioner that senior managers have a fundamental role to play in nurturing a privacy ethos. The Committee takes the view that senior managers have to be actively responsible for applying protective security arrangements within agencies. The overview perspective that senior managers should bring to their work is not always present in more junior officers. The Committee recognises that a senior management that takes an active role in privacy is part of the process of establishing a better privacy culture within agencies.

3.7.7 The ICAC evidence cannot be discounted because it was collected a few years ago. Frequently during the course of the inquiry the Committee was aware of unauthorised disclosures which demonstrated a poor attitude to privacy concerns. For example, the ATO sanctioned several officers who accessed taxpayer files for no proper purpose. The Committee wholeheartedly endorses the words in the ATO circular distributed after staff were detected gaining unauthorised access to the records of certain public figures: 'idle perusal of taxpayer files is *never* acceptable – it is *not* an excuse that there is no intention to make use of information or to pass it on to a third party.'[99]

3.7.8 Unfortunately, the evidence does not support the claims by many to this inquiry that there is an existing privacy ethos. The Committee considers that the establishment of a privacy culture is an important means of ensuring that staff within agencies adhere to administrative measures designed to protect third party information.

---

97 Privacy Commissioner, *Submissions*, p. S566.

98 Dr J. Factor, *Transcript*, p. 397.

99 ATO, *Submissions*, p. S1081.

3.7.9 The Committee considers that senior managers should be more vigilant in their attempts to promote a professional environment which protects information from unauthorised access and to promote the need for such protection within the staff of an agency. It is not convinced by the evidence that enough is being done to nurture a privacy ethos within agencies. Consequently, the Committee believes that agencies should be encouraged to promote privacy values and the procedures adopted to secure privacy as a matter of the highest priority. In particular, the Committee considers that agencies must focus more on education and training to enhance employees' understanding of the concepts of privacy and confidentiality, and the requirement that they incorporate this into their day-to-day work. A greater emphasis needs to be given to ethical values and conduct. In this regard, an important element is the role of an agency's senior managers.

Recommendation 7
The Committee recommends that each agency have a senior manager who is responsible for implementing and promoting privacy standards and the protection of information within an agency. The chosen senior manager should be a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2.

3.7.10 The Committee considers that the development and enhancement of a culture that is sensitive to the responsibility of handling third party information is a matter of great importance and urgency. It is important that such a culture be created and fostered within the public sector generally but it is particularly important for those agencies holding large quantities of confidential information.

3.7.11 The Committee considers that agencies would benefit by establishing focus groups or 'information privacy committees' to review both administrative procedures and compliance with legal requirements. Such committees would assist agency heads to fulfil their responsibilities and their very existence would enhance the 'privacy culture'.

Recommendation 8
The Committee recommends that each agency head establish an Information Protection Committee with the objective of monitoring the protection of third party information within the agency and disseminating information which would foster the greater protection of that information.

3.8 Learning about the demand for confidential information

3.8.1 As well an indicating that confidential information held by the Commonwealth has been bought and sold for illegal purposes, the evidence to ICAC also provided an insight into the nature of the demand for that confidential information and of the persons who create that demand.

3.8.2 Mr Warren Cochrane, Acting National Business Director of the Australian National Audit Office (ANAO) told the Committee that one needs to understand what the market for the information looks like in order to understand weaknesses and to determine the maximum protection needed.[100] He stated further that as a general principle 'we should understand the risks that face us in managing information . . .'.[101]

3.8.3 The Committee notes that these comments were made in relation to the DSS. It considers however, that as part of the active role that senior managers in all agencies must take in promoting privacy within an agency, they should also seek to inform themselves about the possible unsatisfied demand for third party information held by that agency.

> *Recommendation 9*
> The Committee recommends that the senior executive service officers of agencies inform themselves of the demand for confidential third party information held by their respective agencies.

3.9 Function of guidelines and manuals

3.9.1 The role of guidelines and manuals in improving the standards of administrative procedures for dealing with confidential personal and commercial information is important, even where their implementation is voluntary and subject to adaptation to the needs of a particular agency. These general standards have been developed to assist agencies in meeting their obligations and officers in carrying out their duties.

3.9.2 The Committee was keen to assess the role of external assistance in the administrative measures agencies implemented in protecting third party information. Guidance on practices that will enable agencies and officers to meet their legal

---

100 *Transcript*, p. 525.

101 *Transcript*, p. 528.

obligations is contained in the PSC guidelines and the Protective Security Manual (PSM)[102]. There are also the Privacy Commissioner guidelines on the Information Privacy Principles (IPPs) in the Privacy Act and other voluntary guidelines on, for example, data-matching.

3.10 Public Service Commission guidelines

3.10.1 Mr Richard Harding, Assistant Commissioner of the PSC, told the Committee that the PSC had been concerned with making public servants more aware of the standard of conduct that was expected of them in carrying out their duties, including those in relation to the protection of information.[103] To this end, the PSC issues the *Guidelines on Official Conduct of Public Servants*, which specifically address an officer's obligations to protect information. The Privacy Commissioner was consulted on the chapters dealing with information privacy and information management.

3.10.2 Mr Ian Edwards, Director Ethics and Conduct of the PSC, told the Committee that the PSC consulted with agencies about the problems they were having in administering the performance management process.[104] In response to a general perception that there is not a high level of awareness among staff and managers in the APS of the standard of official conduct that is expected of them, the PSC published in 1992 a pamphlet setting out that standard in plain language.[105] It is based on the Public Service Regulations and states clearly that an officer is not permitted to use or disclose information for other than official purposes without the approval of her or his agency.

3.10.3 The PSC has also been involved in the development of 'ethical codes' for individual agencies[106], and in conducting workshops in departments based on standards of conduct, the management of the disciplinary process and on issues relating to ethical conduct. Mr Edwards argued that the whole process had to be cast in a positive light to raise awareness of the standards expected of officers, and of the efficiency, effectiveness,

---

102 See para 2.3 above. The PSM was developed by the Attorney-General's Department in consultation with the Privacy Commissioner and other. Most government agencies have developed their own protective security guidelines based on the PSM.

103 *Transcript*, p. 196.

104 Mr Edwards, *Transcript*, p. 206.

105 PSC, *Submissions*, p. S541.

106 Mr Attridge, *Transcript*, pp. 195–200

image and reputation of the APS.[107] Mr Harding commented further that some departments had focused quite strongly on the promotion of ethics.[108]

3.11 *Protective Security Manual*

3.11.1 The Attorney-General's Department argued that the relevant protective security policies, standards and guidelines set out in the PSM[109] provide a coherent foundation for the establishment of appropriate safeguards for the protection of privacy.[110] Both the Australian National Audit Office (ANAO) and the Privacy Commissioner encourage the use of the PSM. The ANAO uses the PSM as a guide in assessing an agency's approach to protective security policy and the standard of its arrangements. The Privacy Commissioner regards the PSM as a valuable initiative and considers the guidance it offers would help agencies to fulfil their obligations under IPP 4 with respect to the security and storage of personal information. Auditors with the office of the Privacy Commissioner consider that agencies which have adapted general standards, such as those in the PSM, to their particular operational circumstances have 'tended to minimise, more satisfactorily, the likelihood of breaches of security occurring'.[111]

3.11.2 Mr Norman Reaburn, Deputy Secretary of the Attorney-General's Department, advised the Committee that usually departments and agencies adopt the PSM, although there may be variations in protective regimes from agency to agency.[112] Evidence to the inquiry suggested that the PSM is being used as a handbook by some agencies.

3.11.3 The Australian Securities Commission (ASC) claimed it observes the document, file and information security guidelines set out in the PSM in its internal file management system.[113] The ASC provides for information to be provided to persons on a need to know basis, controlled copying, logged file access, register of classified documents, careful disposal of excess copies, physical security controls such as appropriate containers, secure storage areas with restricted access, offices with coded access controls, identity cards for

---

107 *Transcript*, p. 206.

108 *Transcript*, p. 205.

109 For information about the PSM see 2.3 above.

110 Attorney-General's Department, *Submissions*, p. S378.

111 Privacy Commissioner, *Submissions*, p. S561.

112 *Transcript*, pp. 185–186.

113 ASC, *Submissions*, p. S602.

visitors and passwords for computer files.[114] The ASC backs up its use of the PSM with training courses and printed reference guides.

3.11.4 Dr Anthony Butterfield, Assistant Commissioner, National Office and Services of the Australian Taxation Office (ATO), advised the Committee that the ATO has a security manual which is 'entirely consistent' with the PSM.[115] In the ATO manual, computer safeguards such as audit trails, log-ins and encryption are given a very high priority. AUSTEL also advised the Committee that it complies with the PSM for handling and storing confidential commercial information.[116] In particular, AUSTEL officers operate on a need to know basis; documents are copied, copies are numbered and recipients are accountable; and individuals are consulted before the release of information about them.

3.12 Privacy Commissioner's guidelines and advice

3.12.1 The Privacy Commissioner has for some six years provided support, policy advice and guidelines to agencies on privacy issues. Mr Kevin O'Connor, the Privacy Commissioner, considers it necessary and important that agencies develop practices and systems to satisfy the local circumstances of administration.[117] He recognises that variations in procedures between agencies will naturally evolve.

3.12.2 In 1994 he published *Plain English Guidelines to Information Privacy Principles 1–3* and distributed them to staff in agencies with a responsibility for privacy matters. The Privacy Commissioner is working on guidelines for the remaining principles.[118]

3.12.3 Agencies advised the Committee that they followed the Privacy Commissioner guidelines.[119]

3.12.4 The Committee notes that many agencies declared that they complied with best practice manuals and guidelines for the protection of confidential information. While such statements are a positive indicator of awareness at the most senior management levels

---

114 ASC, *Submissions*, pp. S603–S604.

115 Dr Butterfield, *Transcript*, p. 286.

116 AUSTEL, *Submissions*, p. S58.

117 Mr Kevin O'Connor, *Transcript*, p. 494.

118 Privacy Commissioner, *Submissions*, p. S1069.

119 For example, DSS complies with the voluntary data-matching guidelines. Refer DSS, *Submissions*, p. S440.

of agencies, of the need for protection for confidential information, they are not a measure of whether protections are successfully enforced. Nevertheless, it is instructive to review some of the many examples of administrative arrangements agencies have in place for the protection of confidential personal and commercial information.

3.13 Examples of administrative arrangements

3.13.1 There are a many different administrative measures that agencies use to safeguard the third party information they hold and that give effect to and support the standards and manuals. The Committee has not attempted an exhaustive tabulation of measures but has selected examples from the evidence. The chosen measures illustrate the wide variety of administrative measures that protect confidential information – physical security controls, logical computer security controls, the development of procedures for the handling of information, the preparation of guidelines encouraging adherence to standards in legislation, the training and education of staff, the promotion of the importance of privacy issues, agency access agreements and procedures and audit methods.

a) Physical security controls

3.13.2 The Australian Transactions Reports and Analysis Centre (AUSTRAC) is a significant Commonwealth data holder which provides data to all relevant Commonwealth and state law enforcement agencies and the Australian Taxation Office (ATO).[120] Mr Neil Jensen, the director's representative of AUSTRAC, stated that AUSTRAC provides physical security controls such as guards on the premises, clear desk policies, accompanied visitors and identity cards. It also imposes access controls such as personnel security checks, couriers and needs based access to data.[121]

3.13.3 The National Crime Authority (NCA) has a number of internal security measures in place to ensure that staff comply with the prohibition against disclosure of information held by the NCA. These include:

- physical security to protect staff and assets;
- procedures for classifying sensitive material;
- authorised entry to premises;
- secure areas designated for storage of sensitive information;
- security clearances of staff;
- computer security systems such as access control; and

120 W. Coad, *Transcript*, p. 39.

121 AUSTRAC, *Transcript*, pp. 40–41.

- internal distribution of information on a needs to know basis.[122]

3.13.4 AUSTEL stated that its premises have 24 hour electronic security and controlled access during business hours.[123]

b) Computer security controls

3.13.5 The storage of data in computer systems creates particular security concerns which relate to physical security and also to logical security. In terms of logical security, AUSTRAC imposes specific controls such as encryption of information, password access and audit trails on access.[124]

3.13.6 The Department of Social Security (DSS) operates from some 300 locations and has client data stored on computer that can be readily used by officers seeking prompt access at some 20,500 access points.[125] DSS practices provide for each officer position to have an access profile and for access to be governed by a need to know principle.[126] Staff must apply for access to the database and agree to follow departmental policy in relation to its use. Staff are instructed not to divulge their individual logon identifier or password. In support of these measures, the DSS monitors access to the database looking for and investigating patterns which indicate computer browsing or abuse.

3.13.7 Mr John Hawksworth, National Manager Investigations in the Australian Customs Service (ACS), told the Committee that only a limited number of customs officers may access sensitive information and anyone else with a need to know must sign a written request and state a supporting reason. The request is then stored for recording and checking purposes.[127]

3.13.8 Australia Post's internal controls and procedures for data security include encryption of data transmission, logical access controls – passwords, restriction and segregation of data access privileges, message authentication – and physical access being limited to authorised personnel.[128]

---

122 National Crime Authority, *Submissions*, p. S267.
123 AUSTEL, *Submissions*, p. S58.
124 Mr N. Jensen, *Transcript*, pp. 40–41.
125 *Transcript*, p. 538.
126 DSS, *Submissions*, p. S438.
127 *Transcript*, pp. 254–255.
128 Australia Post, *Submissions*, p. S254.

3.13.9 In the Health Insurance Commission a Protective Security Management Committee supports the security responsibilities of the managers. Logical security controls apply to:

- software to control access to mainframe systems;
- access through user identifier and password;
- separation of users into functional groups for access only to specific mainframe applications and data required to perform the group's duties;
- unattended terminals must be reaccessed before work can resume;
- enforced changes to passwords; and
- illegal access attempts are logged, rejected and where possible tracked.[129]

c) Guiding, informing and training staff

3.13.10 The DSS advised the Committee that it issues instructions to staff which govern the way information about clients can be collected, used, protected and disclosed.[130] The Australian Federal Police also advised that it provides training for employees about recognising and dealing with information that is public in nature and information that needs to be protected.[131]

3.13.11 DAS has developed a set of procedures for the protection of contractor information during the procurement process entitled the *Code for Handling Conflict of Interest.*[132] It has also developed a series of information papers and regularly conducts training for all staff. DAS has also developed *Guidelines for the Handling of 'Commercial-In-Confidence' Documents.*

3.13.12 Australia Post issues written procedures dealing with how requests for the divulging of address information are to be handled. It also provides training to staff who handle third party information, such as addresses, redirection and private box details, on their obligations not to improperly disclose information.[133] When they commence work with Australia Post employees are required to acknowledge advice that they are bound by provisions of the Crimes Act.

3.13.13 The Health Insurance Commission provides training to staff on the importance of keeping confidential information secure and issues internal staff notices to remind

---

129 Health Insurance Commission, *Submissions*, p. S197.

130 DSS, *Submissions*, p. S438.

131 AFP, *Submissions*, p. S68.

132 DAS, *Submissions*, pp. S727–S728.

133 Australia Post, *Submissions*, p. S254.

staff.[134] Staff are also required on joining to sign a document acknowledging that they understand the requirement upon them to preserve the confidentiality of information.

d) Joint agency agreements on access

3.13.14 Mr Neil Jensen, Director's Representative of AUSTRAC, considered that it has policies that reflect its sensitivity to both security and privacy aspects of handling information. In particular, AUSTRAC had followed the spirit of privacy principles through the head of AUSTRAC entering memorandums of understanding (MOU) with the chief executives of law enforcement agencies. Each MOU sets out the key elements of the information sharing relationship between the two agencies:

- ability to access information;
- what can be accessed;
- how access is undertaken;
- procedures requirements;
- forms signed by users;
- names of people given access;
- the level of access; and
- the reason for access.[135]

3.13.15 The Australian Federal Police (AFP) has also entered into MOUs to formalise the sharing of information with other law enforcement agencies.[136]

e) Specific access procedures

3.13.16 Australia Post's Security and Investigation Service screens all requests for address information not made under specific provisions of Commonwealth legislation. Australia Post stated that '[t]his was done to ensure that such requests are handled at a senior level and in a consistent manner.'[137] Procedures were introduced following an inquiry into information handling practices in New South Wales. They include:

- requests in writing;
- reasons given;
- a nominated liaison officer in the State branch considers each request;
- replies are faxed to a previously registered and verified fax number at the requesting agency; and
- a record of all inquiries is maintained and subject to audit.

---

134 Health Insurance Commission, *Submissions*, p. S196.

135 AUSTRAC, *Transcript*, p. 45.

136 AFP, *Submissions*, p. S67.

137 Australia Post, *Submissions*, p. S255.

f) Internal audit

3.13.17 The Department of Administrative Services (DAS) stated that its Performance Review and Audit Branch carried out an audit using the Privacy Commissioner's Audit Manual.[138] The auditors concluded that while the implementation of the privacy principles in DAS was satisfactory, there was a need to increase the general awareness level about the Privacy Act within certain areas of the department. This was addressed through a national training program.

3.13.18 Australia Post stated that it backs up its information technology security controls and procedures with independent internal and external audits.[139]

g) Comments on examples of administrative arrangements

3.13.19 The Committee considers that it is both appropriate and desirable for agencies to have a range of administrative measures safeguarding third party information and for them to differ between agencies. They are all considered to be useful measures in contributing to the protection of such confidential information. This means that the specific needs of agencies can be met.

3.13.20 Agencies are subject to monitoring and auditing of their practices, including auditing and monitoring of safeguards for confidential third party information.

3.14 Auditing and monitoring programs

3.14.1 The Auditor General has a broad brief under the *Audit Act 1901* to audit and monitor the activities of Commonwealth agencies[140] and the Privacy Commissioner has a specific brief under the Privacy Act to audit and monitor the practices of agencies with regard to satisfying their obligations under the Privacy Act. Both these offices provide input to the public service wide standards for protection of confidential third party information, and input to the assessment of the adequacy of an individual agency's adaptation of the standards and principles.

3.14.2 The Australian National Audit Office (ANAO) conducts or directs comprehensive audits of the administration and functions of Commonwealth agencies. These audits cover

---

138 DAS, *Submissions*, p. S728.

139 Australia Post, *Submissions*, p. S254.

140 Three Bills designed to replace the Audit Act are currently before the Parliament: the Financial Management and Accountability Bill 1994, the Commonwealth Authorities and Companies Bill 1994 and the Auditor-General Bill 1994.

the protection of all Commonwealth assets, including information held by the Commonwealth.[141] The ANAO has also undertaken and reported on an audit of the efficiency and effectiveness of the protection of confidential client information from unauthorised disclosure by the Department of Social Security.[142]

3.14.3 The ANAO is sensitive to the possibility that the adequacy of its audit programs might be challenged. The ANAO regards its past audit focus on physical security of information as inadequate and intends to take a more comprehensive approach, including the development of practical guidelines so agencies can check and manage their data systems better. The ANAO considers that operational matters are important because a minor weakness in a data system could allow a small number of unauthorised users to access an entire database. This could be a significant risk should those users be targeted by an outsider.

3.14.4 The guidelines the ANAO has only recently developed for protection of personal information address the following kinds of issues:

- has an agency strategically addressed data systems management by putting effective security policies in place;
- what is the extent of access to data by agency staff – who has access, why does each officer have access and is it needed;
- what sorts of controls are in place – how effective are they and is an agency using the latest technology for effective control; and
- are audit trails possible.

3.14.5 The ANAO has commented that agencies are aware of their responsibilities in relation to the security of information and are well intentioned. It recognises that at times however, agencies have difficulties in putting in place effective practical systems to give effect to security policies. The difficulties arise in part from problems in inculcating a culture of security through all levels of an agency's staff, especially where there is a rapid staff turnover.

3.14.6 Under the Privacy Act the Privacy Commissioner has considerable audit and investigation powers. The Privacy Commissioner has conducted an audit program since 1991 under paragraph 27(1)(h) of the Privacy Act to assess whether an agency is complying with the Information Privacy Principles. In 1993–94 seven IPP audits of

---

141 Auditor-General, *Submissions*, p. S140.

142 Auditor-General, *Audit Report No. 23, Department of Social Security – Protection of Confidential Client Information from Unauthorised Disclosure*, AGPS Canberra 1993.

Commonwealth agencies were completed, adding to the 24 completed in previous years.[143] The Privacy Commissioner has mainly relied upon the information obtained from IPP audits to assess the adequacy of security arrangements within agencies.[144] In this regard the adequacy of both security policies and the practices within agencies are relevant.

3.14.7 Auditors in the Privacy Commissioner's office found that although agencies recognised the significance of security for their general operations, the practices of officers sometimes failed to meet the standards of the stated security policies of agencies.[145] Mr Kevin O'Connor, the Privacy Commissioner, gave evidence that agencies generally accept the recommendations that are made in these reports.[146]

3.14.8 The Privacy Commissioner has also conducted an audit program since 1991 under paragraph 28(1)(d) of the Privacy Act to examine the records of the Commissioner of Taxation in relation to tax file numbers and tax file number information.

3.14.9 The Privacy Commissioner also has powers under section 40 to investigate an act or practice that may be an interference with the privacy of an individual, both where a complaint has been made and where he thinks it desirable. Breakdowns in security practices which have come to the attention of the media have been investigated by the Privacy Commissioner.

3.14.10 Auditing is very important in terms of identifying problems with administrative measures for safeguarding third party information. The Committee relies on relevant findings of ICAC and of audits in responding to concerns about administrative measures identified in the inquiry.

3.15 Identified concerns with administrative measures

3.15.1 Weaknesses in administrative protections for confidential third party information are most apparent if unauthorised access occurs. The extent of the weakness may be measured in part by the known incidence and frequency of unauthorised access that has taken place.

---

143 This information was compiled from the Annual Reports of the Privacy Commissioner.

144 Privacy Commissioner, *Submissions*, p. S560.

145 Privacy Commissioner, *Submissions*, pp. S560–561.

146 Kevin O'Connor, *Transcript*, p. 495.

3.15.2 Specific comments were made during the course of the inquiry in regard to incidents and inadequacies. The comments related to both the security and privacy aspects of the inquiry. They addressed concerns about inter-agency transfers of information, physical security of information, security in a computing environment, portable personal computers, controls on data-matching and contracting out by Commonwealth agencies. These comments are considered below and some suggestions of ways to overcome the weaknesses are canvassed.

3.16 Inter-agency transfers of information

3.16.1 The Australian Anti-Bases Campaign Coalition argued that disclosure safeguards were inadequate in the AFP and the DSS.[147] After a demonstration in November 1991 at the Australian International Defence Equipment Exhibition (AIDEX), the AFP provided arrest details on some 238 persons to the DSS. The Privacy Commissioner considered that the AFP may have been in breach of IPP 4, and possibly also in breach of IPP 11.

3.16.2 The Privacy Commissioner considers that inter-agency agreements on transfers of information are valuable because they encourage a disciplined approach to such transfers, and allow more careful consideration of the legal basis for disclosure. They also discourage unauthorised flows of information between individual officers.[148]

3.16.3 The Committee notes that there are various agreements under which agencies provide access to third party information. The Committee also notes that the ICAC report emphasised the importance of regularising the flow of information between agencies and avoiding unofficial information sharing arrangements.[149] The Committee considers that there should be a clear commitment to regularised access and believes that agencies should enter into inter-agency arrangements wherever possible in accordance with guidance from the Privacy Commissioner.

> *Recommendation 10*
> The Committee recommends that agencies be required to enter into inter-agency agreements on the disclosure of confidential personal information to be approved by the Privacy Commissioner.

147 Australian Anti-Bases Campaign Coalition, *Submissions*, pp. S80–S88.

148 Privacy Commissioner, *Submissions*, p. S565.

149 Privacy Commissioner, *Submissions*, p. S564.

3.17 Physical security

3.17.1 The Privacy Commissioner argued that much of the most sensitive personal information held by the Commonwealth is stored in paper form and held on traditional paper files.[150] This is so because the primary file from which computerised data is drawn would include the original and all subsequent documentation. Auditors in the office of the Privacy Commissioner have frequently expressed concern about the level of security afforded to this type of record including inadequate logging of file movements, lack of secure locks on filing cabinets, unattended files and poor file management.

3.17.2 The Privacy Commissioner acknowledged that agencies accept recommendations from the auditors in relation to these issues, but concludes that agencies could do 'a good deal more work' to strengthen practices in these areas.[151] He also commented in relation to security breaches which have received media exposure that the incidents have typically involved bad disposal practices or a breakdown in internal quality control procedures.

3.17.3 The Committee considers there is an ongoing need for security. The Committee notes that both the ANAO and the Privacy Commissioner encourage the use of the PSM. Although some agencies made specific reference to physical security there was not strong emphasis on the need for it. The Committee accepts the Privacy Commissioner's advice that physical security is important. This matter is taken further in the next recommendation.

3.18 Security in a computing environment

3.18.1 The Privacy Commissioner comments that although the personal data held in computerised form tends to be more structured and less sensitive than data held in paper form, the threats to privacy of individuals posed by computer storage are significant.[152] These threats exist because of the volume of data that can be held in such form and the ease with which large volumes of data can be accessed and used.

---

150 Privacy Commissioner, *Submissions*, p. S561.

151 Privacy Commissioner, *Submissions*, p. S562.

152 Privacy Commissioner, *Submissions*, p. S563.

3.18.2 The audit staff of the Privacy Commissioner have surveyed agencies in respect of the security of all types of computing environments.[153] The Privacy Commissioner finds that great weight is usually given in the establishment of computer systems to security issues and that many agencies conduct their own computer security audits. He comments that it is critical that agencies keep under continuous review their computer security policies given the continuing evolution of this technology. Auditors from the Privacy Commissioner's office have found that agencies have made 'prudent choices' in relation to the selection of computer security products. Weaknesses develop however, where key features of these products have not been put into operation. Security features include enforced password changes, automatic screen shutdown, automatic log-off, system lock-out if invalid passwords are used, and automatic deletion of the access facility of retired employees.

3.18.3 Examples from three different agencies highlight the importance of the use of computer security.

a) Department of Social Security

3.18.4 The ANAO conducted an audit of the efficiency and effectiveness of the protection of confidential client information from unauthorised disclosure by DSS. The ANAO was critical of the limited capability of DSS to monitor access to the client database, and recommended that the department consider the use of audit trails for monitoring purposes. Mr James Humphreys, National Manager (Operations) of the DSS, told the Committee that the department, which has some 20,000 employees, at first considered the cost of implementing this ANAO recommendation would be very high.[154] After some development design, the DSS developed a more sophisticated logging system, which would be cost effective.

3.18.5 The Committee believes that this example provides an important demonstration of how technological development can improve the level of protection for confidential third party information held by the Commonwealth. It concludes that computer security can be enhanced by using available technologies more widely.

b) Health Insurance Commission

3.18.6 Several Health Insurance Commission employees were found by the ICAC to have unlawfully released Medicare information, and were subsequently dismissed.

---

153 Privacy Commissioner, *Submissions*, p. S1069.

154 *Transcript*, p. 546.

3.18.7 The Committee raised with the Health Insurance Commission witnesses the matter of whether adequate safeguards had been put in place to deter the unlawful release of confidential data. At the time of the release, the Commission did not have any mechanism to monitor employee access to the database which holds about 17½ million records.[155] The Health Insurance Commission subsequently put into place an audit trail system to track, record and analyse access to Medicare information by employees in order to identify unusual or suspicious access patterns.

c) Australian Taxation Office

3.18.8 The Australian Taxation Office (ATO) made a supplementary submission to the Committee in response to media reports that ATO staff had gained unauthorised access to the tax records of certain public figures. The Internal Investigations Section of the ATO identified officers who had improper access to taxpayers' records through an audit trail on computer files.[156] An audit trail facility which is active on a permanent basis is maintained on every access to a taxpayer's records, and enables identification of the names of all officers who access a record, and the precise times and dates of access.

3.18.9 After preliminary investigation by the Privacy Commissioner, he found that the matter did not warrant formal investigation under section 40(2) of the Privacy Act. He concluded that:

> As presently briefed, it would appear that your internal audit mechanisms have been effective and that firm action has been taken by the ATO. I value the commitment to confidentiality which this action indicates.[157]

d) Conclusions

3.18.10 The Committee considers that computer security is of critical importance to the protection of confidential information. It notes that ICAC findings highlighted computer security as a particular problem. Building on the comments above on physical security, the Committee sees a strong need for a comprehensive approach to security and considers that agencies should adopt adequate security standards.

---

155 Health Insurance Commission, *Transcript*, p. 270.

156 ATO, *Submissions*, p. S1077.

157 ATO, *Submissions*, p. S1079.

Recommendation 11
The Committee recommends that all agencies adopt a comprehensive security system such as that provided by the *Protective Security Manual*. Agencies should adapt general security standards to their particular circumstances.

3.18.11 In particular, the Committee notes that the ICAC recommended that access to protected information be strictly limited, and that an efficient system be maintained to enable all persons who access information to be identified. The Committee also notes that the Privacy Commissioner's office strongly supports the conclusion by ICAC in favour of the automatic logging of user transactions and inquiries on computerised systems to provide audit trails and as a deterrent against misuse.[158]

3.18.12 The Committee considers that the ATO matter discussed above lends strong support to these views about the importance of computer security and of an audit trail and other measures as valuable means of safeguarding third party information. The Committee notes that one of the outcomes of the ANAO audit of DSS, was the development by the ANAO of *Best Practice Guidelines for the Protection of Personal Information held by Government Agencies*. The Committee considers that security measures which are active on a permanent basis should be maintained on computer files which contain third party information. The Committee concludes that computer security would be enhanced by the use of guidelines.

Recommendation 12
The Committee recommends that all agencies adopt adequate standards for computer security. Guidelines should be developed after incorporating advice from existing government agencies with expertise in computer security.

3.18.13 The Committee recognises that if a person is so minded to look at information to which she or he has access even though there is no legitimate need to do so, such access can not always be prevented. Audit trails will at least provide an opportunity to detect that access and to take appropriate action. It is to be hoped that they also provide an impetus to review an individual officer's breadth of access to files, and to the scope

158 Privacy Commissioner, *Submissions*, p. S563.

of information contained within each file. The Committee considers that computer security should also be the subject of express audit to assess its effectiveness. To this end computer security should be integrated into the ANAO program.

Recommendation 13
The Committee recommends that the Australian National Audit Office conduct security efficiency audits of computer systems.

Recommendation 14
The Committee recommends that sufficient resources be allocated to the Australian National Audit Office to support this role.

3.19 Portable personal computers

3.19.1 The Privacy Commissioner expressed concern about the more portable computer equipment which can be used away from the agency site and cautioned that policies that only address protection of 'fixed-site' computers would be found lacking.[159]

3.19.2 One recent unauthorised disclosure of information indicates that the Privacy Commissioner's concerns are well founded. In December 1994 a portable computer was stolen from the home of a senior ACT Comcare employee.[160] Subsequently, Comcare documents containing confidential information in relation to matters before the AAT were printed from a stolen computer and provided to the media.

3.19.3 As a consequence, Comcare issued a directive to staff restating the policy in relation to classified material. It provided that no staff are to work from home without the knowledge and approval of a member of the executive. Comcare also advised the Committee that encryption software is to be placed on all computers to be used for work at home.

3.19.4 The Committee accepts that in the Comcare case, confidential personal material was disclosed because of apparent criminal action by an unknown person. Nevertheless, the Committee considers that in a working environment where the opportunity for home

159 Privacy Commissioner, *Submissions*, p. S563.

160 Comcare, *Submissions*, pp. S1082–S1083.

based work is likely to increase, security for portable computers is an important issue that should be addressed now.

3.19.5 The Committee notes that the survey undertaken by the Privacy Commissioner on security arrangements in computing environments includes portable personal computers. As the Comcare example has shown, for work away from the site of the fixed office such as home based work, the installation and activation of security features for portable computers is an important computer security matter, as are guidelines about officer behaviour. The Committee believes that computer security policies should specifically address portable computers outside the fixed place office.

> *Recommendation 15*
> The Committee recommends that security manuals specifically address the process required to authorise work taken out of the fixed office site and the security features of portable computers.

3.20 Contracting out by Commonwealth agencies

3.20.1 Contracting out is an arrangement whereby a government agency enters into a contract with an external or government supplier for the provision of goods or services. As contracting out has become more common, it has been suggested that contracting out is weakening the protections of the Privacy Act. The Privacy Commissioner observes that '[t]here is a growing trend for functions traditionally carried out by public authorities to be contracted to private sector companies'.[161] This trend applies to functions, including computing, which involve the handling of personal information.

3.20.2 The Attorney-General's Department advised the Committee that confidentiality clauses were included in contracts with service providers as a matter of course.[162] The Department also advised that the Crimes Act and secrecy provisions of other Acts might apply to contractors.[163]

3.20.3 Section 8 of the Privacy Act provides for certain types of acts done on behalf of an agency and which are the subject of complaint to be scrutinised by the Privacy Commissioner. The Privacy Commissioner has concluded that individuals could not assert

---

161 Privacy Commissioner, *Submissions*, p. S574.

162 Attorney-General's Department, *Submissions*, p. S948.

163 Attorney-General's Department, *Submissions*, p. S949.

their rights under the Privacy Act in relation to activities undertaken on behalf of a Commonwealth agency by a contractor. Contracting out he concludes will 'have the side-effect of lowering the level of privacy protection that otherwise attaches to personal information given to, or acquired by, Commonwealth agencies.'[164]

3.20.4 The Privacy Commissioner suggested this might be overcome by legislative or administrative means. The Privacy Act could be amended to make either the agency or the contractor liable for observance of the IPPs. Under an administrative approach the service contract could include terms applying the IPP giving the Privacy Commissioner ability to inspect and ensuring the Privacy Commissioner is involved and the recommendations are adopted.

3.20.5 The Privacy Commissioner has published *Advice for Commonwealth Agencies Considering Contracting Out (Outsourcing) Information Technology and Other Functions* which sets out model clauses and advice applicable to all contracts for information technology services involving personal information.[165] He suggested that section 8 of the Privacy Act be amended so the Act would apply to improper use or disclosure of information by a contractor under an outsourcing arrangement.

3.20.6 The Committee notes that the *Employment Services Act 1995 and the Employment Services (Consequential Amendments) Act 1995*, extended the Privacy Act to contracted case managers. Under the case management system, confidential information about individuals is to be provided to contracted case managers who will not necessarily be aware of the need to protect confidential personal information. The Committee was asked to report on the Bills, in part because of concerns that the scheme proposed by the legislation may have raised issues relating to privacy and confidentiality.[166] The Privacy Commissioner considered the proposed extension of the Privacy Act to be a 'lesser option' than he preferred. He accepted that in terms of the employment services targeted, the proposal would mean that a consistent set of standards

---

164 Privacy Commissioner, *Submissions*, p. S576.

165 Privacy Commissioner, *Submissions*, p. S1070.

166 These Acts provide an example of contracted services with which the Committee is familiar, because the Employment Services Bills were referred to it for an advisory report during their passage through parliament. House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on Employment Services Bill 1994 and Employment Services (Consequential Amendments) Bill 1994*, House of Representatives Printing Unit, September 1994, p. 45.

would be applied whether a person was dealing with a public, community or private sector case manager.[167]

3.20.7 The Committee notes that the Industry Commission received a reference on contracting out for inquiry and report by the end of 1995.[168] In particular, term of reference 3 for that inquiry requires the Industry Commission to report on costs and benefits taking into account the existing legal framework. The Committee considers that contracting out presents an unacceptable opportunity for significantly undermining the privacy regime established under the Privacy Act. In the short term, it favours the legislative approach of an amendment to the Privacy Act that would make the contractor primarily liable for observance of the IPPs.[169] An individual would then be able to pursue a contractor directly as if the contractor were the agency. This would overcome the present position in which the individual is left out of any pursuit of redress against the contractor.[170] The Committee notes that the Privacy Commissioner sees section 11B(5) of the Privacy Act as an analogous provision which applies the Privacy Act similarly to certain agents of credit providers.[171]

> *Recommendation 16*
> The Committee recommends that the *Privacy Act 1988* be amended to make a contractor to a Commonwealth agency primarily liable for observance of the Information Privacy Principles as if the contractor were the agency.

3.21 Conclusions on the adequacy of existing administrative measures

3.21.1 The Committee has considered a range of measures such as security, instructions and guidelines issued by agencies to their employees, specific inter-agency arrangements for the exchange or transfer of data, monitoring mechanisms or audit trails, agency disclosure policies, staff training and attitudes within agencies. This has enabled it to

---

167 House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Employment Services Bill 1994 and the Employment Services (Consequential Amendments) Bill 1994*, House of Representatives Printing Unit, September 1994, p. 48.

168 *Exhibit 43, Contracting Out by Public Sector Agencies*, Terms of Reference, Hon George Gear MP, Assistant Treasurer (8 December 1994).

169 In the long term, the Committee prefers the approach in chapter 10.

170 Ms Joan Sheedy, *Transcript*, p. 512.

171 Privacy Commissioner, *Submissions*, p. S576.

make an assessment of the administrative safeguards and to suggest improvements to the existing measures which are to be found in the recommendations in this chapter.

3.21.2 Generally agencies have adopted adequate security policies. However, there is evidence that the practical systems put in place to give effect to these policies are not always satisfactory. The Committee considers that IPP audits by the Privacy Commissioner and protective security audits by the ANAO should be continued as a means of revealing problems with existing systems and generating solutions to those problems.

3.21.3 Inadequacies in administrative procedures for protecting information are compounded in an environment of rapid technological change bringing an increased capacity to store, analyse and manipulate data. More significantly, the convergence of communications technologies is creating privacy issues requiring broader legislative and administrative responses.

3.21.4 From the evidence available on confidential commercial information held by the Commonwealth, the Committee found that there was greater acceptance by agencies of the need for protection of commercial information than there was for protection of confidential personal information, although it is not obvious why this should be so.

3.21.5 In some circumstances, administrative measures are not sufficient and legal measures are needed. One set of circumstances in which this may be so is when Commonwealth agencies wish to transfer confidential third party information for purposes which may not be related to its original collection.

Chapter 4

Legal safeguards and the legitimate transfer of information

Laws governing the transfer of information between government agencies are contained in the Privacy Act, in various Commonwealth Acts dealing with specific agencies and the FOI Act. It is necessary to balance accessibility to and protection of information. The balance is often between protecting public revenue and expenditure and protecting privacy. Law enforcement is a further area in which the balance is criticised. The Crimes Act, the Privacy Act (particularly IPPs 10 and 11), the FOI Act and various other laws limit the transfer of information.

Some witnesses thought desirable transfers of information were inhibited by various secrecy provisions. The treatment of other government agencies in the same way as the public was criticised.

The Committee concludes that transfers of information between agencies should be regulated by the Privacy Act rather than by the secrecy provisions of Acts specific to particular agencies. Data-matching is of particular concern. The Privacy Commissioner's data-matching guidelines should be made mandatory and data-matching programs should only proceed on the authority of an identified senior manager. The chapter focuses on the role of agency heads in the transfer of information.

4.1 Introduction

4.1.1 As discussed in chapter 2, legal safeguards for third party information are to be found in both the common law and statute law. The law that is critical in determining the extent to which third party information is legitimately transferred between government agencies is contained in the Privacy Act and in the various specific Commonwealth Acts. Some agencies indicated that the FOI Act might also be relied upon to transfer information.[172]

4.1.2 From the standpoint of an agency seeking to collect information, the DSS has stated that it collects information from other agencies either under a common law right to solicit information, by use of its powers under the Social Security Act or by way of administrative arrangements.[173] In deciding whether to release information, it may be necessary for an agency to determine if disclosure would be a breach of the secrecy

172 For example, the AFP, *Submissions*, p. S65.

173 DSS, *Submissions*, p. S443.

provisions in the Crimes Act and possibly other agency specific legislation, or a breach of the FOI Act. For example, section 60A of the *Australian Federal Police Act 1979* prevents a person, including an AFP member from disclosing prescribed information '. . . except for the purposes of this Act or the regulations, or for the purpose of carrying out, performance or exercise of any of the person's duties, functions or powers of the Act or the regulations . . .'.[174]

4.1.3 If the disclosure would not be a breach of the applicable secrecy provisions, it is necessary to consider the application of the Privacy Act. The Privacy Commissioner has highlighted IPPs 10 and 11 as the most directly relevant principles.[175] While IPP 10 limits the use of personal information, IPP 11 limits its disclosure. Both principles provide for a balancing of the privacy interests of the individual concerned and the relevant public interests of enforcement of the criminal law, law imposing a pecuniary penalty and protection of the public revenue.

4.2 Competing concerns in determining legitimate transfers

4.2.1 The balancing of interests evident in IPPs 10 and 11 is an underlying difficulty in determining what are legitimate transfers of information. This issue of what constitutes a legitimate transfer of information between government agencies was one that was not agreed between agencies who gave evidence to this inquiry. In the first instance, legitimacy must be determined by reference to statutory provisions. Strictly interpreted, a legitimate transfer of information is one that is made expressly according to law. Agencies seeking a broader interpretation of what might be transferred argued that legitimacy also rests on established rules, principles or standards. Some agencies that are party to transfers regard those that are not expressly authorised by law as nevertheless legitimate because they would enable official duties to be carried out more efficiently and effectively.

4.2.2 Traditionally, some agencies have had wide access to third party information transferred from other agencies. This was evident from issues raised during the ICAC inquiry. Eleven Australian Federal Police (AFP) personnel were mentioned in the ICAC evidence regarding the release of confidential information, but were not identified in the ICAC report, because as Commonwealth employees mentioned in connection with the release of Commonwealth information, the ICAC was constrained by its terms of reference from making a finding in regard to these individuals. The AFP subsequently

174 AFP, *Submissions*, p. S65.

175 Privacy Commissioner, *Submissions*, p. S567.

conducted inquiries into six of those employees. The AFP Internal Investigation Division found that no criminal or disciplinary offences had been committed by those employees. That internal inquiry was satisfied that the release of information had been done, morally if not legally, for legitimate law enforcement reasons.[176]

4.2.3 The Attorney-General's Department has stated that in determining what should be the legitimate transfer of information between agencies, it is necessary to balance different factors.[177] The Department acknowledges that on the one hand, an unregulated transfer of information has implications in terms of privacy and breach of confidence. However, on the other hand, limits on the access of Commonwealth agencies to information may impede the agencies, particularly in relation to law enforcement and revenue protection.

4.2.4 The Privacy Act expressly provides for the Privacy Commissioner to balance relevant interests. The Privacy Commissioner shall:

> have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.[178]

4.2.5 The AFP is concerned that current approaches to interpretation of the Privacy Act adversely affect law enforcement:

> There is anecdotal evidence that the legitimate sharing of information within the Commonwealth has sometimes been wrongly refused. This appears to be especially so recently at regional level and at junior levels of administration. The publicity surrounding the Privacy Act, combined with inadequate understanding of its application and interpretation, apparently prompts doubtful or fearful administrators to opt for, the safety of non-disclosure. An unfortunate consequence of this so-called 'safe' approach can be to encourage corrupt or unlawful access to information which should be legitimately transferred.
>
> The difficulties for the AFP arguably arise not from existing legal safeguards, but from the interpretation of laws.[179]

4.2.6 The Privacy Commissioner recognises that there is conflict between the interpretation of the IPPs by his office and their interpretation by other agencies, particularly those agencies with responsibilities for fraud control, revenue protection and

---

176 Australian Federal Police, *Exhibit 39.*

177 Attorney-General's Department, *Submissions*, p. S380.

178 Privacy Act, s 29(a).

179 AFP, *Submissions*, p. S70.

law enforcement. However he rejects what he feels is the implication from the second term of reference that although the legal safeguards may adversely affect Commonwealth administration they are nevertheless adequate for protecting privacy.[180]

4.2.7 It is not a straightforward matter to determine whether a transfer of information between government agencies may legitimately occur. How the provisions are interpreted by agencies involved will affect such transfers.

4.3 Mixed views on whether desirable transfers of information are inhibited

4.3.1 The DPP has argued that both secrecy provisions in Commonwealth legislation and the provisions of the Privacy Act 'place a fetter upon the Commonwealth's capacity to detect and prevent fraud against its programs'.[181]

4.3.2 The DSS conducts matching exercises to compare information it holds with that held by other agencies to detect incorrect payment of social security benefits and to minimise fraud. The DSS argued that information transfer between agencies can be impeded by the existing legislative provisions. DEET also commented that the Privacy Act had prevented legitimate transfers of information from occurring.[182]

4.3.3 Former ICAC Assistant Commissioner, the Hon Adrian Roden provided a counter claim to support for a more liberal approach to transfers. Mr Roden states that '[c]are must be exercised to avoid treating departmental convenience as sufficient to give "legitimacy" to the transfer of protected information.'[183]

4.4 Interpretation of secrecy provisions

4.4.1 Mr Kevin O'Connor, the Privacy Commissioner, told the Committee that agencies such as the ATO and DSS have historically been very cautious in releasing their data for police purposes.[184] The ATO however, considers that its secrecy provisions do not inhibit the legitimate transfer of information to other agencies.[185]

---

180 Privacy Commissioner, *Submissions*, p. S567.

181 DPP, *Submissions*, p. S28.

182 DEET, *Submissions*, p. S928.

183 A. Roden, *Submissions*, p. S40.

184 *Transcript*, p. 482.

185 ATO, *Submissions*, p. S333.

4.4.2 The Attorney-General's Department, claims that 'the legitimate needs of the Commonwealth in dealing with law enforcement and fraud control are frequently frustrated by secrecy provisions which prohibit the transfer of relevant information between agencies for legitimate purposes.'[186] The Department points out that many provisions denote the Commonwealth as a collection of discrete departments and not as a single legal entity. As personal information might only be disclosed to one department, other departments cannot receive that information and this may impede the Commonwealth's ability to perform its functions.

4.4.3 The DSS also argued that secrecy provisions in legislation can impede the flow of information which is being sought either for the determination of the payment of correct entitlements or to protect public revenues.[187] The DSS has received many requests for information from other Commonwealth agencies which it may not lawfully provide and cites the following examples:

- DEET would like access to a greater range of information related to overpayment and debt collection purposes for payments made by DEET; and
- State police forces have made numerous complaints both to DSS and the Minister for Social Security about difficulties in obtaining information about missing or dead persons. The Public Interest Guidelines of the Social Security Act permit only limited transfer of information to the police in cases where murder or assault is involved.[188]

4.4.4 The Attorney-General's Department considers that secrecy provisions, which were originally developed to prevent the disclosure of sensitive government information to the public, are not well suited to regulating the exchange of sensitive information between agencies and should not be used for this purpose.[189] It claims they are too inflexible to deal with changing government needs for the legitimate transfer of information and comments that in recent years amendments have been necessary to tax, health and social security legislation to meet changing needs in this area. The Attorney-General's Department suggests that performance standards should govern the flow of information between agencies, and that secrecy provisions should govern the flow of information from agencies to the public.

4.4.5 A solution, proposed by the Attorney-General's Department, is that third party information should only be transferred where the head of the disclosing agency is satisfied

186 Attorney-General's Department, *Submissions*, p. S381.

187 DSS, *Submissions*, p. S444.

188 DSS, *Submissions*, p. S444.

189 Attorney-General's Department, *Submissions*, pp. S381–S382.

that the information will assist the receiving agency in performing its functions or exercising its powers.[190] The Department also suggested that, although secrecy provisions would no longer prevent the legitimate transfer of third party information, transfers should be conducted in accordance with established procedures – the Privacy Act being a useful benchmark.[191] The application of the Privacy Act would ensure that agencies only collected such information where it was relevant for their purposes and that they complied with principles relevant to disclosure. The Privacy Commissioner should be able to inspect records of transfers to ensure that established procedures were followed.

4.4.6 Other evidence was also critical of the use of secrecy provisions for transfers between agencies. Professor Gregory Tucker commented that there has been no consistent approach to secrecy provisions and they are not uniform in their application.[192] The DEET did not support a wide range of secrecy provisions in individual enactments.[193] The ALRC report on privacy also revealed doubts about claims that information suppliers are reassured by the protection offered by secrecy provisions.[194]

4.5 Greater reliance on the Privacy Act

4.5.1 The Committee considers that secrecy provisions have failed to meet adequately the need for flexible regulation of the transfer of information between Commonwealth agencies. It is also difficult to incorporate appropriate privacy protection safeguards in secrecy provisions.

4.5.2 In contrast, the Privacy Act is structured so that it can to regulate the information handling practices of Commonwealth agencies. The Privacy Commissioner considers that agencies now rely on provisions in the Privacy Act to refuse to disclose information in the same way that in the past, agencies relied on secrecy provisions.[195] He suggested that agencies 'blamed' the Privacy Act when they did not want to release information.

---

190 *Submissions*, p. S382.

191 ibid., p. S383.

192 Tucker, *Submissions*, p. S762.

193 DEET, *Submissions*, p. S929.

194 The Law Reform Commission, *Privacy*, ALRC 22, AGPS Canberra 1983.

195 Mr Kevin O'Connor, *Transcript*, p. 482.

4.5.3 The Committee considers that it is unfortunate that the Privacy Act is relied upon as a means to avoid cooperation in otherwise authorised transfers. The Privacy Act should be used as the primary means to regulate the flow of confidential personal information between government agencies, and not to prevent it. The Privacy Act offers greater flexibility than secrecy provisions and incorporates adequate privacy protection safeguards. Moreover, it is significant that both the Privacy Commissioner and the agencies seeking transfers agree that the philosophy underpinning the Act is correct, even if the interpretation of the IPPs is not agreed.

Recommendation 17
The Committee recommends that transfers of confidential personal information between Commonwealth Government agencies should be regulated by the *Privacy Act 1988*, rather than by the by the secrecy provisions in specific statutes. The Privacy Act should be reviewed and amended to ensure that the necessary degree of protection for transferred information is maintained.

Recommendation 18
The Committee further recommends that each Commonwealth Government agency keep a record of authorised transfers of confidential personal information between agencies for the purpose of checking the legitimacy of access to such information. The record should include the names of individuals and organisations about whom information is transferred, the names of individuals and organisations to whom that transfer is made, and the date of the transfer.

4.5.4 It should be noted that other recommendations will also strengthen the Privacy Act.

4.5.5 There appears to be considerable uncertainty about the interpretation of the IPPs. This is significant given the importance of the IPPs. Even if the role of the Privacy Act is not expanded to become the primary means for effecting transfers between agencies, improvements to the IPPs should be given a high priority.

4.6 Need for clarification of the Information Privacy Principles

4.6.1 The Privacy Commissioner says that IPPs 10 and 11 set a weak minimum standard for confidentiality that is largely inadequate.[196] He considers their language to be 'vague and loose', which has resulted in conflict because of differing interpretations by the Privacy Commissioner and by agencies with responsibilities for fraud control, revenue protection and law enforcement. This view is supported by Professor Gregory Tucker who commented that IPPs 10 and 11 suffer from ambiguities which can lead to various interpretations.[197]

4.6.2 In particular, the Privacy Commissioner has highlighted the need to clarify the relationship between the Privacy Act and other legislation containing secrecy provisions. He has adopted the practice that where another statute deals expressly with permissible uses and disclosures of information, the IPP's 10 and 11 should not be seen as providing additional grounds for disclosure.[198] The DPP considers that the principle underlying IPP 11.1(e) strikes a proper balance between competing interests. However, it holds the view that it is a problem that IPP 11.1(e) does not override the specific secrecy provisions in other Acts because they prevent the exchange of information even if there are valid law enforcement reasons for such an exchange.[199]

4.6.3 The Committee agrees that where specific legislation contains express secrecy provisions the Privacy Act should not be used to expand the access that is otherwise permissible. To do so would undermine the protections expressly provided by the secrecy provisions and would allow a distortion of the protective purpose of the Privacy Act.

4.6.4 The Committee agrees with the Privacy Commissioner's views that where other Acts specifically address disclosure or protection of information, the IPPs should not be used to provide additional grounds for disclosure. This aspect of the relationship between the IPPs and secrecy provisions should be addressed in the Privacy Act.

> *Recommendation 19*
> The Committee recommends that the *Privacy Act 1988* be amended to provide that where an Act other than the Privacy Act deals expressly with a matter of permissible use and disclosure, Information Privacy Principles 10 and 11 do not operate to provide additional grounds for disclosure.

196 Privacy Commissioner, *Submissions*, p. S567.

197 Professor G. Tucker, *Submissions*, p. S762.

198 Privacy Commissioner, *Submissions*, pp. S572–S573.

199 DPP, *Submissions*, p. S29.

4.7 Disclosure authorised by law – exceptions 10.1(c) and 11.1(d)

4.7.1 Under IPPs 10.1(c) and 11.1(d) use and disclosure of personal information are permitted where it is 'required or authorised by or under law'. This exception allows for the operation of numerous public interest exceptions found in other legislation. The Privacy Commissioner argued that the exceptions in other legislation may not reflect contemporary information privacy concerns and may need review in light of the policy intention of privacy legislation.[200]

4.7.2 The Privacy Commissioner further considers that this wording means IPPs 10.1(c) and 11.1(d) are susceptible to broad interpretation.[201] At the extreme, it could be argued that any lawful action by an agency must be 'authorised by law', in which case IPPs 10 and 11 would have no effect. The Privacy Commissioner suggests that this problem could be overcome by providing that only a specific requirement or authorisation dealing expressly with the disclosure practice in issue should constitute an exemption from IPPs 10 and 11.

4.7.3 Professor Tucker also favours a narrow interpretation of these provisions because he argues that disclosure should only be available where there is clear language to support it.[202]

4.8 Disclosure is reasonably necessary – exceptions 10.1(d) and 11.1(e)

4.8.1 Under IPPs 10.1(d) and 11.1(e) use and disclosure of personal information are permitted where it is 'reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.' The Privacy Commissioner considers that applying a test of 'reasonable necessity', indicates that any disclosures should be able to be strictly justified.[203] Mr O'Connor told the Committee that agencies involved in revenue protection and law enforcement areas have taken the most liberal view possible of what is meant by reasonably necessary.[204] In particular he was concerned that:

---

200 *Submissions*, p. S572.

201 Privacy Commissioner, *Submissions*, p. S572.

202 Professor G. Tucker, *Submissions*, p. S762.

203 Privacy Commissioner, *Submissions*, p. S569.

204 *Transcript*, p. 481.

> This exception seems to be being interpreted by Commonwealth administration as sufficient to provide a legal justification for any program for data-exchange, data-matching or the like which is considered to have value in identifying law-breakers or people whose conduct may be injurious to the public revenue. The following steps in thinking seem to be involved in reaching this view of exception (e):
>
> * the exception allows for bulk disclosure of data about individuals including entire databases held by agencies;
>
> * whether a disclosure practice is "reasonably necessary" can be decided simply by reference to any current policy position on the use of information held in the administration;
>
> * the term "public revenue" should be expansively interpreted to allow within the scope of the exception any information disclosure practice which, if successful in identifying misconduct, might produce a saving to revenue.[205]

4.8.2 The Privacy Commissioner considers that as a general rule 11.1(e) should only be used in situations where there is a prior suspicion that an offence has been committed. The Attorney-General's Department has stated that the interpretation of exception (e) to IPP 11 by the Privacy Commissioner and other agencies has placed a strong emphasis on privacy interests.[206] The Department considers that the 'reality of Commonwealth criminal law enforcement and administration' requires that a case by case approach be taken in determining what disclosure or use is reasonable in the circumstances. It argues further that the prior suspicion test is not applicable to Commonwealth criminal law enforcement.[207] The AFP considers that the Privacy Commissioner has a restrictive interpretation of 11.1(e) which has hindered its ability to investigate matters and is not consistent with preventative pro-active law enforcement strategies.[208] Nevertheless, it has interpreted the provision to mean that disclosures may be made for criminal intelligence purposes and ascertaining whether criminal activity is occurring in certain areas.[209]

4.8.3 The DPP claims the Privacy Commissioner is of the view that this exception can only apply if there is 'virtual certainty' that the disclosure will advance an existing investigation. It can see no reason why the provision should be interpreted so narrowly.[210] Not surprisingly, perhaps, the NCA is also in favour of a broader interpretation.[211]

---

205 Privacy Commissioner, *Submissions*, p. S570.

206 Attorney-General's Department, *Submissions*, p. S384.

207 Attorney-General's Department, *Submissions*, p. S384.

208 *Transcript*, p. 312.

209 AFP, *Submissions*, p. S71.

210 DPP, *Submissions*, p. S30.

211 NCA, *Submissions*, p. S268.

4.8.4 The Privacy Commissioner proposed that more specific exceptions could help to overcome the present difficulties of interpretation.[212] He points to privacy legislation in Canada as a possible model for more specific and numerous exceptions. It has flexibility because it also provides for agencies to exercise a public interest discretion. The Privacy Commissioner also refers to comments by the Royal Canadian Mounted Police that there is no evidence that this legislation has had any negative effect on police operations.

4.8.5 Notwithstanding the Committee's support for the wider meaning of the expression 'protection of the public revenue', the Committee considers it would make the IPPs meaningless to be subject to broad interpretation. The uncertainty that is created by these differences and difficulties with the interpretation of the IPPs, inhibits in a real sense the legitimate transfer of information between agencies. The Committee notes that the Canadian privacy legislation appears to operate without the difficulties of interpretation raised here, with more specific and numerous exceptions. The Committee agrees with the Privacy Commissioner that clarification of the matter is essential and that the language of these exceptions should be more specific not in the least because exception (e) is relied upon to permit data-matching.

Recommendation 20
The Committee recommends that as part of the review of the scope of the *Privacy Act 1988*, that the exceptions in Information Privacy Principles 10 and 11 should be more specific.

4.8.6 With regard to the specific term 'public revenue', the Attorney-General's Department considers that it is a term that is broad enough to cover moneys paid to as well as received by the Commonwealth.[213]

4.8.7 The Committee notes the Attorney-General's Department's concerns that the Privacy Commissioner doubted whether 'protection of the public revenue' included both express revenue as well as expenditure matters.[214] The Committee supports the interpretation of the Attorney-General's Department that based on judicial interpretation of the term 'revenue', it is not limited to incoming moneys from taxation. The Committee

212 Privacy Commissioner, *Submissions*, pp. S571–S572.

213 *Submissions*, p. S386.

214 Attorney-General's Department, *Submissions*, p. S386.

believes the Privacy Act should be amended to clarify the meaning of the expression 'protection of the public revenue'.

> *Recommendation 21*
> The Committee recommends that the *Privacy Act 1988* be amended to clarify the meaning of the term 'protection of the public revenue'.

4.9 Providing for express transfers

4.9.1 The Department of Veterans Affairs referred to one example where a desirable transfer of information was inhibited by the existing legislation.[215] In that case, the secrecy provisions of the *Health Insurance Act* inhibited the ability of that Department to cross-check records of the Health Insurance Commission against those of the department to detect practitioners billing both Medicare and the Repatriation Commission for the same health services.

4.9.2 Where the law is amended in such a case, there is little doubt as to the intended scope of the provisions. The Committee considers that it is appropriate that clarification occurs through legislation when the ability of an agency to transfer third party information is affected.

> *Recommendation 22*
> The Committee recommends that permitted transfers of confidential third party information between Commonwealth Government agencies be accommodated by way of exceptions to the Information Privacy Principles.

4.9.3 The Committee notes that the Public Service Commission has stated that it has experienced difficulties arising out of the application of the Privacy Act to its work as a central personnel policy agency. It complains that compliance with the Privacy Act limits its access to the personnel records on staff of the Australian Public Service held by the Department of Finance. Where an agency seeks to refer case histories or files to the PSC for advice there is potential for breach of the Privacy Act because it would not have been contemplated at the time of the making of these documents that they would be referred

215 Department of Veterans' Affairs, *Submissions*, p. S640.

to the PSC. It argues that the referral of such matters to it is a legitimate use of the information and that in such cases mechanisms should not be imposed to prevent disclosure.[216]

4.9.4 While the Committee is not persuaded by that there is sufficient evidence on the matter for it to recommend that the PSC be given access by was of an exemption to the IPPs, it may be possible for the PSC to raise its concerns when the exemptions to the Privacy Act are being clarified.

4.10 Controls on data-matching

4.10.1 One particularly important matter in the computing environment is data-matching. Although the Privacy Act does not regulate data-matching programs, the *Data-matching Program (Assistance and Tax) Act 1990* contains specific controls for data-matching activities that involve the use of tax file numbers. The Privacy Commissioner has issued guidelines under section 17 of the Privacy Act which are intended to protect the privacy of the individual by restricting the use of tax file number information. Compliance with these guidelines is mandatory.

4.10.2 There are also data-matching programs that do not involve the use of tax file numbers. Many of these programs are initiated and carried out at the discretion of the agencies concerned often in reliance on IPP 11.1(e). The Privacy Act does not specifically regulate these data-matching programs, although the Privacy Commissioner has issued data-matching guidelines under section 27(1)(e) of the Privacy Act. Compliance with these guidelines is voluntary.

4.10.3 In 1994 the Privacy Commissioner reviewed and reported on the voluntary data-matching guidelines including ways of defining the scope of programs to target more precisely those that have serious implications for privacy. The review targeted those programs which compare the information held on different databases to identify instances where there is a particular correlation or discrepancy between the information about an individual from different sources.[217]

4.10.4 The Privacy Commissioner has found that although a large number of agencies has agreed to comply with the guidelines on a voluntary basis, only two agencies have

---

216 PSC, *Submissions*, p. S544.

217 Privacy Commissioner, *Submissions*, p. S1069.

prepared appropriate documentation for the data-matching programs that they are conducting. By contrast, he found that responses to statutory obligations under the Data-matching Program Act have been prompt and rigorous. He concluded that agencies are less likely to give priority to meeting a voluntary requirement and considered this to be a weakness because it hinders the achievement of a uniform standard for Commonwealth data-matching activities. He recommended that uniform controls for data-matching carried out by Commonwealth agencies should be incorporated into the Privacy Act and thereby made a legal obligation.[218]

4.10.5 Clearly the Attorney-General's Department is not alone in saying that effective detection of possible fraudulent or criminal activity requires extensive matching and comparison of third party information.[219] For this to continue however, there must be appropriate safeguards.

4.10.6 The Committee supports the Privacy Commissioner's call for uniform controls on data-matching by Commonwealth agencies. It considers that the nature of data-matching means that the scope for accessing information is such that consistent high standards of control need to be applied. Data-matching, other than tax file data-matching, should be governed by statutory guidelines incorporated into the Privacy Act, rather than voluntary guidelines as is now the case.

> *Recommendation 23*
> The Committee recommends that uniform controls for data-matching carried out by Commonwealth Government agencies be made a legal obligation and incorporated into the *Privacy Act 1988*.

4.10.7 The Privacy Commissioner also argued that major data-matching programs should be specifically authorised by legislation. The Committee agrees that because data-matching enables confidential personal information about a large number of individuals to be cross-referenced that major data-matching programs should be specifically authorised. Given the safeguards provided for in other recommendations, the Committee considers it would be appropriate for a clearly identified senior manager to authorise an agency's major data-matching programs.

---

218 Privacy Commissioner, *Submissions*, p. S1070.

219 Attorney-General's Department, *Submissions*, p. S385.

Recommendation 24
The Committee further recommends that major data-matching programs proceed with the authority of a clearly identified senior executive service officer who is, where practicable, at a level no lower than SES Band 2.

4.11 Use of information that involves disclosure

4.11.1 The Privacy Commissioner identified as a problem, those situations where the use of information for its original purpose involves disclosure.[220] There are two possible arrangements which would be reasonable but which are not addressed by the IPPs. One is where an agency enters a contract for tasks such as data-processing or mailing. The other is where an agency becomes involved in a program for which information has previously been collected.

4.11.2 The Privacy Commissioner cautions that provisions to overcome possible problems should not be used to circumvent notification and consent provisions. He suggests that a discretion to permit disclosure should be subject to:

- the necessity of the disclosure;
- the disclosure being an integral part of the use for which the information was obtained; and
- notification or consent procedures being demonstrably inappropriate.[221]

4.11.3 The Committee agrees that the arrangements of the kind described by the Privacy Commissioner are within the realm of an agency's routine operations. It would be an unnecessary burden on administration if the disclosure of information in such circumstances were to be inhibited. The Committee notes the Privacy Commissioner's concerns that an exemption for such disclosures should not be abused. Accordingly, the Committee agrees that a discretion to permit such disclosures should be provided in the terms suggested by the Privacy Commissioner, and that it be subject to the scrutiny of the Privacy Commissioner.

220 Privacy Commissioner, *Submissions*, pp. S578–S579.

221 Privacy Commissioner, *Submissions*, p. S579.

Recommendation 25
The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information held by the agency where notification of or consent for disclosure is not a reasonable possibility. This discretion is to be subject to:

- the necessity of the disclosure;
- the disclosure being an integral part of the use for which the information was obtained; and
- notification or consent procedures being demonstrably inappropriate.

Recommendation 26
The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner.

4.12 Disclosures in the individual's interest

4.12.1 The Privacy Commissioner also indicated that there were situations where it was in the interests of an individual for disclosure to be made, but IPP 11 prevented it because the individual's consent could not be obtained.[222] An example of where this would be a problem is where a public trustee is seeking to locate an individual to notify her or him of a bequest. IPP 11 prevents Commonwealth agencies disclosing information to the trustee to assist in locating the individual unless consent is obtained, which may not be possible. The Privacy Commissioner suggested that a limited discretion should be provided for to permit disclosure of information when it would be in the interest of the individual concerned to do so and consent could not be obtained.

4.12.2 The Committee agrees that in some limited circumstances it would be desirable to permit disclosure of confidential personal information where consent could not be obtained. The Committee considers that in any case where such discretion is exercised the decision by the agency head should be subject to the scrutiny of the Privacy Commissioner.

222 Privacy Commissioner, *Submissions*, p. S579.

Recommendation 27
The Committee recommends that agency heads be provided with a discretion to permit disclosure of confidential personal information where a disclosure is clearly in the individual's interest and consent could not be obtained.

Recommendation 28
The Committee further recommends that agencies be required to report, within 14 days of the disclosure, all such exercises of that discretion to the Privacy Commissioner.

4.12.3 Finally, in terms of the legislative structure for effecting transfers of information, two remaining proposals will be dealt with in this chapter, although the Committee does not make further recommendations.

4.13 No licensing system for data users

4.13.1 The Victorian Council for Civil Liberties (VCCL) has proposed that a licensing system for all dealings in confidential personal information be introduced.[223] Under the proposed system all authorised users of confidential personal data held by the Commonwealth would be required to be licensed and supervised by the Privacy Commissioner. The VCCL argued that a licensing system would be the most effective means of identification of users and providing for scrutiny by the Privacy Commissioner.

4.13.2 Dr Gordon Hughes, a solicitor with expertise in data protection, told the Committee that based on his knowledge of such an approach in England, that he thought licensing would cause resentment and would not be completely effective.[224] Like Dr Hughes, Mr Kevin O'Connor, the Privacy Commissioner, said that based on his knowledge of other licensing systems including the English one, he considered that the licensing proposal would not be an effective use of resources and would expand the bureaucracy unnecessarily.[225]

---

223 VCCL, *Submissions*, p. S155–S156.

224 *Transcript*, p. 413.

225 *Transcript*, pp. 485–486.

4.13.3 The Committee is not persuaded by the evidence that a licensing system would lead to improvements in the way authorised disclosures of confidential third party information are managed. Consequently, it does not support the suggestion for a licensing system of users of confidential personal information.

4.14 A special relationship between the Privacy Act and the FOI Act

4.14.1 Mrs Loane Skene, one time Principal Research Officer with the now defunct Victorian Law Reform Commission, suggested that the Privacy Act and the FOI Act be amalgamated.[226] Mrs Skene argued that such an amalgamation would provide for greater administrative efficiency and cost-effectiveness.

4.14.2 The Attorney-General's Department however, does not believe that an amalgamation of the two Acts would result in an improvement of the public's rights relating to personal information. It lists six reasons for arguing against amalgamation.[227]

4.14.3 The first reason is that the resulting amalgamated Act is likely to be extremely large and convoluted, which could result in further complications for institutions and individuals relying on it. The second reason is that amalgamation will not necessarily enable those relying on the Act to understand the way in which the issues of privacy and access to information complement rather than conflict with each other.

4.14.4 The third reason is that because the roles of the two Acts are substantially different, their amalgamation would lead to confusion and unnecessary complexity. The fourth reason is that the roles of the Privacy Commissioner and the AAT might become difficult to define. The fifth reason is that the FOI Act applies to a broader scope of information than the Privacy Act. The sixth reason is that the rights of review are different under each Act and if they co-existed in the one Act might be confusing.

4.14.5 A review of the Freedom of Information Act is being conducted jointly by the Australian Law Reform Commission and the Administrative Review Council. The Privacy Commissioner advised the Committee that in the context of that inquiry, he proposed that the rights of access and correction to one's own personal information under the Privacy Act and the FOI Act should be aligned so that there is consistency in the way those rights are framed. The Committee considers this suggestion by the Privacy Commissioner to be reasonable and sensible.

---

226 L. Skene, *Submissions*, p. S549.

227 Attorney-General's Department, *Submissions*, p. S1039–S1040.

4.14.6 The Committee notes that the review of the FOI Act has suggested that the two Acts, together with the Archives Act, should be combined into a single Act.[228] The Committee notes that both these Acts govern information access however, the Committee is not persuaded by arguments before it that the FOI Act and the Privacy Act should be combined into a single Act. As there is already a broad review of the FOI Act at present underway by the ALRC and the ARC the Committee thinks it would be appropriate for this matter to be resolved in that context.

228 ALRC & ARC, *Freedom of information*, Discussion Paper 59, ALRC DP 59, May 1995, p. 132.

Chapter 5

Sanctions and penalties for public servants who wrongly disclose information

This chapter examines the administrative sanctions and criminal penalties that can be applied to public service officers who wrongfully disclose confidential third party information. The Committee outlines those sanctions and penalties which apply to members of the Australian Public Service as well those which apply to members of the Australian Defence Force and employees of some government business enterprises.

The adequacy of the criminal penalties and the secrecy provisions themselves are interrelated. The Committee outlines the problems with the relevant secrecy provisions in the Crimes Act 1914 and the secrecy provisions in the specific statutes. It considers that there is a need for a more consistent approach to protect confidential third party information from disclosure. Terms of reference (c), (d) and (e) are interrelated and recommendations arising from this and the following two chapters are located at the end of chapter 7.

5.1 Introduction

5.1.1 This chapter deals with term of reference (c), that is, the adequacy of the penalties and administrative sanctions which can be applied to officers who wrongly disclose third party information. The nature of the relevant sanctions and penalties are outlined and then the adequacy of these sanctions and penalties are assessed. Some criticisms of the general and specific secrecy provisions are made.

5.1.2 Terms of reference (d) and (e) are closely related to the issues raised in this chapter. Chapter six addresses the adequacy of penalties which can be applied to persons who procure the wrongful disclosure of third party information. Chapter seven considers the application of the criminal law to these matters and whether the application of a general criminal law (rather than the inclusion of criminal provisions in specific statutes) is desirable. The Committee's recommendations in relation to the three terms of reference are at the end of chapter seven. Consequently, it is useful to consider the three chapters together.

5.2 Relevant administrative sanctions

5.2.1 The administrative sanctions relevant to the wrongful disclosure of third party information are contained in the *Public Service Act 1922*. The disciplinary code in the

Public Service Act establishes a system for managing occurrences of misconduct and it provides a mechanism for correcting any misconduct. The emphasis of the code is on correction and not punishment.[229]

5.2.2 Two Public Service Regulations are relevant in this context, namely regulation 8A and regulation 35[230]. Regulation 8A sets out the standards with which public servants are expected to comply. Regulation 35 prohibits the disclosure of information by a Commonwealth officer except in the course of her or his duties. Regulation 35 provides:

> Except in the course of official duty, no information concerning public business or any matter of which an officer or employee has knowledge officially shall be given, directly or indirectly, nor shall the contents of official letters be disclosed, by an officer or employee without the express authority of the Chief Officer.

5.2.3 The combined effect of those regulations is that the unauthorised disclosure of most confidential third party information by a public servant will attract the disciplinary measures contained in the Public Service Act.[231] Subsection 62(6) of the Act details the disciplinary measures which include admonition, deduction of a sum not exceeding $500 from salary, transfer, reducing salary to a lower point in the same salary range, demotion, dismissal or a combination of these measures. It is also possible to take disciplinary action under the Public Service Act in tandem with criminal charges.[232]

5.2.4 The link between the criminal law and administrative sanctions in the Public Service Act should be noted. Subsection 63(1) of the Public Service Act provides that where an officer is found guilty of a criminal offence, the Secretary of that officer's employing department may direct that the officer be transferred, demoted or dismissed if it is the Secretary's opinion that such action is justified in the interests of the Public Service. In making a decision as to whether to take such action, the Secretary should have regard to the nature and seriousness of the offence, the circumstances and the nature of the officer's duties.[233]

5.2.5 An issue on which the Committee received some evidence was the possible need for review of regulation 35. The Public Service Commission (PSC) submitted that this regulation is somewhat out of date. The PSC suggested that it may be preferable to

---

229 PSC, *Submissions*, p. S542.

230 See also Chapter 2. Regulation 8A is set out at 2.2.4.

231 Attorney-General's Department, *Submissions*, p. S367. Note that subparagraph 56(f)(i) provides that a Public Servant has failed to fulfil his or her duty as an officer if he or she fails to comply with the regulations.

232 See PSC, *Submissions*, p. S541.

233 Attorney-General's Department, *Submissions*, p. S387.

frame the regulation so that it specifically protects the disclosure of third party information (as opposed to the current regulation which effectively prohibits the disclosure of all government-held information).[234] Professor Finn was also critical of regulation 35. He suggested that it:

> is unacceptably broad in its coverage; is unambiguous in its terms; sits ill beside the policies of FOI legislation and of the common law and is in urgent need of reformation.[235]

5.2.6 He also considered that the regulation is manifestly unsuited to the modern circumstances of the Commonwealth Government.[236]

5.2.7 The Committee notes the criticisms of regulation 35 that have been expressed. The Public Service regulations will need to be reviewed in light of the current redrafting of the Public Service Act and the Committee suggests that this issue should be considered in that context.

5.3 The adequacy of relevant administrative sanctions

5.3.1 In considering the adequacy of the relevant administrative sanctions, the Committee will address three issues. Those issues are the range of sanctions available under the Public Service Act; consistency in the application of sanctions and the persons to whom these sanctions apply. The Committee will also briefly refer to the recommendations of the Public Service Act Review Group.

a) Range of sanctions

5.3.2 It was the view of the Attorney-General's Department that the range of sanctions was adequate for cases where disciplinary measures rather than criminal penalties are appropriate.[237] The Department's submission noted that while consistency in the application of disciplinary sanctions is desirable, it is also important to provide a wide range of penalties to suit all circumstances[238] because the unauthorised disclosure of

---

234 *Submissions*, p. S998.

235 Finn P., *Official Information*, Integrity in Government Project: Interim Report 1, Australian National University, Canberra, 1991, p. 178.

236 ibid.

237 Attorney-General's Department, *Submissions*, p. S387.. See also Australian Bankers' Association, *Submissions*, p. S821.

238 ibid.

third party information can take a variety of forms. At one end of the spectrum, the conduct may be relatively innocuous. However, at the other end, the disclosure may be deliberate and highly intrusive and therefore deserving of strict measures, such as demotion or dismissal.[239] The Director of Public Prosecutions (DPP) noted that it has no role in the enforcement of administrative sanctions and agreed that the range of administrative sanctions are adequate.

5.3.3 The Department of Social Security (DSS) informed the Committee that it had recommended in a submission to the Public Service Commission[240] that the discipline provisions in the Public Service Act be amended to make it a real disincentive to disclose information to third parties.[241] The Department recommended that there should be mandatory dismissal for serious offences, for example, disclosing information to third parties in specified circumstances. It was also suggested that the penalties under the current disciplinary options were too limited. DSS noted that reduction of salary or transfer to a lower position cannot be applied to staff at or near the bottom of a salary range. DSS also noted that the maximum fine of $500 is not a significant amount and that figure has remained unchanged for many years.[242]

5.3.4 The PSC disagreed with the DSS view on the adequacy of the penalties in the Public Service Act. The Commission's view is that the range of sanctions in the Act is sufficiently wide to assist in correcting behaviour. The Commission submitted that a wider range of penalties would not accord with the philosophy of the disciplinary code. It noted that the code is not constructed to enable the imposition of punishment appropriate to a criminal offence and that all of the sanctions, apart from the fine, are administrative in character. According to the Commission, the imposition of the maximum fine of $500 would indicate the seriousness of the relevant misconduct.[243]

5.3.5 The Privacy Commissioner suggested that there is too broad a discrepancy in sanctions between the maximum fine available and dismissal. In his 1989-1990 Annual Report the Commissioner noted that faced with the choice of the maximum fine or dismissal, it is not surprising that tribunals err on the side of a fine. He also suggested

---

239 ibid. See also DPP, *Submissions*, p. S1074.

240 In 1991 the PSC began a review of existing disciplinary measures under the Public Service Act. This review was not completed. In 1992 DSS informed the Committee that it understood the Commission had decided to pursue longer term approaches rather than pursue a review of discipline provisions (see *Submissions*, p. S446).

241 ibid.

242 ibid.

243 PSC, *Submissions*, p. S542.

that a wider range of penalties would assist in avoiding the impression that corrupt disclosure is not dealt with strongly.[244]

5.3.6 The PSC addressed this criticism, commenting that the range of sanctions available are not intended to be a range of 'punishments to fit the crime.'[245] The Commission commented that while a decision to dismiss an officer for misconduct is often overturned on appeal, the appeal committee usually takes this action on the basis that a second chance is warranted. It was submitted that dismissal, even if overturned on appeal, is a clear message that the officer's misconduct is regarded very seriously by the department involved. The mechanism gives officers a second chance and it is usually clear that further misconduct will result in dismissal.[246] The Commission considered that an increase in the current maximum fine would be a sanction which would not fit the objectives of the disciplinary code.[247]

b) Consistency and delay in the application of sanctions

5.3.7 Formal disciplinary action in the APS is not centrally administered or coordinated, and departmental secretaries are responsible for discipline in their individual departments.[248]

5.3.8 DSS indicated that it was concerned about the consistency of disciplinary decisions and noted that there are long delays in finalising cases.[249] The ANAO agreed with DSS and stated that the existing mechanisms to process disciplinary matters are slower than necessary and '... do not adequately support management initiatives to deal with inefficient officers or those who seek to avoid or delay management action by invoking other provisions'.[250]

5.3.9 The DPP queried whether the appropriate sanctions are always applied in practice. The office commented that 'it is our impression, based on anecdotal evidence, that appropriate sanctions are often not applied'.[251] The DPP suggested that central supervision of the administration of disciplinary proceedings by Commonwealth agencies may be appropriate.[252] However, when discussing this issue later in a public hearing,

---

244 *Second Annual Report on the Operation of the Privacy Act*, PP 21/1991, p. 16.
245 *Submissions*, p. S542.
246 ibid.
247 ibid.
248 See PSC, *Submissions*, p. S996.
249 *Submissions*, p. S446.
250 *Submissions*, p. S141.
251 DPP, *Submissions*, p. S30.
252 ibid.

a DPP officer indicated that the DPP had recanted from that position. The officer stated that although the idea of a centralised agency for disciplinary proceedings has some merit and force, the suggestion that disciplinary treatment is not necessarily identical in all regions is based on anecdotal evidence only.[253]

5.3.10 In commenting on the perceived inconsistency in administrative sanctions, the PSC submitted that in an environment where responsibility for disciplinary matters lies with Secretaries, there may be some disparity between departments in the application of sanctions.[254]

5.3.11 It was noted that the culture of each organisation is a significant variable in any discussion concerning consistency in the application of administrative sanctions. Increased emphasis may be placed on the security of third party information in some departments than others because of the nature of a department's operations. For example, as officers of some departments are subject to legislation which imposes criminal sanctions on the disclosure of particular information, it may be expected that stronger disciplinary action would be taken against those officers than officers in other departments[255] where penal sanctions do not exist.

5.3.12 The PSC suggested that a sanction regime will have achieved its purpose if it deters misconduct, corrects misconduct when it occurs and works to minimise or eliminate further occurrences.[256]

c) Persons to whom sanctions apply

5.3.13 The disciplinary code only applies to persons employed under the Public Service Act while they continue to be employed under that Act. The sanctions do not apply to private individuals who may have access to third party information held by the Commonwealth or those who unlawfully obtain such access.[257]

5.3.14 The strongest sanction under the code is dismissal. Once an officer ceases to be employed in the Public Service, he or she is beyond the reach of the disciplinary provisions. Consequently, the disciplinary provisions do not apply to persons who have retired from the public service or who resign when investigations commence.[258]

---

253 *Transcript*, p. 349.

254 PSC, *Submissions*, p. S543.

255 ibid.

256 ibid.

257 Attorney-General's Department, *Submissions*, p. S396.

258 ibid.

5.3.15 The PSC claimed that where an officer resigns before a notice of dismissal for misconduct has taken effect, the action proposed by the Department will have been pre-empted rather than frustrated because, in both situations, the officer ceases to be employed in the Public Service.[259] Officers who have resigned are still be subject to the criminal prohibition against disclosure of information by former Commonwealth officers in subsection 70(2) of the *Crimes Act 1914.*

5.3.16 The PSC suggested that if the broad provisions of the Crimes Act were removed, there may be opportunities for officers to resign so as to escape any sanction. Consequently, the PSC noted that if the broad provisions were removed, there may need to be a new statutory provision relating to the use of third party information because the disciplinary provisions would not provide comprehensive coverage.[260]

5.3.17 The disciplinary provisions in the Public Service Act do not cover major categories of employees in Commonwealth authorities and the defence forces. The disciplinary provisions relevant to the employees of Commonwealth authorities vary greatly. The various authorities are responsible for administering the provisions themselves and the PSC has no central record of the disciplinary provisions relevant to each authority. The provisions relevant to some authorities mirror those of the Public Service Act; others do not. The relevant provisions of some authorities are located in the authority's enabling legislation while others are located in industry awards. Where the disciplinary provisions are located in enabling legislation, some Acts provide that when the enabling Act is silent on a particular issue, the provisions of the Public Service Act apply.

5.3.18 Employees of the government business enterprise (GBE)[261], Australia Post, are subject to secrecy provisions. The *Australian Postal Corporation Act 1989* prohibits current employees from using or disclosing information or documents acquired in the course of employment, except in specified circumstances[262]. The categories of information and documents to which the prohibition applies include where the information or document relates to the affairs or personal particulars (including name

---

259 *Submissions*, pp. S543–S544.

260 ibid.

261 A recent report of the Administrative Review Council identifies three characteristics that can be used to identify GBEs. Those characteristics are that the enterprise is under Government control, is principally involved in commercial activities and is a legal personality separate to a government department (ARC, *Government Business Enterprises and Commonwealth Administrative Law*, Report No. 38, Commonwealth of Australia, 1995, see pp. 5-7). Schedule 3 of the Legislative Instruments Bill 1995 lists GBEs as including the Australian Postal Corporation and Telstra Corporation (see *ARC Report*, p. 6).

262 Subsection 90H(2) of the Australian Postal Corporation Act.

or address) of another person. Breach of the prohibition can attract disciplinary or criminal sanctions depending on the circumstances. Under Australia Post's internal disciplinary procedures, there are a range of administrative penalties including counselling, a fine of up to $500, reduction in classification and dismissal.[263]

5.3.19 Public servants employed by the Department of Defence (DOD) are subject to the Public Service Act. Members of the Australian Defence Force (ADF) are not employed under the Public Service Act but they are subject to administrative sanctions if they are found to have wrongfully disclosed third party information. DOD holds commercially sensitive information including tenders, quotations, contracts, cost records as well as financial, technical and commercial information provided by tenderers and contractors.[264] The personal information held by DOD includes medical details and disciplinary records of defence personnel, as well as the personnel records of public servants employed by DOD. DOD informed the Committee that there are strict regulations governing the transmission of personal information.[265] For example, Australian Military Regulation 770 (which applies to the Army) prescribes to whom, and the circumstances under which, personal information may be disclosed.[266]

5.3.20 Defence Instruction General (08-1) provides that a member of the ADF is not to make public comment or disseminate information which is protected by a security classification or in-confidence or other privacy marking.[267] This instruction would appear to apply to the disclosure of both personal and commercial information. Failure to comply with a defence instruction can also result in a criminal charge.[268]

5.3.21 There are a range of punishments that can be imposed by a service tribunal. These punishments include criminal penalties as well as administrative measures such as a reduction in rank, forfeiture of service for the purposes of promotion, forfeiture of seniority, a fine (not exceeding 28 days pay where the convicted person is a member of the Defence Force), reprimand, restriction of privileges and extra duties.[269]

---

263 *Submissions*, p. S255 and *Transcript*, p. 470.

264 *Submissions*, p. S648.

265 ibid., p. S810.

266 ibid., p. S808.

267 DOD, *Submissions*, p. S647. The Instruction is reproduced at pp. S653–S656.

268 See paragraph 5.4.16.

269 See subsection 68(1) of the *Defence Force Discipline Act 1982*.

d) Public Service Act Review Group

5.3.22 As part of its recent study, the Public Service Act Review Group considered the manner in which misconduct is dealt with in the Public Service. The Review Group reported that:

> There was widespread criticism of the complexity and legalistic nature of the current provisions and their heavy emphasis on process and concepts analogous to the criminal law. The philosophy and language of the process is outdated and out of touch with modern management philosophies.[270]

5.3.23 The Review Group established a working party to examine the issue and to propose a new set of provisions. The recommendations of the working party were largely endorsed by the Review Group. The Review Group recommended that the language of the misconduct provisions should be decriminalised as the relevant offences generally concern administrative misdemeanours.[271] The Review Group also recommended that the new Act should, among other things, define misconduct, contain heads of power for secretaries to deal with allegations of misconduct expeditiously and emphasise that less serious misconduct should be dealt with as far as possible by informal means (such as counselling and mediation) and a more formal process should only be adopted in serious cases.[272]

5.3.24 The Assistant Minister for Industrial Relations, the Hon Gary Johns MP, issued a media release commenting on the Review of the Public Service Act on 4 May 1995. The Government indicated that it would proceed with all but six of the recommendations in the Review Report (the recommendations which will not be implemented do not relate to the discussion above). The Government will replace the current Act with a new 'principles-based' Act.[273] The Government also expressly agreed to the inclusion of a broadly based code of conduct in the new Act.[274]

e) Conclusions

5.3.25 The Committee notes the PSC's view that the range of sanctions currently available is adequate and that any extension of the range of penalties would not accord with the philosophy of the disciplinary code. The view of the Public Service Act Review

---

270 *Report of the Public Service Act Review Group*, AGPS, Canberra, December 1994, p. 65.

271 ibid., p. 66, p. 67 (See recommendation 60).

272 ibid., p. 67. (See recommendations 58, 61, and 65).

273 The Hon Garry Johns MP, *Media Release: Review of the Public Service Act*, 4 May 1995, p. 1.

274 ibid., p. 3.

Group appears to be in line with this philosophy as it favours decriminalisation of the existing misconduct provisions.

5.3.26 The Committee recognises that as the disciplinary system is fully devolved and disciplinary matters are the responsibility of departmental secretaries, the application of sanctions may vary slightly between departments. However, the Committee notes that including heads of power in the new Act which will allow secretaries to deal with misconduct expeditiously (as recommended by the Public Service Act Review Group) may alleviate some of the concerns expressed in submissions to the inquiry about delays in the application of sanctions for misconduct. The Committee agrees with the Public Service Act Review Group that the language of the Act should reflect that the offences are administrative in character and less serious misconduct should be dealt with by informal means where possible.

5.3.27 The Committee concludes that the existing administrative sanctions which can be applied to officers who wrongly disclose third party information are adequate. It does not favour an increase in the maximum fine under the Public Service Act as an increase would make the fine more akin to a criminal penalty than an administrative sanction. This would not be in accordance with the philosophy of a disciplinary code.

5.4 Relevant criminal penalties

5.4.1 In earlier chapters, the Committee noted a number of measures that can assist in preventing the disclosure of confidential third party information. Those measures include physical security, computer audit trails, the information privacy principles and fostering a 'privacy culture' within the Commonwealth Government and its agencies. Criminal secrecy provisions provides a means of ensuring that penal sanctions can be imposed for serious misuse of confidential information. The existence of such provisions complements the development of a 'privacy culture' and reinforces the value that should be placed on the confidentiality of third party personal and commercial information.

5.4.2 For the purposes of the following discussion, the relevant provisions of the Crimes Act will be referred to as general secrecy provisions. The secrecy provisions in legislation dealing with the activities of various departments will be referred to as specific secrecy provisions.

5.4.3 It is useful to preface a discussion of penalties for criminal offences with an outline of some of the general sentencing provisions in the Crimes Act. Section 4D of the Crimes

Act provides that all penalties contained in the Act are maximum penalties.[275] The pecuniary penalty is calculated by reference to a formula contained in the Crimes Act[276]. According to that formula, twelve months imprisonment equates to 60 penalty units. As a penalty unit is $100[277], twelve months imprisonment is equivalent to a $6000 fine. A pecuniary penalty can be imposed in addition to, or instead of, a penalty of imprisonment.[278]

5.4.4 As outlined in chapter 2, the general offences in the Crimes Act which are relevant to the disclosure of third party confidential information are principally section 70, section 79, section 73 and sections 76B and 76D. Subsection 70(1) prohibits the disclosure of information by Commonwealth officers. It provides that:

> A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he is authorized to publish or communicate it, any fact or document which comes to his knowledge, or into his possession, by virtue of being a Commonwealth officer, and which it is his duty not to disclose, shall be guilty of an offence.

Subsection 70(2) creates a similar offence for former Commonwealth officers. The maximum penalty for these offences is two years imprisonment.

5.4.5 A Commonwealth officer includes officers within the meaning of the Public Service Act; persons permanently or temporarily employed in the Public Service of a Territory or with the Defence Force or in the Service of a Commonwealth public authority; a member of the Australian Federal Police; persons who perform services for or on behalf of the Commonwealth in certain circumstances and employees of Australia Post in some circumstances.[279]

5.4.6 Subsection 79(3) of the Crimes Act is also a relevant provision. Subsection 79(3) provides that:

> If a person communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information to a person, other than:
> (a) a person to whom he is authorized to communicate it; or
> (b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his duty to communicate it:

---

275 Courts can, of course, impose lesser sentences.

276 Subsection 4B(2) of the Crimes Act.

277 Subsection 4AA(1) of the Crimes Act.

278 Subsection 4B(2A) of the Crimes Act. The penalty may not exceed 2000 penalty units.

279 Subsection 3(1) of the Crimes Act.

> or permits a person, other than a person referred to in paragraph (a) or (b), to have access to it, he shall be guilty of an offence.

The definition of prescribed information refers to a duty to keep certain information secret. The maximum penalty for this offence is 2 years imprisonment.

5.4.7 Section 70 and subsection 79(3) do not indicate in themselves the circumstances in which a duty arises. For persons employed under the Public Service Act the relevant duty arises under regulation 35 of the Public Service Regulations.[280] Regulation 35 is set out at paragraph 5.2.2.

5.4.8 Section 73 of the Crimes Act is also relevant to the protection of confidential third party information. It deals with the corruption and bribery of Commonwealth officers. Subsection 73(2) creates an offence where a Commonwealth officer asks for or receives a benefit on the understanding that the exercise of her or his duty as a Commonwealth officer will be influenced or affected. Subsection 73(3) provides that an offence has been committed where a person, in order to influence or affect a Commonwealth officer in the exercise of her or his duty, gives or confers or promises a benefit to a Commonwealth officer. The corruption and bribery of Commonwealth officers attracts a maximum penalty of two years imprisonment.

5.4.9 There are also various offences relating to computers which are relevant to a discussion of penalties concerning the wrongful disclosure of confidential information. These offences protect information while it is in a computer system. The relevant offences include obtaining unlawful access to data in Commonwealth and other computers or obtaining access by means of a Commonwealth facility.[281] The offences attract a maximum penalty of six months imprisonment.

5.4.10 There are also aggravated offences where the offender intends to defraud or gain access to data which the person knows or ought reasonably to know relates to prescribed matters[282]. Prescribed matters include, among other things, the personal affairs of any person, trade secrets and commercial information the disclosure of which could cause advantage or disadvantage to any person. These offences carry a maximum penalty of two years imprisonment.

---

280 ibid., *Submissions*, p. S361.

281 Subsections 76B(1) and 76D(1) of the Crimes Act.

282 Paragraphs 76B(2)(b) and 76D(2)(b) of the Crimes Act.

5.4.11 Evidently a maximum penalty of two years imprisonment is generally standard for the offences in the Crimes Act which are relevant to the protection of third party information (with the exception of the two computer offences described at paragraph 5.4.9).

5.4.12 The penalties of the specific secrecy provisions vary greatly. For example, a breach of subsection 130(1) of the *Health Insurance Act 1973* attracts a penalty of $500 while a breach of section 16 of the *Income Tax Assessment Act 1936* carries a $10 000 fine or 2 years imprisonment or both. The penalties which attach to all the various secrecy provisions are listed in tabular form at Appendix D of the original submission of the Attorney-General's Department.[283]

5.4.13 It is also interesting to note the secrecy provisions relevant to government business enterprises. As mentioned in the discussion of administrative sanctions, subsection 90H(2) of the *Australian Postal Corporation Act 1989* prohibits a person from knowingly or recklessly engaging in prohibited conduct. Prohibited conduct is the unauthorised use or disclosure of information or a document.[284] The same prohibitions are also imposed on former employees.[285] The maximum penalty for these offences is two years imprisonment. Alternatively, disclosure of third party information by former or current employees of Australia Post may invoke prosecution under section 70 of the Crimes Act. Furthermore, on engagement all employees are required to acknowledge that they are bound by section 70 of the Crimes Act and that sensitive information will not be used post employment to the detriment of Australia Post.[286]

5.4.14 The *Telecommunications Act 1991* contains confidentiality provisions relevant to Telstra employees. Subsections 88(1) and 88(2) of the Act prevent a person that is, or has been, a prescribed person from disclosing or using any information or document that relates to certain matters (including the affairs or personal particulars of another person[287]) or comes to the person's knowledge because the person is a prescribed person. A prescribed person means an employee of a carrier, a supplier and an employee of a supplier.[288] The maximum penalty for these offences is two years imprisonment.

---

283 *Submissions*, p. S418. The table was prepared as at October 1992.

284 Subsection 90H(1) of the Australian Postal Corporation Act.

285 Subsections 90LB(1) & (2) of the Australian Postal Corporation Act.

286 *Submissions*, pp. S254 and S261.

287 Affairs or personal particulars include unlisted telephone numbers and addresses.

288 Subsection 88(5) of the Telecommunications Act.

5.4.15 Obligations of confidentiality are imposed on persons who acquire third party information in the course of performing a contract with the Commonwealth. Confidentiality clauses are included as a matter of course in Commonwealth contracts where the contractor may have access to confidential third party information.[289] The Attorney-General's Department informed the Committee that the intending contractor's attention would usually be drawn to the relevant provisions in Commonwealth legislation.[290] Commonwealth contractors must comply with the provisions of the Crimes Act, including section 70. Section 70 of the Crimes Act applies to Commonwealth contractors by reason of the definition of 'Commonwealth officer' as a person who 'performs services for or on behalf of the Commonwealth, a Territory or a public authority under the Commonwealth'.[291]

5.4.16 As outlined at paragraph 5.3.20, Defence Instruction General (08-1) appears to deal with the protection of confidential information held by the ADF.[292] Failure to comply with such an instruction can result in a charge under section 29 of the *Defence Force Discipline Act 1982*.[293] The maximum penalty for an offence under that section is twelve months imprisonment. Members of the ADF may also subject to section 70 of the Crimes Act by virtue of the definition of 'Commonwealth officer' in that Act.[294]

5.5 Adequacy of applicable criminal penalties

a) General secrecy provisions

5.5.1 It appears that two years imprisonment is the standard maximum penalty in the general secrecy provisions of the Crimes Act relevant to the disclosure of third party information.[295] The evidence did not generally focus on the adequacy of the penalties in the Crimes Act as departments tended to concentrate on their own specific legislation in assessing the adequacy of penalties for the unauthorised disclosure of third party information. The Australian Taxation Office (ATO) did comment that the penalties in

289 Attorney-General's Department, *Submissions*, p. S949.

290 ibid.

291 See paragraph 3(1)(c) of the Crimes Act.

292 See paragraph 5.3.20.

293 DOD, *Submissions*, p. S647. The scale of punishments in subsection 68(1) of the Defence Force Discipline Act is also relevant from paragraph (d) onwards, but the maximum period of detention would only be one year.

294 See paragraph 3(1)(aa) of the Crimes Act.

295 Although subsections 76B(1) and 76D(1) are exceptions to this general rule.

the Crimes Act, combined with the secrecy provisions in the laws administered by the Commissioner of Taxation, worked well.[296]

5.5.2 If a penalty is adequate, then it may act as a deterrent to the commission of a crime. Indeed it has been suggested that the worth of the secrecy provisions in the Crimes Act is measured by governments not in the number of prosecutions, which are few, but in their deterrence value.[297] However, while prosecutions under the Crimes Act are few, this may not indicate the adequacy of the penalty in deterring potential offenders, but rather may be illustrative of the small number of people actually apprehended for those particular offences.[298]

5.5.3 Having noted the difficulties in determining the adequacy of the penalties in the secrecy provisions of the Crimes Act, it is relevant to focus also on the adequacy of the provisions themselves as the issues are interrelated.

(i) Section 70

5.5.4 Section 70 of the Crimes Act does not delimit the type of information it protects other than by reference to a duty not to disclose.[299] It is a broad catch-all provision and could potentially apply to both the disclosure of official information as well as the disclosure of third party information.[300] But despite the breadth of the provision, there have been few prosecutions under it. The section has been described as:

> . . . very difficult to get off the ground . . . and magistrates and other judicial officers tend to regard it as being such a broad provision as to perhaps impact adversely on its utility.[301]

5.5.5 The need for reform of section 70 has been recognised for some time. In 1979 the Senate Standing Committee on Legal and Constitutional Affairs recommended that section 70 be amended to limit the categories of information that it is an offence to disclose and to establish procedural safeguards for any person who may face prosecution

---

296 *Submissions*, p. S334. See also comment by DILGEA (as it then was) that it was happy with the penalties imposed (*Transcript*, p. 358).

297 See McGuiness J., 'Secrecy Provisions in Commonwealth Legislation', (1990) FLR 49 at 72.

298 For example, see paragraphs 5.5.6–5.5.8.

299 DPP, *Transcript*, p. 339.

300 For these purposes, official information includes, among other things, information relating to national security, defence and foreign affairs.

301 DPP, *Transcript*, p. 339

under that section.[302] In 1983 the Human Rights Commission recommended that section 70 be limited to restrictions which are necessary to protect the rights and reputations of others and to protect national security, public order or public health or morals.[303] The Commission also noted that the provisions of the existing law were viewed as seriously defective from the point of view of effective law enforcement.[304]

5.5.6 A survey of the prosecution statistics in the annual reports of the Director of Public Prosecutions reveals the small number of prosecutions. In 1993-4 one offence under section 70 was dealt with on indictment and there were no summary offences.[305] In 1992–93 there was one indictable offence under section 70 of the Crimes Act and five matters were dealt with summarily.[306]

5.5.7 In the period 1 July 1991 – 29 January 1993, 34 offences under section 70 of the Crimes Act were investigated by the AFP and 7 offences were cleared.[307] The AFP concluded that the statistics indicate that referral of suspected secrecy breaches to the AFP is a reasonably rare occurrence.[308] Evidently there are not a large number of investigations or prosecutions under section 70 of the Crimes Act.

5.5.8 Following the DPP's appearance at a public hearing, the Office made a further submission addressing the utility of section 70 of the Crimes Act in preventing the unauthorised disclosure of information, particularly taxation information. The DPP records list thirteen completed prosecutions under section 70 in the five years preceding December 1992.[309] It appears that, as far as can be ascertained, only one of the defendants in those cases was an employee of the ATO.[310] The DPP suggested that the

---

302 *Report on Aspects of the Freedom of Information Bill 1978 and the Archives Bill 1978*, para 21.27 cited in the Attorney-General's Department, *The disclosure of official information*, p. 13.

303 *Review of Crimes Act 1914 and other Crimes Legislation of the Commonwealth*, para. 26 cited in Attorney-General's Department, ibid., p. 13.

304 Cited in ibid., p. 13. Also see Australian Federal Police, *Submissions*, p. S990.

305 Commonwealth Director of Public Prosecutions, *Annual Report 1993-94*, AGPS, Canberra, pp. 132, 129.

306 Commonwealth Director of Public Prosecutions, *Annual Report 1992-93*, AGPS, Canberra, pp 125, 121.

307 *Submissions*, p. S989.

308 ibid.

309 See *Transcript*, p. 339 and *Submissions*, p. S976.

310 The DPP noted that there may have been other matters which were not recorded. At December 1992 (the time of the submission), the computerised case management system did not operate in Hobart or Darwin and, at that stage, it had only been in operation in the Australian Capital Territory for eighteen months.

threat of prosecution under section 70 may have been a factor in deterring ATO officers from unlawfully releasing confidential information.[311]

5.5.9 A number of problems with section 70 were identified during the Committee's inquiry. A prosecution under section 70 requires the identification of a duty not to disclose. The source of this duty (which creates the legal liability) is not located in the Crimes Act and therefore lacks precision. As noted earlier, the general duty imposed on all public servants by regulation 35 of the Public Service Regulations is the source of the duty. It has been suggested that the primary duty should be expressed in a statute as it would then receive greater scrutiny and would be more accessible to those to whom it applies.

5.5.10 Where Commonwealth officers are not employed under the Public Service Act[312], a duty may arise out of the terms and conditions of the person's contract of employment or contract to perform services. If such a term does not exist, a duty of non-disclosure would need to be implied. The Attorney-General's Department suggested that *it is not clear that such a term would be implied because a court may be reluctant to find* that an offence has been committed if the breach of duty is only a moral obligation (and not imposed by law).[313]

(ii) Section 79

5.5.11 The disclosure of third party information may be an offence under subsection 79(3) of the Crimes Act. The liability of a Commonwealth officer under subsection 79(3) is dependent on the existence of a duty to keep the information secret. The information protected includes information held by a person where 'by reason of its nature or the circumstances under which it was entrusted to him or it was made or obtained by him or for any other reason, it is his duty to treat it as secret'[314]. Subsection 79(3) makes it a criminal offence for any person to disclose such information. The maximum penalty for this offence is two years imprisonment.

5.5.12 It has been suggested that '. . . this linkage to a separate duty is unsatisfactory, because it has potentially very wide application and renders the operation of the law less certain'.[315] The general secrecy provisions (that is, sections 70 and 79) have also been

311 *Submissions*, p. S976.

312 See subsection 3(1) of the Crimes Act.

313 *Submissions*, p. S361.

314 See subsection 79(1)(b) of the Crimes Act.

315 Attorney-General's Department, *The protection of official information*, October 1993, p. 13.

criticised because the provisions make no distinction between the nature or importance of the duties of a Minister and those of the lowest public servant.[316]

5.5.13 Section 79 is rarely used in practice. For example, during 1993–94 there was only one offence on indictment under this section[317], one offence on indictment of the same character during 1992–93[318] and no offences on indictment in 1991–92[319].

(iii) Section 73

5.5.14 The disclosure of confidential information for financial gain may amount to a breach of section 73 of the Crimes Act (which deals with bribery and corruption). The maximum penalty for the offences under that section is two years imprisonment. Persons convicted of that offence may be required to surrender the proceeds of, or benefits derived from, the commission of such offences.[320] Under the *Proceeds of Crime Act 1987*, the Commonwealth may confiscate the proceeds from a crime if a Commonwealth officer has been convicted of an indictable offence.[321]

5.5.15 The ICAC report discussed the bribery laws in the New South Wales context. It commented that the law relating to bribery may be invoked if a public official was paid for releasing the information. However, the offence is not relevant where no public official was paid (or no payment can be proved).[322] The same issue arises in relation to section 73 of the Crimes Act and consequently, that provision may have limited utility in protecting confidential information.

5.5.16 Section 73 of the Crimes Act is another general provision which is rarely used in practice. In 1993–94 there were three defendants dealt with on indictment under section 73 (and section 73A[323]) and three summary offences under the same section.[324]

---

316 McGuiness, op. cit., p. 52.

317 Commonwealth Director of Public Prosecutions, *Annual Report 1993-94*, AGPS, Canberra, 1994, p. 132. There was also one offence of this type dealt with summarily in 1993-94 (see *Annual Report*, p. 129).

318 Commonwealth Director of Public Prosecutions, *Annual Report 1992-93*, op. cit., p. 126. There were no offences of this type that were dealt with summarily in the same period (see *Annual Report*, p. 122).

319 Commonwealth Director of Public Prosecutions, *Annual Report 1991-92*, AGPS, Canberra, p. 169. There were no summary offences (see *Annual Report*, p. 164).

320 Attorney-General's Department, *Submissions*, p. S390.

321 See section 14 of the Proceeds of Crime Act 1987. Note that, under section 19, the tainted property may be forfeited to the Commonwealth.

322 Independent Commission Against Corruption, *Report on Unauthorised Release of Government Information* Volume 1 (*ICAC Report*), August 1992, p. 169.

323 Section 73A of the Crimes Act deals with the corruption and bribery of Members of Parliament.

During 1992–93 there were no defendants dealt with on indictment and four matters were dealt with summarily.[325]

5.5.17 However, while prosecutions under section 73 are reasonably rare, the DIEA brought a charge under that section to the attention of the Committee.[326] An officer of that department was charged with agreeing to accept monies in connection with unauthorised disclosure of data.[327] The sanctions imposed on the officer were a 15 month good behaviour bond and 156 hours of community work.

(iv) *Sections 76B and 76D*

5.5.18 Although sections 76B and 76D of the Crimes Act were identified as other general secrecy provisions by the Attorney-General's Department, there was little discussion of the adequacy of the penalties and the provisions themselves during the inquiry. The ICAC Report noted that, in relation to the New South Wales law dealing with unauthorised access to computer data, the laws could only be invoked if the information was accessed or obtained through use of a computer.[328] Obviously sections 76B and 76D would only be useful in penalising officers who wrongly disclose third party information in limited circumstances.

5.5.19 In 1993–94 there were two defendants dealt with on indictment under sections 76B–76E and five offences dealt with summarily[329], and during 1992–93 there was one matter dealt with on indictment and eight matters dealt with summarily.[330] The statistics do not detail whether the offences related to the unauthorised disclosure of third party information held by the Commonwealth Government and its agencies.

5.5.20 As outlined at paragraph 5.4.11, a maximum penalty of two years imprisonment is generally standard for the relevant offences in the Crimes Act. The evidence does not appear to support the conclusion that the penalties in the Crimes Act provisions are inadequate. Rather it is the provisions themselves which may be inadequate because of problems with specification of the duty, problems arising from the breadth of the information which is protected and difficulties in relation to prosecutions. It appears that the insertion of provisions in the Crimes Act which deal expressly with the protection of

---

324 *DPP Annual Report 1993-94*, op. cit., pp. 132, 129.

325 *DPP Annual Report 1992-93*, op. cit., pp. 125, 121.

326 *Submissions*, p. S897.

327 The officer was charged under subsection 73(1) of the Crimes Act and the *Secret Commissions Act*.

328 *ICAC Report*, op. cit., p. 169.

329 *DPP Annual Report 1993-94*, op. cit., pp. 132, 129.

330 *DPP Annual Report 1992-93*, op. cit., pp. 125, 122.

third party information may be advisable and proposals for reform are discussed in chapter 7.

b) Specific secrecy provisions

5.5.21 There are now more than 150 secrecy provisions in Commonwealth laws and more than 100 different statutes which contain one or more such provision.[331] As was illustrated at paragraph 5.4.12, the penalties for disclosing confidential third party information vary markedly in the specific secrecy provisions from a $500 fine to a $10 000 fine or two years imprisonment or both.

5.5.22 Some departments commented favourably on the adequacy of the penalties for secrecy offences in their respective legislation. For example, the Australian Customs Service considered the penalty in section 16 of the *Customs Administration Act 1985* adequate and the ATO considered that the penalties in the statutes it administers 'work well'.[332]

5.5.23 Consistency in the application of criminal penalties in this area was commented upon. Some submissions made general comments concerning the desirability of uniformity in penalties[333] or at least consistency in the application of penalties and sanctions across all Commonwealth agencies.[334]

5.5.24 An example of the current inconsistencies in some penalties was brought to the Committee's attention by the Health Insurance Commission.[335] The inconsistency exists in relation to subsection 135A(1) of the *National Health Act 1953* and subsection 130(1) of the *Health Insurance Act 1973*.

5.5.25 Subsection 135A(1) of the National Health Act effectively provides that it is an offence for an officer to directly or indirectly divulge or communicate any information with respect to the affairs of a third person acquired by the officer in the performance

---

331 *Submissions*, p. S362.

332 *Submissions*, p. S494 and *Submissions*, p. S334 respectively. See also Department of Defence, *Submissions*, p. S647 and Australian Bankers Association, *Submissions*, p. S821.

333 Department of Health, Housing and Community Services (as it then was), *Submissions*, p. S625.

334 For example, AIHW, *Submissions*, p. S90; HIC, *Submissions*, p. S201; DSS, *Submissions*, p. S447; Law Society of New South Wales, *Submissions*, p. S859; and DEET, *Submissions*, p. S929.

335 See *Submissions*, p. S201.

of his duties. Exceptions to this prohibition exist such that the information can be divulged to certain individuals or organisations for specified circumstances. If this occurs, subsection 135A(9) of the Act makes it an offence for the person to whom the information is legally divulged to then divulge or communicate that information to any other person. The maximum penalties for these offences are a $5000 fine or 2 years imprisonment or both.

5.5.26 Subsections 130(1) and 130(9) of the Health Insurance Act create almost identical offences, yet the penalty for those offences is $500. Information acquired under the National Health Act relates predominantly to pharmaceutical benefits and aged care. Information acquired under the Health Insurance Act deals with Medicare benefits, pathology and diagnostic imaging. It does not appear that the information acquired under the National Health Act is any more sensitive than that acquired under the Health Insurance Act. Therefore, consistent penalties for secrecy offences in these statutes appear to be justified. (The Committee notes that the Australian Law Reform Commission may examine the elements of secrecy offences in health legislation and relevant penalties as part of its reference on health, housing and community services legislation.[336] Recommendation 29 is relevant in this context.[337])

5.5.27 Penalties in a number of the specific provisions are out of step with the general sentencing provisions in the Crimes Act. As outlined at paragraph 5.4.3, the effect of the section 4B of the Crimes Act is that, unless a contrary intention appears, a pecuniary penalty can be imposed in addition to, or instead of, a penalty of imprisonment for a Commonwealth offence and twelve months imprisonment is equivalent to a $6000 fine. The penalties in some statutes reveal a contrary intention. For example, the penalty under subsection 135A(1) of the *National Health Act 1953* is expressed as '$5000 or imprisonment for 2 years, or both' and the penalty for a breach of subsection 3C(2) of the *Taxation Administration Act 1953* is expressed as '$10,000 or imprisonment for 2 years, or both'. Penalties under the Crimes Act are expressed as imprisonment terms. A two year imprisonment term equates to a pecuniary penalty of $12 000. Thus the penalties in a number of statutes are out of step with the formula in the Crimes Act. Consistency in the range and expression of penalties in criminal secrecy provisions is desirable.

---

336 The ALRC received this reference on 18 August 1992. The Commission is to make recommendations on how Commonwealth legal policies (including administrative law, secrecy, privacy and criminal law), social justice and human rights should be reflected in new program legislation. In relation to this reference, the ALRC has completed a report on aged care and an interim report on child care, and it has commenced work on disability services. The review of health legislation will then follow.

337 See para. 7.7.3.

5.5.28 However, the Committee notes that while consistency in penalties is desirable as an overall objective, there may need to be some flexibility depending on the sensitivity of the information to be protected. The Law Society of New South Wales noted that the statute establishing the agency should address the peculiar penalties and sanctions required for protecting the category of information collected and used by that agency.[338] Mr Roden also commented that the varying degrees of sensitivity of certain types of protected information may justify different penalties.[339] Other submissions recognised the need for a broad span of penalties.[340]

5.5.29 The Committee acknowledges the need for some variation in penalties proportionate to the sensitivity of the information involved. However, the Committee does not consider that this need for flexibility should necessarily result in marked differences between maximum penalties in various statutes for third party information offences.

5.5.30 The Attorney-General's Department noted that in assessing the adequacy of penalties, it is necessary to consider the potential seriousness of the offence. The maximum penalty is appropriate to the worst kind of breach and it is important to provide courts with a range of sentencing options up to the maximum term of imprisonment or fine.[341] Setting a maximum penalty which is appropriate for the most serious crimes still allows the imposition of a lesser penalty where the situation warrants it.

5.5.31 There was some comment to the effect that agencies would generally use the secrecy provisions in their own statutes to prosecute the unauthorised disclosure of confidential information and would only refer serious breaches to the AFP for prosecution under the general Crimes Act provisions.[342] At least one agency expressed a preference for using the provisions in the Crimes Act.[343]

5.5.32 The specific secrecy provisions have been criticised as neither uniform nor consistent.[344] The Attorney-General's Department commented that:

---

338 *Submissions*, p. S859.

339 *Submissions*, p. S39.

340 For example, Attorney-General's Department, *Submissions*, p. S347; Privacy Commissioner, *Submissions*, p. S559.

341 *Submissions*, p. S390.

342 For example, ANAO, *Submissions*, p. S141 and ATO, *Submissions*, p. S334.

343 DILGEA (as it then was), *Transcript*, p. 358.

344 See, for example, Professor Greg Tucker, *Submissions*, p. S845.

> . . . the large number and diverging nature of the specific secrecy provisions means that the law in this area has become increasingly complex. The provisions have been enacted over a number of years in a piecemeal fashion to deal with specific areas of Commonwealth activity and to meet perceived deficiencies in the Crimes Act provisions. Their scope has been influenced by varying philosophies at different periods.[345]

5.5.33 Secrecy provisions do not generally impose a total prohibition on the dissemination or use of information acquired by Government. Some provisions protect all information acquired by an officer in the performance of his or her duties; other provisions are narrower in effect. Most provisions include some exceptions to the prohibition on disclosure. The exceptions to the prohibition on disclosure vary greatly in expression and effect.[346] So as well as the inconsistent penalties, the specific secrecy provisions also reveal other inconsistencies in the information protected and the exceptions to the prohibition on disclosure.

5.5.34 The submission of the Attorney-General's Department discusses the different approaches to protecting information that are evident in existing legislation.[347] An example of those differing approaches is outlined below.

5.5.35 Subsection 127(1) of the *Australian Securities Commission Act 1989* requires the Commission to 'take all reasonable measures to protect from unauthorised use or disclosure information given to it in confidence.' However, subsection 127(4) provides that where the Chairperson of the Commission is satisfied that particular information will enable or assist any agency within the meaning of the *Freedom of Information Act 1982* (or the government or agency of a State, Territory or foreign country) to perform or exercise its functions or powers, then disclosure to the agency is authorised. In contrast, section 16 of the *Income Tax Assessment Act 1936* is more restrictive. Subsection 16(4) of that Act provides that the principal secrecy provision does not prohibit the Commissioner, or any other authorised person, from communicating any information to specified persons.[348] Paragraphs (a) to (l) of subsection 16(4) list officials who may receive information for specific purposes.

5.5.36 It has been suggested that the different approaches adopted in the specific provisions have confused the principles regulating the handling of information within government.[349] It has also been suggested that the extent to which the coverage of the

---

345 Attorney-General's Department, *Submissions*, p. S362.

346 ibid.

347 *Submissions*, p. S365.

348 ibid., p. S365.

349 McGuiness, op. cit., p. 61.

specific secrecy provisions is appropriate with regard to the disclosure of personal information by officers is open to question.[350] The Privacy Commissioner commented that 'the extent of the patchwork of secrecy provisions is uncertain, but does not provide general coverage of all Commonwealth organisations'.[351]

5.5.37 There was also some concern that the information protected by some statutes may be too broadly defined. The Department of Community Services and Health (as it then was) noted that the secrecy provisions in the National Health Act protect 'information with respect to the affairs of a third person'.[352] The Department gave an example of the material which the current definition covers. It includes data about a patient's medical services, the practice addresses of doctors and pharmacy addresses. Information concerning an individual's medical services is clearly sensitive and should be protected while doctors' and pharmacy addresses can be found in telephone directories.[353] The Department suggested that it should be possible to distinguish between the two categories of information.[354] As mentioned previously, the Australian Law Reform Commission currently has a reference on health and community services legislation. It may be appropriate for that inquiry to consider this issue.

5.5.38 The Attorney-General's Department viewed the crucial question as whether the existing regime effectively targets the type of confidential third party information which requires protection.[355] A later submission from the Department identified some classes of 'third party' information which were not protected by specific secrecy provisions at that time.[356] The examples cited include:

(a) information relating to the payment of benefits and medical treatment for veterans which is held by the Department of Veterans Affairs;
(b) information concerning applicants for legal aid from the Commonwealth;
(c) certain educational records held by the Commonwealth for the purposes of programs administered by the Department of Employment, Education and Training; and
(d) personnel records of most Commonwealth public servants.[357]

---

350 Attorney-General's Department, *Submissions*, p. S388.

351 *Submissions*, p. S582.

352 *Submissions*, p. S628. See subsection 135A(1) of the National Health Act and also subsection 130(1) of the Health Insurance Act.

353 ibid.

354 ibid.

355 Attorney-General's Department, *Submissions*, p. S388.

356 The relevant submission was dated 4 January 1994.

357 See *Submissions*, p. S1001.

5.5.39 The Department noted that the unauthorised disclosure of these classes of information is subject to section 70 of the Crimes Act. However, if the proposals of the Review of Commonwealth Criminal Law (chaired by the Rt Hon Sir Harry Gibbs AC KBE and known as the Gibbs Committee[358]) for the repeal of section 70 of the Crimes Act were adopted (and the Crimes Act were to prohibit only the disclosure of official information and not the disclosure of third party information), there would be no criminal penalties that would apply to the disclosure of those classes of confidential information outlined at paragraph 5.5.38.[359]

c) Conclusions

5.5.40 While some departments view the current penalties for the wrongful disclosure of confidential information as adequate, the current piecemeal approach to protecting third party information, as illustrated in the various specific secrecy provisions, suggests there is a need for a more consistent approach to the protection of third party information. The specific secrecy provisions have been influenced by a variety of philosophies and impose varying penalties. They also protect information to varying extents and there are different qualifications to the prohibitions on disclosure.

5.5.41 As outlined previously, the problems with the general secrecy provisions in the Crimes Act include the breadth of section 70, failure to include the duties in the principal Act, a lack of precision in the duties, deficiencies from the point of view of law enforcement and the limited application of sections 73, 76B and 76D of the Crimes Act. The problems with the general and specific secrecy provisions reveal a need for rationalisation and the Committee discusses proposals for rationalisation in chapter 7.

5.5.42 Having determined that there is a need for a new approach to the existing secrecy provisions which deal with the disclosure of confidential third party information held by the Commonwealth Government, the adequacy of the penalties that can be applied to the persons who procure the wrongful disclosure of third party information will now be considered.

---

358 The recommendations of the Gibbs Committee in this area are discussed in chapter 7.

359 See Attorney-General's Department, *Submissions*, p. S388. The Department of Health, Housing and Community Services (as it then was) noted also that if the Gibbs Committee proposal was adopted, then it would not be able to rely wholly on the provisions of the Crimes Act to assist in protecting sensitive information which is not subject to a specific secrecy provision. See *Submissions*, p. S626.